Carlos Ivorra Castillo

TEORÍA DE GRUPOS

La importancia de la teoría de grupos se puso de relieve hace muy poco, cuando unos físicos, usando la teoría de grupos, predijeron la existencia de una partícula que no había sido observada nunca, y describieron las propiedades que debía tener. Experimentos posteriores demostraron que esa partícula existe realmente y tiene esas propiedades.

IRVING ADLER

Índice General

Preámbulo

Este libro forma parte de la "tercera edición" de mis libros de *Álgebra* [Al], *Geometría* [G] y *Análisis Matemático* [An], de los que he separado la *Teoría de grupos* en un nuevo volumen [TG]. La diferencia esencial es que he suprimido muchos ejemplos y aplicaciones que ahora se encuentran en la serie de libros "introductorios" *Introducción a la teoría algebraica de números* [ITAl], *Introducción a la geometría euclídea* [IGE], *Introducción a la teoría analítica de números* [ITAn] e *Introducción al cálculo diferencial* [IC] y los he sustituido por contenidos nuevos.

Como en la edición anterior, los contenidos están distribuidos entre los cuatro libros de modo que pueden leerse simultáneamente siguiendo el orden que muestra el esquema de la página siguiente.

El primer capítulo de [Al] es una introducción a la teoría de conjuntos, cuyos aspectos más técnicos (los relacionados con el axioma de elección y la teoría de cardinales infinitos) se han relegado a dos apéndices. La teoría descrita es la teoría de Zermelo, que resulta más que suficiente para formalizar los contenidos de los cuatro libros. El único inconveniente es que "se queda corta" para desarrollar plenamente la teoría de cardinales infinitos, pero hemos preferido reducirla a lo imprescindible, aun al precio de no poder enunciar con total precisión algunos resultados sobre rango y dimensión de módulos y espacios vectoriales de dimensión infinita que, aunque resulta natural presentarlos al tratar estos conceptos, no son realmente necesarios en ningún momento.

El libro de Álgebra consta ahora (tras el capítulo [Al I] de fundamentos) de un primer bloque de cinco temas con los contenidos básicos del "álgebra abstracta" (incluyendo el álgebra lineal) y un segundo bloque de aplicaciones y resultados más avanzados.

El libro de Geometría empieza con dos capítulos que exponen la geometría euclídea a partir de unos axiomas al estilo de Hilbert, seguidos de un segundo bloque de cuatro capítulos dedicados a la geometría analítica y sus aplicaciones y un tercer bloque en el que analizamos más a fondo las geometrías afín y euclídea estudiadas en el bloque precedente e introducimos la geometría proyectiva y las geometrías no euclídeas.

El libro de Análisis consta de un primer bloque con los preliminares topológicos, un segundo bloque con los hechos básicos del cálculo diferencial e integral y un tercer bloque con temas más avanzados.

Álgebra	Geometría	Análisis	Grupos
Al I Conjuntos			
Al II Anillos	**G I** G. absoluta		
Al III Aritmética	**G II** G. euclídea	**An I** Números reales	**TG I** Elementos
Al IV Módulos	**G III** G. analítica	**An II** Topología I	**TG II** Permutaciones I
Al V Cuerpos I	**G IV** Cuaternios	**An III** Topología II	**TG III** Estructura
Al VI Álgebra lineal	**G V** Biyecciones afines	**An IV** Tª de la medida I	**TG IV** Resolubles
Al VII Ecuaciones	**G VI** Regla y compás	**An V** Calc. diferencial	**TG V** Nilpotentes
Al VIII Enteros algebraicos	**G VII** G. afín	**An VI** Tª de la medida II	**TG VI** Caracteres
Al IX Cuerpos II	**G VIII** G. proyectiva	**An VII** Variedades	**TG VII** Permutaciones II
Al Ap A Ax. de elección	**G IX** Cónicas	**An VIII** Cálc. vectorial	**TG VIII** Clásicos I
Al Ap B Ctos. infinitos	**G X** G. parabólica	**An IX** An. harmónico	**TG IX** Clásicos II
Al Ap C Cuadrados latinos	**G XI** G. hiperbólica	**An X** Holomorfas	**TG Ap A** Banach-Tarski
	G XII G. elíptica	**An Ap A** Sólidos rígidos	
	G Ap A G. Inversiva	**An Ap B** Gravitación	
	G Ap B Hamming		

Finalmente, el libro de Teoría de grupos aparece dividido en el esquema anterior en un primer bloque con la teoría básica y un segundo bloque con contenidos más avanzados.

Salvo los dos apéndices sobre teoría de conjuntos de [Al], los demás apéndices contienen aplicaciones que, por motivos diversos, era preferible exponer unificadamente en lugar de dejarlas dispersas por el texto.

Remitimos a las introducciones de cada uno de los libros para una panorámica general más detallada de sus contenidos.

Introducción

Tal y como se recoge en la introducción de [Al], Cardano publicó en 1545 su *Ars magna,* en la que presentaba fórmulas generales para resolver ecuaciones polinómicas de tercer y cuarto grado, análogas —pero mucho más complicadas— a la conocida fórmula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

para resolver una ecuación $ax^2+bx+c = 0$ de segundo grado. En 1770 Lagrange publicó el primero de una serie de trabajos en los que estudiaba más a fondo las raíces de un polinomio de tercer o cuarto grado, tratando de encontrar una teoría de fondo que permitiera entender las fórmulas de Cardano-Ferrari y, a ser posible, generalizarlas al caso de polinomios de grado mayor que 4. Ese mismo año, el violinista francés Alexandre-Théophile Vandermonde empezó a interesarse por las matemáticas, y en 1771 publicó su *Mémoire sur la résolution des equations,* en la que estudiaba las raíces de los polinomios ciclotómicos, y para ello se valió del estudio de las funciones que quedaban invariantes al permutar dichas raíces.

En términos modernos, podemos hacernos una idea de lo que esto supone considerando el análisis de los números ciclotómicos de orden 5 que llevamos a cabo en el capítulo XVII de [ITAl] para demostrar el último teorema de Fermat para el exponente $p = 5$. Allí consideramos los *números ciclotómicos* (de orden 5), que son los de la forma

$$a_4\omega^4 + a_3\omega^3 + a_2\omega^2 + a_1\omega,$$

donde $a_i \in \mathbb{Q}$. Estos números forman un cuerpo K (el cuerpo ciclotómico de orden 5), que es, de hecho, el menor subcuerpo de $\mathbb{C}$ que contiene las raíces del polinomio ciclotómico quinto

$$c_5(x) = x^4 + x^3 + x^2 + x + 1.$$

En la sección [ITAl 17.3] vimos que el cuerpo K tiene cuatro conjugaciones, es decir, que existen exactamente cuatro aplicaciones $\sigma : K \longrightarrow K$ tales que

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta), \qquad \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$$

(lo que ahora se conoce como los *automorfismos* de K).

En efecto, una aplicación en estas condiciones cumple $\sigma(q) = q$ para todo $q \in \mathbb{Q}$, de donde a su vez se sigue que

$$\sigma(\omega)^4 + \sigma(\omega)^3 + \sigma(\omega)^2 + \sigma(\omega) + 1 = 0,$$

por lo que $\sigma(\omega)$ es necesariamente una de las raíces del polinomio $c_5(x)$, es decir, que $\sigma(\omega) = \omega^i$, para $i = 1, 2, 3, 4$. Además esto determina completamente a σ, luego tenemos exactamente cuatro conjugaciones σ_i determinadas por que $\sigma_i(\omega) = \omega^i$.

En particular, cada conjugación σ_i determina y queda determinada por una permutación de las raíces del polinomio ciclotómico. Por ejemplo, σ_2 se corresponde con la permutación

ω^i	ω	ω^2	ω^3	ω^4
$\sigma_2(\omega^i)$	ω^2	ω^4	ω	ω^3

Lo destacable es que, en principio, podríamos haber dispuesto las cuatro potencias de ω de 24 formas distintas en la segunda fila de la tabla anterior, pero de esas 24 permutaciones posibles, sólo cuatro de ellas determinan conjugaciones del cuerpo ciclotómico K.

Galois Lagrange pronto incorporó a sus investigaciones la técnica de considerar permutaciones de las raíces de un polinomio que eran "admisibles" en el sentido de determinar y estar determinadas por conjugaciones, pero el primero que expresó estas ideas explícitamente —aunque a la vez de forma bastante confusa— fue un joven matemático francés llamado Évariste Galois, que en 1829, a sus 18 años, redactó una memoria en la que esbozó lo que hoy se conoce como la *teoría de Galois,* que unificaba y generalizaba drásticamente algunos de los resultados obtenidos por Lagrange y Vandermonde.

En términos modernos, si $p(x)$ es un polinomio irreducible en el anillo de polinomios $\mathbb{Q}[x]$, existe un único cuerpo $\mathbb{Q} \subset K \subset \mathbb{C}$ determinado por la propiedad de ser el menor cuerpo que contiene a todas las raíces de $p(x)$. Es el que se conoce como *cuerpo de escisión* del polinomio $p(x)$ [Al 5.17], y sus automorfismos forman lo que Galois llamó un *grupo de permutaciones* de sus raíces, el que ahora se conoce como *grupo de Galois* del polinomio dado [Al 7.11].

Para explicar estos términos definimos una *permutación* de un conjunto X como una aplicación $f : X \longrightarrow X$ biyectiva. Es fácil ver que si el conjunto X tiene n elementos, hay exactamente $n!$ permutaciones de X. Por ejemplo, podemos expresar las 6 permutaciones de un conjunto de 3 elementos como

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Así, la segunda permutación σ es la dada por $1\sigma = 2$, $2\sigma = 3$, $3\sigma = 1$, mientras que la última τ es la dada por $1\tau = 1$, $2\tau = 3$, $3\tau = 2$.

Dos permutaciones cualesquiera, como σ y τ, se pueden *componer,* para dar lugar a la permutación $\sigma\tau$ que hace actuar primero a σ y luego a τ, lo que en nuestro ejemplo nos da

$$1(\sigma\tau) = 2\tau = 3, \quad 2(\sigma\tau) = 3\tau = 2, \quad 3(\sigma\tau) = 1\tau = 1,$$

luego $\sigma\tau$ es la quinta de la lista de las seis permutaciones.

Galois definió un *grupo de permutaciones* de un conjunto X como un conjunto (no vacío) G de permutaciones de X que cumpliera dos propiedades:

1. Si $\sigma, \tau \in G$, entonces $\sigma\tau \in G$.
2. Si $\sigma \in G$, entonces $\sigma^{-1} \in G$, donde σ^{-1} es la permutación inversa de σ, es decir, la que cumple $a\sigma^{-1} = b$ si y sólo si $b\sigma = a$.

Por ejemplo, es obvio que el conjunto de todas las permutaciones de un conjunto X es un grupo, al que nos referiremos como el *grupo de simetrías* de X o *grupo simétrico* de X, y lo representaremos por Σ_X. Habitualmente llamaremos Σ_n al grupo de todas las permutaciones de un conjunto de n elementos. Es claro que la naturaleza de tales elementos es irrelevante. Por ejemplo, el grupo Σ_3 consta de las seis permutaciones que hemos indicado más arriba, donde es irrelevante que los objetos permutados se llamen $1, 2, 3$ o bien a, b, c o bien $\omega, \omega^2, \omega^3$, con tal de que sean tres objetos distintos.

En estos términos, Galois observó que las conjugaciones (o los automorfismos) del cuerpo de escisión K de un polinomio irreducible $p(x) \in \mathbb{Q}[x]$ pueden identificarse con los elementos de un grupo de permutaciones del conjunto de sus raíces, que no es necesariamente el grupo formado por todas ellas, sino que puede ser un subgrupo. Así, hemos visto que, aunque el grupo Σ_4 consta de 24 permutaciones, el grupo de Galois del polinomio ciclotómico quinto es un subgrupo formado únicamente por 4 de ellas. En general, calcular el grupo de Galois de un polinomio es un problema no trivial.

Para tratar con grupos de permutaciones conviene introducir una notación más concisa. Así, las seis permutaciones de Σ_3 que hemos enumerado más arriba se expresan más eficientemente en la forma

$$1, \quad (123), \quad (321), \quad (12), \quad (13), \quad (23).$$

Con más detalle: la permutación 1 es la *permutación identidad,* la dada por $a1 = a$, para todo a, la permutación (123) es el *ciclo* que envía el 1 al 2, el 2 al 3 y el 3 de vuelta al 1, mientras que la *transposición* (12) intercambia el 1 con el 2 y deja al 3 invariante.

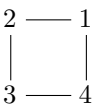
En estos términos, el grupo de Galois del polinomio ciclotómico quinto está formado por las cuatro permutaciones

$$\sigma_1 = 1, \quad \sigma_2 = (\omega, \omega^2, \omega^4, \omega^3), \quad \sigma_3 = (\omega, \omega^3, \omega^4, \omega^2), \quad \sigma_4 = (\omega, \omega^4)(\omega^2, \omega^3).$$

Galois intentó que su memoria sobre la teoría de las ecuaciones algebraicas fuera aceptada por la *Académie des Sciencies,* pero sin éxito. Su primer intento fue rechazado por Cauchy, aunque éste reconoció el valor de las ideas de Galois y en febrero 1830 le dijo que uniera dos de sus trabajos y los enviara al secretario de la Academia, Joseph Fourier. Sin embargo Fourier murió en mayo de ese mismo año, y la memoria de Galois se perdió. No obstante, Galois pudo publicar tres artículos ese año. En 1831 Siméon Denis Poisson declaró que los trabajos de Galois eran incomprensibles, de modo que era imposible juzgar su corrección, pero le sugirió que redactara una versión unificada de sus trabajos. Sin embargo, Galois murió en un duelo en 1832 con 20 años de edad, y sus trabajos permanecieron inéditos hasta que en 1843 Joseph Liouville reconoció su valor y se encargó de que fueran publicados, cosa que sucedió en 1846.

Grupos de permutaciones Aprovechamos las más de dos décadas que los trabajos de Galois permanecieron inéditos para hacer una digresión sobre los grupos de permutaciones, cuyo interés va mucho más allá de su aplicación al estudio de las raíces de las ecuaciones polinómicas.

Por ejemplo, consideremos el grupo de las permutaciones de los cuatro vértices de un cuadrado. Se trata del grupo Σ_4, pero, de entre todas ellas, sólo hay cuatro que pueden obtenerse girando el cuadrado:



$$1, \quad (1234), \quad (13)(24), \qquad (4321).$$

La identidad se obtiene con un giro de 0 grados, la segunda se obtiene girando el cuadrado 90° en sentido antihorario (lo que lleva el 1 al 2, el 2 al 3, etc.), la tercera se corresponde con un giro de 180° y la cuarta con un giro de 270° en sentido antihorario o de 90° en sentido horario.

Estas cuatro permutaciones forman un grupo, conocido como el grupo *cíclico* de orden 4, y que representaremos por C_4. En general, las permutaciones que se obtienen girando los vértices de un polígono regular de n lados forman un grupo que llamaremos C_n.

Pero si admitimos también la posibilidad de "voltear" el cuadrado, lo cual equivale a aplicarle simetrías axiales, podemos conseguir otras cuatro permutaciones más:

$$(12)(34), \qquad (14)(23), \qquad (24), \qquad (13).$$

La primera corresponde a la simetría respecto a la recta vertical que pasa por los puntos medios de los lados horizontales, la segunda a la simetría respecto a la recta análoga horizontal, y las dos últimas se obtienen con las simetrías respecto a las diagonales del cuadrado. Estas ocho permutaciones forman también un grupo. Más en general, el conjunto de las permutaciones de los vértices de un polígono regular de n lados que pueden obtenerse mediante movimientos y simetrías recibe el nombre de *grupo diédrico* de orden $2n$, y se representa por D_{2n}. Las ocho permutaciones que acabamos de enumerar forman, pues, el grupo D_8.

Igualmente podemos estudiar las permutaciones del conjunto de vértices de un poliedro que pueden obtenerse mediante movimientos. En el caso de un cubo, de las $8! = 40\,320$ permutaciones posibles, sólo 24 de ellas pueden obtenerse a partir de movimientos, y el grupo que forman resulta ser "esencialmente el mismo" que el grupo completo de permutaciones Σ_4. En cambio, veremos que, de las $12! = 479\,001\,600$ permutaciones posibles de los vértices de un icosaedro regular, sólo 60 son realizables mediante movimientos.

¿Y de qué sirve conocer los grupos de simetrías de los polígonos y los poliedros? Entre otras cosas, veremos que ello permite resolver problemas de combinatoria no triviales. Por ejemplo:

> *¿Cuántas pulseras distintas se pueden formar ensartando en un hilo circular seis cuentas de hasta cinco colores distintos?*

Aquí es esencial entender que dos pulseras se consideran la misma si se pueden superponer de modo que coincidan los colores de sus cuentas girándola o volteándola. Sucede que hay 1 505, pero no es trivial cómo llegar a este número. En la sección 2.7 resolveremos sistemáticamente este problema y otros similares a partir de un resultado conocido como *lema de Burnside* (teorema 2.39), si bien Burnside se limitó a incluirlo en un libro suyo de 1897 citando un trabajo de Ferdinand Georg Frobenius de 1887, pero Cauchy ya lo había demostrado en 1845. La aplicación del lema de Burnside al problema planteado requiere estudiar el grupo diédrico D_{12}.

Otro resultado combinatorio que puede probarse mediante el lema de Burnside es:

> *El número de formas distintas de pintar las caras de un cubo con k colores es*
> $$\frac{k^6 + 3k^4 + 12k^3 + 8k^2}{24}.$$

Para llegar a esta conclusión necesitamos estudiar el grupo de las simetrías de un cubo o, equivalentemente, el grupo de permutaciones Σ_4.

Grupos abstractos Para la época en la que fueron publicados los trabajos de Galois la teoría de grupos ya era una rama incipiente de la matemática, que había recibido el impulso de Cauchy o de Camille Jordan, que fue, de hecho, el que difundió el uso del término "grupo" para referirse a los grupos de permutaciones. Jordan introdujo también el concepto de "isomorfismo de grupos", que plasma el hecho de que dos grupos de permutaciones pueden ser, en esencia, "un mismo grupo", como sucede con Σ_4 y el grupo de las simetrías de un cubo.

Más precisamente, un *isomorfismo* entre dos grupos G y H es una biyección $f : G \longrightarrow H$ con la propiedad de que

$$f(g_1g_2) = f(g_1)f(g_2), \qquad \text{para todo } g_1, g_2 \in G.$$

Dos grupos se dicen *isomorfos* si existe un isomorfismo entre ellos, y ello se traduce en que son indistinguibles como grupos. Por ejemplo, el grupo de Galois del polinomio ciclotómico quinto es isomorfo al grupo C_4 de los giros de un cuadrado, pues si llamamos $a = \omega$ en el primero y $a = (1234)$ en el segundo, el producto en ambos grupos viene dado por la tabla

	1	a	a^2	a^3
1	1	a	a^2	a^3
a	a	a^2	a^3	1
a^2	a^2	a^3	1	a
a^3	a^3	1	a	a^2

de modo que si decimos, por ejemplo, que $a^4 = 1$, no podemos saber si estamos hablando de $a = \omega$ o de $a = (1234)$, pues la tabla es la misma para ambos grupos.

En 1854 Arthur Cayley[1] introdujo la noción abstracta de grupo que se usa actualmente, según la cual los elementos de un grupo no tienen por qué ser permutaciones, sino que un grupo es cualquier conjunto G dotado de una operación $\cdot : G \times G \longrightarrow G$ que satisfaga las propiedades siguientes:

1. $(ab)c = a(bc)$, para todos los elementos $a, b, c \in G$.
2. Existe $1 \in G$ tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in G$.
3. Para cada $a \in G$ existe $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

No se exige que la operación sea conmutativa, es decir, que $ab = ba$, para todo $a, b \in G$. Los grupos que tienen esta propiedad se llaman *grupos abelianos.*

Si un grupo G es finito, su número de elementos recibe el nombre de *orden* de G y se representa por $|G|$.

Ésta es la definición que dimos en la sección [ITAl 3.6] y de la que partiremos en el capítulo I de este libro, donde introduciremos el (rico) lenguaje y los resultados básicos de la teoría de grupos abstracta. En el capítulo II presentaremos los hechos básicos sobre grupos de permutaciones y en particular demostraremos el teorema de Cayley 2.26, según el cual, la definición abstracta de grupo no es realmente más general que el concepto clásico de "grupo de permutaciones", pues todo grupo G es isomorfo a un grupo de permutaciones sobre sí mismo.

En [ITAl 3.26] definimos un grupo cíclico como un grupo G cuyos elementos son todos potencias de un mismo elemento generador. Para cada número natural $n \geq 1$, existe salvo isomorfismo un único grupo cíclico C_n de orden n, de modo que el grupo de los giros de un polígono regular de n lados es simplemente un ejemplo de grupo cíclico de orden n.

[1] Con un total de 967 artículos publicados, Cayley es el tercer matemático más prolífico de la historia, sólo superado por Euler y Cauchy.

La teoría de Galois Pasamos finalmente a describir los resultados que había obtenido Galois sobre las ecuaciones polinómicas. Uno de los pilares de su teoría es lo que hoy se conoce como *teorema fundamental de la teoría de Galois* [Al 5.44], según el cual existe una correspondencia biunívoca entre los subgrupos H del grupo de Galois G de un polinomio y los subcuerpos L de su cuerpo de escisión K.

Explícitamente la correspondencia de Galois $H \leftrightarrow L$ asigna a cada subgrupo H el subcuerpo

$$F = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ para todo } \sigma \in H\}$$

y a cada subcuerpo L el subgrupo

$$H = \{\sigma \in G \mid \sigma(\alpha) = \alpha \text{ para todo } \alpha \in L\}.$$

Por ejemplo, si K es el cuerpo de escisión del polinomio ciclotómico quinto, sabemos que su grupo de Galois es cíclico de orden 4, generado por la conjugación $\sigma_2 = (\omega, \omega^2, \omega^4, \omega^3)$, y es fácil ver que G tiene exactamente tres subgrupos:

$$1 = \{1\}, \qquad H = \{1, (\omega, \omega^4)(\omega^2, \omega^3)\}, \qquad G,$$

por lo que el cuerpo ciclotómico K tiene exactamente tres subcuerpos:

$$1 \leftrightarrow \mathbb{Q}, \qquad H \leftrightarrow L, \qquad G \leftrightarrow K,$$

de los cuales, el único subcuerpo propio es el asociado a $H = \{1, \sigma_4\}$, que es

$$L = \{\alpha \in K \mid \sigma_4(\alpha) = \alpha\}.$$

Como todo elemento de K es de la forma

$$\alpha = a_4\omega^4 + a_3\omega^3 + a_2\omega^2 + a_1\omega$$

y

$$\sigma_4(\alpha) = a_4\omega + a_3\omega^2 + a_2\omega^3 + a_1\omega^4,$$

la igualdad $\sigma_4(\alpha) = \alpha$ equivale a que $a_1 = a_4 = a$, $a_2 = a_3 = b$, luego L está formado por los números ciclotómicos de la forma $a(\omega + \omega^4) + b(\omega^2 + \omega^3)$, con $a, b \in \mathbb{Q}$. En [ITAl 17.6] (véase la discusión precedente) identificamos este cuerpo L como $L = \mathbb{Q}(\sqrt{5})$, el cuerpo de los enteros ciclotómicos reales. El teorema [ITAl 17.7] prueba la correspondencia de Galois $1 \leftrightarrow \mathbb{Q}$, mientras que $G \leftrightarrow K$ es inmediato.

De este modo, la teoría de Galois permite considerar los cálculos específicos que hicimos en la sección [ITAl 17.3] como casos particulares de una teoría general que podemos aplicar sistemáticamente. En general, es mucho más fácil encontrar los subgrupos de un grupo finito dado que encontrar los subcuerpos de un cuerpo dado, pero la teoría de Galois hace que ambas cosas sean equivalentes.

Conviene señalar en este punto que si K es el cuerpo de escisión de un polinomio $p(x)$ y la correspondencia de Galois relaciona un subgrupo H del

grupo de Galois G de $p(x)$ con un subcuerpo L del cuerpo de escisión K, no es necesariamente cierto que L sea el cuerpo de escisión de algún otro polinomio. Galois llamó *cuerpos normales* a los cuerpos L que son el cuerpo de escisión de un polinomio $p(x) \in \mathbb{Q}[x]$, y *subgrupos normales* a los subgrupos H que se corresponden con los cuerpos normales, pero sucede que los subgrupos normales admiten una caracterización puramente algebraica, de modo que, dado un grupo abstracto G, tiene sentido distinguir cuáles de sus subgrupos son normales, sin necesidad de que G sea el grupo de Galois de ningún polinomio. La notación $N \trianglelefteq G$ se usa para expresar que N es un subgrupo normal de G.

Si comparamos un grupo G con un anillo (por simplicidad, conmutativo y unitario) A, los subgrupos normales de G representan un papel análogo al de los ideales de A. En particular, del mismo modo que tiene sentido calcular el anillo cociente A/I de un anillo A sobre un ideal I, también puede definirse el grupo cociente G/N de un grupo G sobre un subgrupo normal N. De hecho, un subgrupo N es normal si y sólo si cumple lo necesario para que pueda definirse un anillo cociente G/N de forma análoga a como se hace en un anillo.

A partir de la correspondencia que hoy lleva su nombre, Galois pudo dar una condición necesaria y suficiente sobre el grupo de Galois de un polinomio $p(x)$ para que sus raíces puedan expresarse a partir de sus coeficientes en términos de sumas, restas, productos, cocientes y extracción de raíces. Concretamente, esto sucede si y sólo si el grupo de Galois G es *resoluble,* lo cual significa que existe una cadena de subgrupos

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

tal que cada grupo cociente G_i/G_{i-1} es un grupo abeliano. Salvo por cierta cuestión técnica sobre raíces de la unidad que requiere ciertos ajustes y que no vamos a detallar aquí, esto equivale a la existencia de una cadena de cuerpos

$$\mathbb{Q} = L_n \subset \cdots \subset L_1 \subset L_0 = K,$$

donde el hecho de que los cocientes G_i/G_{i-1} sean abelianos se traduce en que el cuerpo L_{i-1} se obtiene de L_i añadiéndole una raíz n-sima de un elemento de L_i, por lo que todos los elementos de K (en particular las raíces de $p(x)$) pueden expresarse en términos de sumas, restas, productos, cocientes y extracción de raíces.

Tal y como señalamos en la introducción de [Al], en 1813 Abel probó que no existe una fórmula general para resolver una ecuación polinómica de grado $n \geq 5$ en términos de sumas, restas, productos, cocientes y extracción de raíces, es decir, que no hay fórmulas análogas a la conocida fórmula para resolver las ecuaciones de segundo grado ni a las fórmulas de Cardano-Ferrari para las ecuaciones de tercer y cuarto grado.

Sin embargo, Abel sólo demostró que no existe ninguna fórmula general, lo cual no excluía que las raíces de cualquier ecuación polinómica pudieran expresarse en términos de sus coeficientes mediante sumas, restas, productos, cocientes y extracción de raíces, pero con expresiones distintas en función de

cada polinomio, aunque no siguieran todas un mismo esquema general, como sucede con las ecuaciones de grado $2, 3, 4$.

En los términos que estamos considerando aquí, lo que demostró Abel fue que el grupo de Galois de un polinomio $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ con "coeficientes indeterminados" es todo el grupo de permutaciones Σ_n [Al 7.29], y Galois demostró que este grupo sólo es resoluble para $n \leq 4$. En cambio, un polinomio de grado $n \geq 5$ con coeficientes racionales puede tener un grupo de Galois mucho menor que Σ_n y ser resoluble por radicales. Por ejemplo, el grupo de Galois del polinomio ciclotómico séptimo

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

resulta ser cíclico de orden 6, por lo que es resoluble (ya que todo grupo abeliano es trivialmente resoluble) y ello se corresponde con que las raíces del polinomio son trivialmente expresables en términos de raíces, pues son precisamente las seis raíces séptimas de la unidad no triviales.

Abel murió en 1829, y la Académie des Sciencies le concedió póstumamente en 1830 —junto a Jacobi) el mismo premio que Galois había aspirado a ganar con la memoria que le rechazaron. Sin embargo, la teoría de Galois permite mostrar ejemplos explícitos de polinomios de grado ≥ 5 que no son resolubles por radicales. Por ejemplo, tras [Al 7.27] probaremos que la ecuación

$$x^5 - 4x + 2 = 0$$

no es resoluble por radicales, porque el grupo de Galois de su miembro izquierdo es Σ_5 que, como ya hemos señalado, no es resoluble.

Constructibilidad con regla y compás Los argumentos que relacionan la resolubilidad por radicales de una ecuación polinómica y la resolubilidad de su grupo de Galois se pueden adaptar —y simplificar— para obtener una caracterización algebraica de los números algebraicos constructibles con regla y compás [G 6.4]. En este caso no se obtiene una caracterización puramente en términos del grupo de Galois, pero, por ejemplo, si un polinomio tiene grupo de Galois de orden 2^n, entonces sus raíces son constructibles con regla y compás. Esto lo probaremos en [G 6.8], pero la prueba se basa en una propiedad no trivial sobre grupos que demostraremos en 3.6, a saber:

> *Todo grupo de orden potencia de primo tiene subgrupos de todos los órdenes que dividen al orden del grupo.*

Teoremas de estructura El resultado precedente es un ejemplo de cómo un "teorema de estructura", es decir, un teorema sobre qué podemos encontrar en un grupo con unas características dadas (en este caso, un grupo de orden potencia de primo) resulta ser un ingrediente esencial en la prueba de un hecho que en principio no está relacionado con la teoría de grupos (como es la constructibilidad de un número algebraico), pero que puede ser reformulado en términos de grupos.

Entre los teoremas más importantes de este tipo se encuentran los teoremas de Sylow, publicados en 1872 por el matemático noruego Peter Ludwig Sylow. Entre otras cosas, afirman lo siguiente:

> *Si un grupo G tiene orden $|G| = p^n m$, donde p es primo y $p \mid m$, entonces G tiene un subgrupo de orden p^n.*

Por ejemplo, combinando la teoría de Galois con este teorema de existencia y el teorema previo sobre existencia de subgrupos en grupos de orden primo es posible dar una demostración algebraica sencilla del teorema fundamental del álgebra [Al 5.50].

Dedicaremos el capítulo III a probar los principales teoremas de estructura sobre grupos finitos y en el capítulo IV estudiaremos los grupos resolubles, probando primeramente los hechos básicos, necesarios entre otras cosas para probar la relación con la resolubilidad de ecuaciones por radicales y la constructibilidad con regla y compás, y luego veremos que los grupos resolubles cumplen teoremas de estructura mucho más potentes que los válidos para grupos cualesquiera. Por ejemplo, en 1928 el matemático británico Philip Hall probó que los grupos resolubles satisfacen versiones fuertes de los teoremas de Sylow, como ésta:

> *Si un grupo resoluble G tiene orden $|G| = mn$, donde m y n son primos entre sí, entonces G tiene un subgrupo de orden m.*

En 1870 Kronecker demostró un teorema de estructura sobre grupos abelianos finitos que en realidad es más que eso, pues es un teorema de clasificación, que permite determinar cuántos grupos abelianos hay de un orden dado, junto con una descripción operativa de cada uno de ellos.

Para enunciarlo tenemos que observar primero que si G_1 y G_2 son grupos, el producto cartesiano $G_1 \times G_2$, formado por todos los pares (g_1, g_2) tales que $g_i \in G_i$, se convierte a su vez en un grupo con la operación dada por

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2').$$

Igualmente se puede calcular el producto de cualquier número finito de grupos dados. El teorema de clasificación de los grupos abelianos finitos (enunciado para una clase de grupos ligeramente más general en 3.4) afirma lo siguiente:

> *Todo grupo abeliano finito es isomorfo a un producto de grupos cíclicos, y la descomposición es única si exigimos que los factores tengan orden potencia de primo.*

Por ejemplo, existen, salvo isomorfismo, 3 grupos abelianos de orden 20, que son:

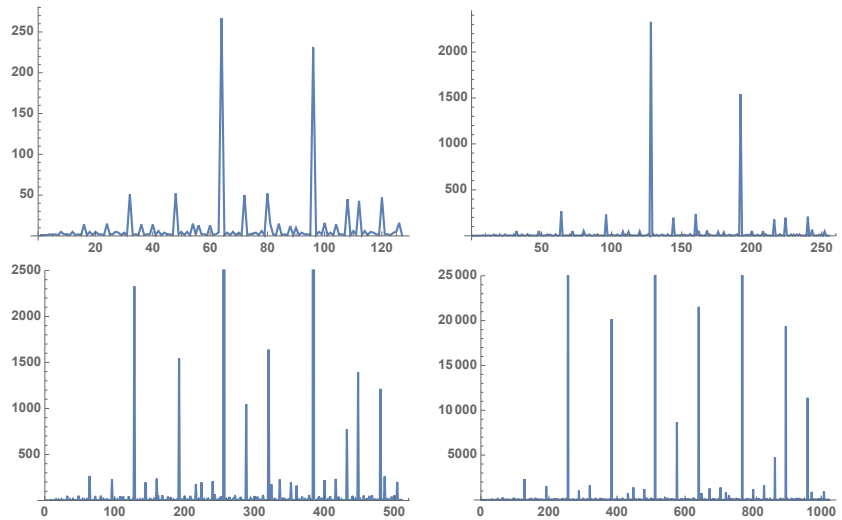
$$C_{20}, \qquad C_4 \times C_5, \qquad C_2 \times C_2 \times C_5.$$

No necesitamos incluir en la lista, por ejemplo, $C_2 \times C_{10}$, porque C_{10} es isomorfo a $C_2 \times C_5$, por lo que $C_2 \times C_{10}$ es isomorfo al tercer grupo de la lista. A partir de estas descomposiciones en producto es fácil responder cualquier pregunta sobre las características algebraicas de cualquiera de estos grupos, por lo que podemos afirmar que los grupos abelianos finitos se conocen perfectamente.

La situación es completamente distinta para los grupos finitos en general. No se conoce ningún criterio que permita determinar sistemáticamente (por un medio que no sea la mera enumeración explícita de todos los casos posibles, que es computacionalmente inviable a partir de cierta magnitud) cuántos grupos existen de un orden dado, junto con una descripción operativa de los mismos. Podemos probar, por ejemplo, que todo grupo de orde 6 es isomorfo a C_6 (es cíclico) o a D_6 (es diédrico) según si es abeliano o no, y del mismo modo podemos clasificar todos los grupos de distintos órdenes, pero los argumentos que hay que emplear y la familia de grupos obtenidos son diferentes en cada caso y no siguen un patrón general. Es posible encontrar algunos patrones particulares. Por ejemplo, en 1.39 probaremos que todo grupo de orden $2p$, con p primo es necesariamente isomorfo a C_{2p} o a D_{2p}, pero con esta clase de resultados sólo abarcamos algunas familias infinitas de órdenes posibles que no cubren, ni mucho menos, todos los casos posibles.

En el capítulo 3 llegaremos a clasificar todos los grupos finitos de orden menor que 32. No es casual que nos hayamos detenido precisamente en dicho orden, porque, como muestra la tabla 3.1, el mayor número de grupos de un orden n dado menor que 32 se alcanza con $n = 24$, con un total de 15 grupos, mientras que para $n = 32$ el número de grupos distintos resulta ser de 51, con lo que su clasificación se vuelve inevitablemente muy laboriosa.

En general, los órdenes con un mayor número de grupos son las potencias de 2 en el sentido de que, por ejemplo, la primera de las gráficas siguientes muestra el número $N(n)$ de grupos de orden $n < 128$, que tiene picos en los valores $N(2^6) = 267$ y $N(2^5 \cdot 3) = 231$, mientras que $N(2^7) = 2\,328$.



La segunda gráfica muestra el número de grupos para $n < 256 = 2^8$, que tiene otro pico en $N(2^6 \cdot 3) = 1\,543$, pero $N(2^8) = 56\,092$. La tercera gráfica llega hasta $511 = 2^9 - 1$, y sólo dos valores quedan fuera del rango representado, $N(2^8) = 56\,092$ y $N(2^7 \cdot 3) = 20\,169$, pero $N(2^9) = 10\,494\,213$. Por último, la

cuarta gráfica llega hasta $1\,023 = 2^{10} - 1$ y sólo tres valores quedan fuera del rango representado:

$$N(2^8) = 56\,092, \qquad N(2^9) = 10\,494\,213, \qquad N(2^8 \cdot 3) = 1\,090\,235,$$

mientras que $N(2^{10}) = 49\,487\,365\,422$. El número total de grupos de orden menor o igual que $1\,024$ es $49\,499\,125\,314$, por lo que los grupos de orden 2^{10} constituyen el 99.97% del total.

Similarmente, los grupos de orden $64 = 2^6$ constituyen el 45.56% de los grupos hasta ese orden, los de orden $128 = 2^7$ constituyen el 64.73% y los de orden $256 = 2^8$ constituyen el 88.89%.

Si llamamos $N(n)$ al número de grupos de orden n no isomorfos dos a dos, es posible estudiar el comportamiento asintótico de la función $N(n)$ sin necesidad de calcular su valor exacto. Así, en 5.60 probaremos la desigualdad

$$p^{\frac{2}{27}n^3 - \frac{4}{9}n^2} \leq N(p^n).$$

Más aún, puede probarse[2] que el número de grupos de orden p^n cumple

$$p^{\frac{2}{27}n^3 - \frac{4}{9}n^2} \leq N(p^n) \leq p^{\frac{2}{27}n^3 + O(n^{5/2})}.$$

En otras palabras, si expresamos $N(p^n) = p^{E_p(n)}$, el exponente cumple

$$E_2^-(n) = \frac{2}{27}n^3 - \frac{4}{9}n^2 \leq E_p(n) \leq \frac{2}{27}n^3 + O(n^{5/2}),$$

de modo que

$$\frac{E_p(n) - E_2^-(n)}{E_p(n)} \leq \frac{\frac{4}{9}n^2 + O(n^{5/2})}{\frac{2}{27}n^3 - \frac{4}{9}n^2} \to 0,$$

es decir, que el error relativo de la aproximación de $E_p(n)$ por la función $E_2^-(n)$ tiende a 0 a medida que n crece. (Lo mismo vale si aproximamos $E_p(n)$ por $(2/27)n^3$, aunque entonces la aproximación ya no es una cota inferior.) Esto significa que crecimiento asintótico es cúbico y que el coeficiente $2/27$ en la aproximación que probaremos es exacto.

La tabla siguiente compara la aproximación que hemos obtenido con los valores reales. Por desgracia, no se conoce el valor exacto de $N(2^{11})$, por lo que sólo podemos comparar cuatro valores, una cantidad muy pequeña para que podamos hacernos una idea de la calidad de la aproximación cuando n aumenta. Vemos que el porcentaje de error en la aproximación del exponente va decreciendo hasta el 16.6% en el caso de 2^{10}. Para 2^{11} hemos probado que hay al menos casi 31 billones de grupos de dicho orden, y si extrapolamos la tendencia con la que se va reduciendo el porcentaje de error en el exponente, éste debería ser del orden del 11.52%. Con ese error, el número de grupos podría exceder los 11 000 billones.

[2] Véase Blackburn, S., Neumann, P., y Venkataraman, G. (2007). *Enumeration of Finite Groups* Cambridge University Press.

n	$N(2^n)$	$2^{E_2^-(n)}$	$E_2(n)$	$E_2^-(n)$	%
1	1	–	0	–	–
2	2	–	1	–	–
3	5	–	2.32	–	–
4	14	–	3.81	–	–
5	51	–	5.67	–	–
6	267	–	8.06	–	–
7	2 328	12.37	11.18	3.63	67.5
8	56 092	714.84	15.78	9.48	39.9
9	10 494 213	262 144	23.32	18.00	22.8
10	49 487 365 422	830 629 361.9	35.53	29.63	16.6
11	?	30 945 927 902 369.45	?	44.81	–

Antes hemos dicho que si comparamos los grupos con los anillos (conmutativos y unitarios), entonces los subgrupos normales son los análogos a los ideales y, según esta analogía, los grupos simples son el concepto análogo al de los anillos que no tienen ideales propios, que son precisamente los cuerpos. Del mismo modo que los cuerpos forman una clase muy particular de anillos, con propiedades muy diferentes a las de los anillos arbitrarios, los grupos simples también son una clase muy particular de grupos.

Los grupos que son simples y resolubles a la vez coinciden con los que son simples y abelianos a la vez, que resultan ser los grupos cíclicos de orden primo (o simplemente los grupos de orden primo, pues éstos son necesariamente cíclicos). Al margen de este punto de encuentro, los grupos simples no abelianos pueden pensarse como una clase radicalmente opuesta a la de los grupos resolubles. No es cierto que ser simple no abeliano equivalga a no ser resoluble, ni viceversa, pero sí que es cierto que un grupo que tenga un subgrupo o un cociente simple no abeliano no puede ser resoluble, y que un grupo resoluble no puede ser simple no abeliano.

Fue el propio Galois el que introdujo el concepto de grupo simple, precisamente para demostrar que los grupos de permutaciones Σ_n no son resolubles cuando $n \geq 5$. En efecto, aunque no son grupos simples, en 1831 Galois demostró que Σ_n posee un único subgrupo de orden $n!/2$, que recibe el nombre de *grupo alternado* A_n, y probó que A_n es un grupo simple no abeliano siempre que $n \geq 5$ (teorema 2.22).

Existen muchos teoremas que permiten probar que "la mayoría" de los grupos finitos son resolubles, y cada vez que extendemos el alcance de la clase de los grupos resolubles estamos restringiendo las posibilidades para que un grupo sea simple no abeliano. Y así resulta que los grupos simples no abelianos finitos son objetos muy raros, en el sentido de que se dan con poca frecuencia. Por ejemplo, el grupo alternado A_5, de orden 60, resulta ser el único grupo simple no abeliano de orden menor o igual que 100, y sólo hay cinco grupos simples no abelianos de orden menor o igual que 1 000 y un total de 31 de orden menor o igual que 100 000.

En una carta fechada el 29 de mayo de 1832, dos días antes de su muerte, Galois presentó otra familia infinita de grupos finitos simples no abelianos. Se trataba de los que actualmente se conocen como *grupos lineales especiales proyectivos* $\mathrm{LEP}(2,p)$, donde $p \geq 5$ es un número primo. Se trata de grupos construidos a partir de grupos de matrices 2×2 con coeficientes en el cuerpo de p elementos.

Así pues, en tiempos de Galois se conocían dos familias infinitas de grupos simples finitos no abelianos (más la familia de los grupos cíclicos de orden primo, que son los grupos simples abelianos). En 1861 el matemático francés Émile Léonard Mathieu encontró dos grupos simples, los que ahora se conocen como M_{11} y M_{12}, de órdenes respectivos 7 920 y 95 040 y esbozó la posibilidad de construir otro más, que ahora se conoce como M_{24}.

En 1870 Camille Jordan presentó cuatro familias infinitas de grupos simples finitos no abelianos, construidas a partir de grupos de matrices $n \times n$ sobre el cuerpo de p elementos, una de las cuales era la clase de los grupos $\mathrm{LEP}(n,p)$, que extendía a la encontrada por Galois. Estas cuatro familias, generalizadas para admitir cuerpos finitos arbitrarios, no necesariamente de cardinal primo, constituyen los llamados grupos simples clásicos. La familia de los grupos $\mathrm{LEP}(n,q)$ (donde q es el número de elementos de un cuerpo finito) la estudiaremos en la sección 7.2, donde veremos que todos son simples salvo $\mathrm{LEP}(2,2)$ y $\mathrm{LEP}(2,3)$. Las otras tres familias las estudiaremos en los capítulos VIII y 9, donde veremos que también son grupos simples salvo en unos pocos casos excepcionales.

En 1873 Mathieu describió con más detalle el grupo M_{24}, cuyo orden es 244 823 040, y encontró otros dos grupos simples más, M_{22} y M_{23}, de órdenes 443 520 y 10 200 960, respectivamente, que completan los que ahora se conocen como los cinco grupos de Mathieu. Estudiaremos estos grupos en la sección 7.3.

En 1897 William Burnside publicó un libro de texto clásico de la teoría de grupos, titulado *La teoría de grupos de orden finito,* en el que llamó *grupos simples esporádicos* a los grupos de Mathieu, porque tenían la peculiaridad de que su construcción, al contrario de las demás construcciones conocidas, no permitía obtener una familia infinita de grupos simples, sino únicamente cinco.

En 1899 una matemática estadounidense, Ida May Schottenfels, probó que los grupos $\mathrm{LEP}(4,2)$ y A_8 no son isomorfos (teorema 7.43), a pesar de que ambos tienen 20 160 elementos. Fue el primer caso conocido de dos grupos simples no isomorfos del mismo orden. En el capítulo 9 veremos que en realidad existen infinitos pares de grupos simples del mismo orden no isomorfos entre sí. El menor ejemplo, después del encontrado por Schottenfels, corresponde a dos grupos de 1 451 520 elementos.

En 1873 el matemático noruego Sophus Lie había iniciado las investigaciones que le llevarían a estudiar los llamados *grupos de Lie,* que son grupos dotados de una estructura de variedad diferenciable en el sentido que estudiaremos en el capítulo VII de [An] (en realidad en un sentido de variedad diferencial abstracta un poco más general). Por ejemplo, un grupo de Lie es grupo lineal general

$\mathrm{LG}(2,\mathbb{R})$, formado por todas las matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

de coeficientes reales y con determinante $ad - bc \neq 0$. Estas matrices se corresponden biunívocamente con los puntos del abierto

$$U = \{(a,b,c,d) \in \mathbb{R}^4 \mid ad - bc \neq 0\} \subset \mathbb{R}^4,$$

de modo que, a través de esta identificación, tanto el producto como la aplicación que a cada matriz le hace corresponder su inversa pueden verse como aplicaciones infinitamente derivables

$$U \times U \longrightarrow U, \qquad U \longrightarrow U,$$

y esto es precisamente lo que significa que $\mathrm{LG}(2,\mathbb{R})$ es un grupo de Lie.

El propósito de Lie era trasladar las ideas de Galois al contexto de la geometría diferencial con vistas a aplicarlas al estudio de las ecuaciones diferenciales. Hacia 1880, el matemático alemán Wilhelm Killing introdujo independientemente del trabajo de Lie las que ahora se conocen como álgebras de Lie, y hacia 1890 obtuvo una clasificación de las llamadas *álgebras de Lie simples* sobre el cuerpo $\mathbb{C}$ de los números complejos.

En 1901 el matemático estadounidense Leonard Eugene Dickson publicó su libro *Grupos lineales con una exposición de la teoría de cuerpos de Galois,* que es el primer texto en el que se estudian de forma sistemática los cuerpos finitos, y que además contenía una presentación sistemática de las cuatro clases de grupos simples estudiadas por Jordan, pero generalizadas para considerar matrices $n \times n$ sobre cuerpos finitos arbitrarios, no necesariamente con un número primo de elementos. Estas cuatro familias de grupos simples reciben ahora el nombre de *grupos simples clásicos.* Dickson tomo como guía de su trabajo la analogía con los resultados de Killing sustituyendo el cuerpo $\mathbb{C}$ de los números complejos por cuerpos finitos, y encontró otras dos familias infinitas de grupos simples finitos, a las que llamó "familias excepcionales".

De este modo, al principios del siglo XX los grupos simples finitos conocidos eran lo suficientemente numerosos como para que se pudieran formular conjeturas razonables sobre ellos y lo suficientemente escasos como para que no fuera descabellado plantearse si existían más o si ya se conocían todos.

Uno de los principales matemáticos que se dedicaron a "acotar" las posibilidades para los grupos simples no abelianos fue Burnside. Uno de sus resultados más notables lo obtuvo en 1904, cuando probó el teorema siguiente:

> *Si el orden de un grupo finito G sólo es divisible entre dos primos, entonces G es resoluble.*

Aunque Burnside demostró muchos teoremas, éste en particular es el conocido simplemente como *teorema de Burnside.* Como consecuencia, el orden de un grupo simple no abeliano debe ser divisible al menos entre tres primos. La prueba de Burnside aplicaba la teoría de caracteres de grupos que había empezado a desarrollar en 1896 el matemático alemán Ferdinand Frobenius. En 1837 Dirichlet había demostrado su teorema sobre primos en progresiones aritméticas [ITAn 7.24] generalizando la noción de "carácter" introducida por Gauss al caso de grupos abelianos finitos, y ahora Frobenius la extendía a su vez de forma nada obvia al caso de grupos arbitrarios, no necesariamente abelianos. Esta teoría se desarrolló rápidamente en los años siguientes y Burnside se dio cuenta de su potencial, que quedó fuera de toda duda con la demostración de su resultado. En el capítulo VI expondremos los resultados básicos de la teoría de caracteres de grupos necesarios para demostrar el teorema de Burnside 6.40. Es posible demostrar el teorema sin recurrir a la teoría de caracteres, pero la prueba "elemental" es mucho más complicada y no se completó hasta 1972.

Incidentalmente, como una aplicación curiosa de la teoría de caracteres, probaremos esta caracterización de los grupos abelianos 6.41:

Si G es un grupo finito y

$$\frac{|\{(g,h) \in G \times G \mid gh = hg\}|}{|G|^2} > \frac{5}{8},$$

entonces G es abeliano.

En otras palabras, si la probabilidad de que dos elementos de un grupo finito elegidos al azar conmuten es mayor que 5/8, entonces el grupo es abeliano.

En 1911 Burnside publicó la segunda edición de su libro de 1897, en la que añadió la teoría de caracteres necesaria para demostrar el teorema de Burnside, así como una conjetura destacada:

Todo grupo de orden impar es resoluble.

De ella se sigue que todo grupo simple no abeliano tiene que tener orden par. Esto era especialmente relevante porque Burnside había advertido que una estrategia prometedora de cara a una posible clasiificación de los grupos simples era estudiar sus involuciones (sus elementos $g \neq 1$ tales que $g^2 = 1$), pero sólo los grupos de orden par tienen involuciones.

En 5.36 demostraremos que todo grupo de orden impar $\leq 1\,000$ es resoluble, y uno de los ingredientes esenciales de la prueba —además del teorema de Burnside— es el teorema del p-complemento normal 5.32, también de Burnside, que apareció por primera vez en la segunda edición de su libro y que es un tanto más técnico y más elemental en comparación con el anterior, pero también de una gran potencia.

En 1955 Brauer y Fowler demostraron un teorema según el cual sólo puede haber un número finito de grupos simples en los que el centralizador de una

involución (el subgrupo de elementos que conmutan con ella) fuera de un tipo dado. Esto sugería un camino concreto para clasificar los grupos simples finitos a través de sus involuciones, tal y como había sugerido Burnside, y daba más trascendencia a su conjetura de que todos los grupos simples tienen orden par.

En los últimos años, el francés Claude Chevalley había advertido que muchos resultados sobre grupos de Lie definidos sobre los números reales podían generalizarse a resultados análogos sobre *grupos algebraicos,* que son grupos definidos en el contexto de la geometría algebraica en lugar de la geometría diferencial, lo cual permitía sustituir el cuerpo $\mathbb{R}$ por un cuerpo arbitrario, en particular por un cuerpo finito, y así obtener sistemáticamente varias familias de grupos simples finitos que ahora se conocen conjuntamente como *grupos de Chevalley* o *grupos de tipo de Lie.* Concretamente, en 1955 Chevalley definió cuatro familias de grupos simples que coincidían con las cuatro familias de grupos clásicos excepto parte de una de ellas, así como otras cinco familias excepcionales que incluían las dos que había encontrado Dickson. En 1959 el matemático canadiense Robert Steinberg modificó la construcción de Chevalley para incluir los grupos clásicos restantes en dos nuevas familias y encontró dos familias excepcionales. En ese momento se conocían 13 familias de grupos simples y los 5 grupos esporádicos de Mathieu, aunque en 1960 el japonés Michio Suzuki encontraría una más y en 1962 el coreano-canadiense Rimhak Ree descubrió otras dos, con lo que se llegó a un total de 16.

En 1963 el austríaco Walter Feit y el estadounidense John Griggs Thompson publicaron un artículo de 255 páginas en el que demostraban la conjetura de Burnside, que desde entonces se conoce como el *teorema de Feit-Thompson,* y que se considera el primer paso hacia una clasificación de los grupos simples finitos.

En 1965 el yugoslavo Zvonimir Janko sorprendió a la comunidad matemática con el descubrimiento de un nuevo grupo simple esporádico, ahora conocido como J_1, de orden 175 560, a la vez que conjeturaba la existencia de otros dos, J_2 y J_3. Hasta entonces se conjeturaba que los grupos de Mathieu serían los únicos grupos simples esporádicos.[3] Durante los años siguientes aparecerían muchos más, hasta un total de 26. El último en ser descubierto fue el *grupo monstruo* M, cuya existencia había sido conjeturada en 1973 por el alemán Bernd Fisher y por el estadounidense Robert Griess y que demostrada finalmente por éste en 1980. Su orden es

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000.$$

En 1983 el estadounidense Daniel Gorenstein anunció que la clasificación de los grupos simples finitos se había completado, aunque posteriormente se encontraron dos lagunas en la prueba que no serían subsanadas hasta 2004 y 2008, respectivamente. El enunciado final del teorema de clasificación es el siguiente:

[3] El especialista en teoría de grupos Bertram Huppert dice en la introducción de su tratado *Endliche Gruppen* que sólo hay dos cosas que le sorprendieron en su vida: el descubrimiento del primer grupo de Janko y la caída del muro de Berlín.

> *Todo grupo simple finito es un grupo cíclico de orden primo C_p, un grupo alternado A_n con $n \geq 5$, uno de los grupos de las* 16 *familias de grupos de tipo de Lie o bien uno de los 26 grupos simples esporádicos.*

No hace falta aclarar que la prueba de este teorema excede con creces el nivel de este libro. Se estima que ocupa unas 10 000 páginas repartidas entre más de 500 artículos de más de un centenar de autores. No obstante, varios de los contenidos de este libro tienen relación con el teorema de clasificación, por lo que hemos considerado oportuno presentarlo en esta introducción.

La teoría de grupos y otras ramas de la matemática La estructura de grupo aparece en los contextos más diversos, desde la teoría de números hasta la física teórica, de tal suerte que no podemos dar aquí una perspectiva general del papel que representan los grupos en la matemática moderna. En [ITAl] tuvimos ocasión de constatar cómo algunos resultados aritméticos elementales, como los teoremas de Fermat o de Euler sobre congruencias, o los resultados de Gauss sobre raíces de la unidad, se entienden mejor y se demuestran más elegantemente en el contexto de la teoría de grupos, o que la teoría de Gauss sobre las formas cuadráticas binarias permite entender por qué formas cuadráticas distintas tienen un comportamiento muy diferente en cuanto a los números que representan o en cuanto a las ecuaciones diofánticas que determinan en términos de los grupos de clases y de géneros correspondientes a cada discriminante posible.

Del mismo modo en que uno no esperaría que encontrar las soluciones enteras de la ecuación

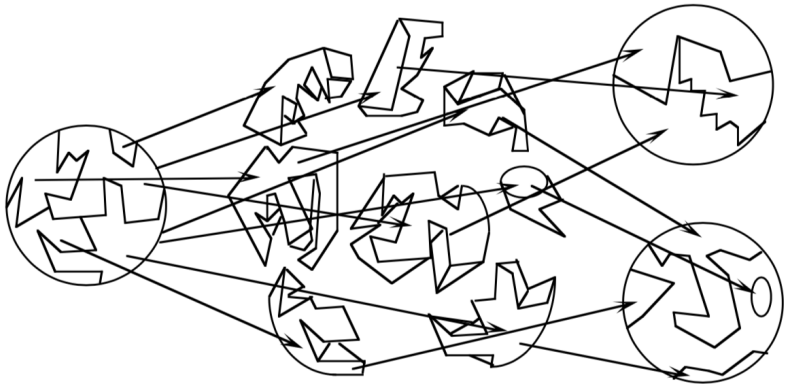
$$2x^2 + 22xy - 7y^2 = 77$$

—por poner uno de los ejemplos estudiados en [ITAl]— lleve al análisis de un grupo finito, hay muchos otros contextos en los que un problema sin relación aparente con la teoría de grupos conduce hasta ella.

A modo de ilustración, en el apéndice A presentamos dos resultados (uno a caballo entre la teoría de conjuntos y la geometría y otro relacionado con la teoría de la medida) en los que intervienen grupos de forma relevante y que vamos a describir a continuación:

La paradoja de Banach-Tarski En 1924 Stephan Banach y Alfred Tarski publicaron un artículo en el que demostraban lo siguiente:

> *Es posible partir una esfera sólida en un número finito de piezas de modo que, moviéndolas y ensamblándolas de nuevo, formen dos esferas del mismo radio que la de partida.*



La prueba es un refinamiento de la de un resultado de Hausdorff de 1914 que a su vez se basa en el hecho de que el grupo de los giros en el espacio tridimensional respecto a ejes que pasan por un mismo punto contiene un subgrupo libre[4] de rango 2. Los grupos libres los estudiaremos en la sección 3.2. Un grupo libre de rango 2 es un grupo L que contiene dos elementos σ, τ de modo que cada elemento de L distinto de 1 admite una expresión de tipo

$$\sigma\tau\sigma\sigma\tau\sigma^{-1}\tau\sigma\tau^{-1}\tau^{-1}\tau^{-1}\sigma$$

que es única sin más que exigir que en ella no aparezcan consecutivamente σ y σ^{-1} o bien τ y τ^{-1}.

Más aún, a partir de este resultado se puede probar fácilmente una versión mucho más general:

> *Si A, B son dos subconjuntos de $\mathbb{R}^3$ de interior no vacío, entonces A se puede descomponer en un número finito de trozos que, moviéndolos adecuadamente, pueden reensamblarse para formar B.*

Por ejemplo, una esfera de un centímetro de radio puede partirse en un número finito de trozos que, debidamente reensamblados, pueden formar una esfera del tamaño de la Tierra.

Estos resultados se conocen como *paradoja de Banach-Tarski,* pero no porque sean falsos o contradictorios, sino meramente porque a primera vista uno pensaría que tienen que ser falsos. Incluso uno puede sentirse tentado de razonar que son falsos argumentando así:

> Si partimos una esfera en un número finito de trozos, el volumen de la esfera será la suma de los volúmenes de los trozos, y éstos volúmenes no se alteran al moverlos, por lo que el volumen de las dos esferas también tiene que ser igual a la suma de los volúmenes de los trozos, y así llegamos a la contradicción de que un número no nulo es igual a su doble.

[4]En realidad Hausdorff encontró lo que se conoce como el producto libre de C_2 y C_3, pero la prueba se simplifica si aprovechamos que el grupo de giros contiene también un grupo libre.

Lo que falla en el "razonamiento" anterior es un hecho muy sutil: los trozos en los que se divide la esfera para duplicarla ¡no tienen volumen! En el apéndice A de [ITAn] definimos el área de una figura plana a través de la medida de Jordan, que no está definida sobre todos los subconjuntos de $\mathbb{R}^2$, sino únicamente sobre los del anillo de los conjuntos medibles Jordan. En el capítulo IV de [An] generalizaremos la medida de Jordan a $\mathbb{R}^n$ y a su vez la extenderemos a la medida de Lebesgue, que tampoco está definida sobre todos los subconjuntos de $\mathbb{R}^n$, sino únicamente sobre la σ-álgebra de los conjuntos medibles Lebesgue.

Lo que prueba el razonamiento precedente es que los fragmentos en los que se divide la esfera en la paradoja de Banach-Tarski no pueden ser medibles Lebesgue, pues la medida de Lebesgue es invariante por movimientos, luego si fueran medibles el razonamiento sería aplicable y llegaríamos a una contradicción.

Equivalentemente, lo que prueba la paradoja de Banach-Tarski es que no es posible extender la medida de Lebesgue en $\mathbb{R}^3$ a una medida definida sobre todos los subconjuntos de $\mathbb{R}^3$ y que siga siendo invariante por movimientos. En otras palabras, hay subconjuntos de $\mathbb{R}^3$ a los que no es posible asignarles un volumen de forma coherente con las condiciones que cabe esperar que cumpla el concepto de volumen (como la de ser invariante por movimientos).

Medidas finitamente aditivas La paradoja de Banach-Tarski puede probarse sin cambios esenciales para cualquier $\mathbb{R}^n$ con $n \geq 3$. Sin embargo, no se cumple en dos dimensiones, es decir, no es posible partir un círculo en un número finito de trozos que, debidamente reordenados, formen dos círculos del mismo radio. Y del mismo modo que la teoría de grupos interviene en la construcción de la partición de la esfera tridimensional, también interviene en la demostración de que no puede darse una partición análoga de un círculo.

En efecto, en el apéndice A demostraremos también que es posible extender la medida de Lebesgue a una medida finitamente aditiva [ITAn A.5] sobre todos los subconjuntos de $\mathbb{R}^2$ que sea invariante por movimientos, y una de las claves para ello será que el grupo de los movimientos en $\mathbb{R}^2$ es resoluble.

Así, entendiendo por "volumen" el valor que proporciona una tal medida, el argumento con el que antes hemos tratado de refutar la paradoja de Banach-Tarski sí que es aplicable en $\mathbb{R}^2$, y demuestra que la paradoja no tiene un análogo bidimensional.

La teoría de grupos finitos La mayor parte de los grupos que vamos a estudiar en este libro son grupos finitos. Conviene pensar en la teoría de grupos finitos como una especie de "teoría de números abstracta" en el sentido siguiente: es indudable que los números aparecen en prácticamente todas las ramas de la matemática y que cualquier dato sobre su comportamiento puede tener aplicaciones en contextos diversos, pero no es menos cierto que las propiedades de los números que estudia la teoría de números no se eligen pensando en sus posibles aplicaciones, sino que su interés radica más frecuentemente en la curiosidad por encontrar un razonamiento que justifique un comportamiento que se puede conjeturar de forma natural al observar un número suficiente de casos particulares, o bien porque algunos enunciados muy simples de formular requieren teorías sofisticadas para ser justificados. Lo mismo sucede con la teoría de grupos finitos.

Los grupos finitos son como los números: es fácil encontrarlos en los contextos más diversos, pero su estudio no está motivado tanto por sus posibles aplicaciones como porque plantean problemas de la misma naturaleza que los que aborda la teoría de números. No hay mucha diferencia conceptual entre el problema de encontrar las soluciones de una ecuación diofántica o encontrar todos los grupos de un orden dado; clasificar todos los grupos simples finitos es un reto de la misma naturaleza que el de demostrar el Último Teorema de Fermat; probar que todo primo congruente con 1 módulo 4 es suma de dos cuadrados es un problema análogo al de probar que todo grupo de orden p^2 (con p primo) es abeliano, etc. En ambos casos tenemos unos objetos (los números enteros o los grupos finitos) con una definición muy simple que, no obstante, permite plantear problemas muy variados que pueden resolverse con técnicas de niveles muy variados, y que a menudo tienen soluciones sorprendentes en algún sentido.

Terminamos esta introducción con un ejemplo del tipo de curiosidades que plantea la teoría de grupos finitos y cuyo planteamiento puede considerarse tan "elemental" como el de cualquier problema de la teoría de números para todo aquel que se haya familiarizado con los conceptos elementales de la teoría:

Si G es un grupo, podemos considerar el grupo $\mathrm{Aut}(G)$ de todos sus automorfismos (los isomorfismos de G en sí mismo). Calcular el grupo de automorfismos de un grupo dado es un ejercicio interesante de por sí, pero la situación es especialmente curiosa en el caso de los grupos de permutaciones Σ_n. Puede probarse que existe un isomorfismo natural muy sencillo entre $\mathrm{Aut}(\Sigma_n)$ y el propio grupo grupo Σ_n para todo valor de n salvo dos excepciones: $n = 2, 6$. El caso $n = 2$ no tiene nada de sorprendente, pues Σ_2 no es sino el grupo cíclico C_2 y es obvio que no puede tener más que el automorfismo trivial (la identidad). En cambio, $\mathrm{Aut}(\Sigma_6)$ es un grupo de orden $2 \cdot 6! = 1\,440$, que contiene un subgrupo isomorfo a Σ_6, de modo que, además de los $6! = 720$ automorfismos de Σ_6 que cabría esperar, excepcionalmente hay otros 720 más, que en realidad suponen un único automorfismo excepcional τ, ya que los otros pueden verse como los productos $\tau\sigma$, donde σ recorre los automorfismos "usuales". Todo esto lo probaremos en la sección 2.5, pero, aun viendo la demostración, no deja de ser un misterio que Σ_6 admita más automorfismos que el resto de los grupos de "su familia".

Invitamos al lector a que se interese por los resultados expuestos en este libro con el mismo espíritu que le puede llevar a interesarse por cualquier resultado de la teoría de números: una vez esté familiarizado con los conceptos básicos expuestos en el capítulo I y los equipare a los conceptos básicos de la aritmética, podrá ver buena parte de los enunciados sobre grupos (especialmente sobre grupos finitos) como problemas "elementales" en cuanto a su planteamiento, cuya solución puede variar entre un argumento sencillo, un razonamiento más o menos sofisticado, o un razonamiento que requiere, pese a la simplicidad del enunciado, de técnicas matemáticas abstractas más o menos complejas, según el caso, que en ocasiones requieren miles de páginas y quedan sólo al alcance de los especialistas.

Capítulo I

Elementos de la teoría de grupos

En este primer capítulo presentaremos los conceptos y resultados básicos de la teoría de grupos, análogos a los que hemos presentado sobre anillos en los capítulos II y III de [Al]. El concepto de grupo lo introdujimos en la sección [ITAl 3.6], donde vimos que algunos resultados sobre los grupos U_n de las unidades de los anillos $\mathbb{Z}_n$ se entienden mejor si se enuncian y se demuestran en términos de la teoría de grupos. Posteriormente encontramos distintos contextos en los que grupos de diversa naturaleza aparecen en la teoría de números.

1.1 Grupos

Conceptualmente, un grupo no es más que un conjunto en el que hay definida una operación que cumple unas propiedades básicas. Si el conjunto es finito, su estructura de grupo viene determinada por una tabla. Por ejemplo, el grupo U_8 de las unidades de $\mathbb{Z}_8$ viene determinado por la tabla siguiente:

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Por ejemplo, $5 \cdot 3 = 15 \equiv 7$ (mód 8).

La definición de grupo que vamos a dar a continuación formaliza esta idea en el seno del lenguaje conjuntista y especifica las propiedades que debe cumplir una operación para definir un grupo:

Definición 1.1 Un *grupo* es un par ordenado $(G, \cdot)$, donde G es un conjunto y $\cdot : G \times G \longrightarrow G$ es una ley de composición interna en G que cumpla las propiedades siguientes:

1. $g_1(g_2g_3) = (g_1g_2)g_3$, para todo $g_1, g_2, g_3 \in G$ (propiedad asociativa).
2. Existe un $1 \in G$ tal que $g \cdot 1 = 1 \cdot g = g$ para todo $g \in G$ (existencia de elemento neutro).
3. Para todo $g \in G$ existe $g^{-1} \in G$ tal que $gg^{-1} = g^{-1}g = 1$ (existencia de opuesto).

   El grupo G se dice *abeliano* si además cumple:

4. $g_1g_2 = g_2g_1$, para todo $g_1, g_2 \in G$ (propiedad conmutativa).

En la práctica escribiremos simplemente G en lugar de $(G, \cdot)$. Si G es un conjunto finito, su número de elementos se llama *orden* del grupo y se representa por $|G|$.

He aquí algunas observaciones elementales sobre grupos:

- Hemos dado la definición con notación multiplicativa, pero en el caso de los grupos abelianos es frecuente usar también la notación aditiva (véase la definición [Al 2.2]), con la cual la operación se representa por $g_1 + g_2$, el elemento neutro se representa por 0 y el elemento opuesto se representa por $-g$.

- En la sección 2.6 de [Al] se justifica que la propiedad asociativa nos permite escribir expresiones como $g_1 \cdots g_n$ sin necesidad de poner paréntesis que especifiquen en qué orden deben asociarse los factores, pues el resultado será el mismo siempre y cuando no se cambie su orden, es decir, que, por ejemplo,
$$g_1((g_2g_3)(g_4(g_5g_6))) = (g_1g_2)((g_3(g_4g_5))g_6).$$
  Si el grupo es abeliano, además podemos desordenar los factores de cualquier modo sin alterar el resultado.

- Aunque el grupo no sea abeliano, hemos exigido en la definición que el elemento neutro conmute con todos los elementos del grupo, es decir, que sea a la vez neutro por la izquierda y por la derecha, y que cada elemento conmute con su opuesto. En realidad esto se cumple necesariamente. Si modificamos la definición de grupo exigiendo únicamente que el elemento neutro cumpla $g \cdot 1 = g$ y que los elementos opuestos cumplan $g \cdot g^{-1} = 1$, en realidad se cumple la definición que hemos dado. En efecto:
$$g^{-1}g = g^{-1}g \cdot 1 = g^{-1}gg^{-1}(g^{-1})^{-1} = g^{-1} \cdot 1 \cdot (g^{-1})^{-1} = g^{-1}(g^{-1})^{-1} = 1,$$
$$1 \cdot g = gg^{-1}g = g \cdot 1 = g.$$

- Otro hecho básico es que el elemento neutro es único (pues si hubiera dos, tendrían que cumplir $1 = 1 \cdot 1' = 1'$), y que cada elemento g del grupo tiene un único opuesto, pues si tuviera dos, digamos g^{-1} y $\bar{b}^{-1}$, tendrían que cumplir
$$g^{-1} = g^{-1} \cdot 1 = g^{-1} \cdot g \cdot \bar{g}^{-1} = \bar{g}^{-1}.$$

- Una relación básica al operar en un grupo es que $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$ (donde el cambio de orden es crucial si los elementos no conmutan), lo cual se justifica sin más que comprobar que $g_1g_2g_2^{-1}g_1^{-1} = 1$.
- Otro hecho elemental, pero útil, es que en un grupo el elemento neutro es el único que cumple $g \cdot g = g$, pues multiplicando por g^{-1} obtenemos $g = 1$.

Potencias Si G es un grupo y $g \in G$, podemos definir (con notación multiplicativa) las potencias

$$g^0 = 1, \qquad g^{n+1} = g^n \cdot g,$$

con lo que tenemos definido g^n para todo número natural n, y si n es un entero negativo definimos $g^n = (g^{-1})^{-n}$, con lo que g^n está definido para todo $n \in \mathbb{Z}$.

Comprobaciones rutinarias muestran que se cumplen las propiedades:

$$g^{m+n} = g^m g^n, \qquad (g^m)^n = g^{mn}, \qquad (g_1g_2)^m = g_1^m g_2^m \quad \text{si} \quad g_1g_2 = g_2g_1.$$

Con notación aditiva (para grupos abelianos) estas propiedades se expresan así:

$$(m+n)g = mg + ng, \quad n(mg) = (nm)g, \quad m(g_1 + g_2) = mg_1 + mg_2.$$

Primeros ejemplos Observemos que si $(A, +, \cdot)$ es cualquier anillo, entonces $(A, +)$ es un grupo abeliano. En particular, son grupos abelianos $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, etc. Los anillos de restos $\mathbb{Z}/n\mathbb{Z}$ son ejemplos de grupos abelianos finitos.

El conjunto $U(A)$ de las unidades de A (definición [Al 2.19]) es un grupo con el producto. En particular, si K es un cuerpo, entonces $K^* = K \setminus \{0\}$ es un grupo abeliano con el producto. El grupo de las unidades de $\mathbb{Z}$ es $\{\pm 1\}$, que es un grupo abeliano con dos elementos.

Al grupo de las unidades del anillo $\mathbb{Z}/n\mathbb{Z}$ lo llamaremos U_n. Según [Al 3.41], está formado por las clases $[m]$ de los números enteros que cumplen $(m, n) = 1$.

La función $\phi(n) = |U_n|$ se llama *función de Euler* (véase [ITAl 3.22] y la discusión posterior).

Estas tablas muestran la suma en el grupo $\mathbb{Z}/6\mathbb{Z}$ y el producto en U_7:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

En ellas observamos algunas características que no son casuales. Por ejemplo, que en todas las filas y columnas aparezca el elemento neutro expresa la

existencia de elemento simétrico; el hecho de que no se repitan elementos en ninguna fila o columna expresa que si $gh = gk$, necesariamente, $h = k$, como resulta de multiplicar la ecuación por g^{-1}, y el hecho de que en cada fila aparezcan todos los elementos del grupo se debe a que $g(g^{-1}h) = h$, luego siempre puede obtenerse cualquier elemento h multiplicando g por el elemento adecuado. Por último, el hecho de que las tablas sean simétricas respecto a la diagonal indica que los grupos son abelianos. ∎

Producto de grupos Una forma sencilla de construir nuevos grupos a partir de otros dados es mediante el producto cartesiano:

Definición 1.2 Si $G_1, \ldots, G_n$ son grupos, podemos dotar de estructura de grupo al producto $G_1 \times \cdots \times G_n$ mediante la operación

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n).$$

El lector puede comprobar que, en efecto, esta operación cumple la definición de grupo, de modo que el elemento neutro es $1 = (1, \ldots, 1)$ y los inversos se calculan mediante $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$. También es obvio que un producto de grupos es abeliano si y sólo si todos los factores lo son.

Por ejemplo, el grupo $V_4 = \{\pm 1\} \times \{\pm 1\}$ recibe el nombre de *grupo de Klein*. He aquí su tabla:

	$(1, 1)$	$(-1, 1)$	$(1, -1)$	$(-1, -1)$
$(1, 1)$	$(1, 1)$	$(-1, 1)$	$(1, -1)$	$(-1, -1)$
$(-1, 1)$	$(-1, 1)$	$(1, 1)$	$(-1, -1)$	$(1, -1)$
$(1, -1)$	$(1, -1)$	$(-1, -1)$	$(1, 1)$	$(-1, 1)$
$(-1, -1)$	$(-1, -1)$	$(1, -1)$	$(-1, 1)$	$(1, 1)$

Grupos de permutaciones Si A es un conjunto no vacío, llamaremos *grupo simétrico* de A al conjunto Σ_A de todas las aplicaciones $\sigma : A \longrightarrow A$ biyectivas, que es un grupo con el producto determinado por la composición de aplicaciones, es decir, con el producto dado por $(\sigma\tau)(a) = \tau(\sigma(a))$. Los elementos de Σ_A se llaman *permutaciones* de A.

El elemento neutro es la aplicación identidad, dada por $1(a) = a$, y el elemento opuesto de una permutación σ es su inversa como función σ^{-1}, es decir, la permutación que cumple $\sigma^{-1}(a) = b$ si y sólo si $\sigma(b) = a$.

El grupo simétrico del conjunto $I_n = \{1, 2, \ldots, n\}$ se representa simplemente por Σ_n, y nos referiremos a él como el grupo de las permutaciones de n elementos. Según hemos visto en [Al 1.38] su orden es $n!$

Por ejemplo, el grupo Σ_3 consta de las seis permutaciones siguientes, donde la notación que usamos indica que la permutación asigna a cada elemento de la fila superior el que tiene debajo. Por ejemplo, $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$:

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

No hemos dado nombre a las tres últimas permutaciones porque podemos expresarlas en términos de las precedentes. Por ejemplo,

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

El cálculo consiste en observar que el primer factor transforma el 1 en el 2 y el segundo el 2 en el 3, luego el producto transforma el 1 en el 3. Similarmente, $2 \mapsto 3 \mapsto 1$ y $3 \mapsto 1 \mapsto 2$. Igualmente, el lector puede calcular:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Por lo tanto, se cumple que $\Sigma_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. La tabla del grupo es

$\cdot$	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
1	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	1	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	1	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	1	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	1	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	1

El lector puede calcular una a una las 36 entradas de la tabla, pero en realidad basta comprobar las relaciones

$$\sigma^3 = \tau^2 = 1, \quad \tau\sigma = \sigma^2\tau.$$

Sabiendo esto, podemos usar la última relación para poner todas las sigmas a la izquierda y todas las taus a la derecha, y luego usar las dos primeras relaciones para simplificar los productos de sigmas y de taus. Por ejemplo:

$$(\sigma^2\tau)(\sigma\tau) = \sigma^2\tau\sigma\tau = \sigma^2\sigma^2\tau\tau = \sigma^3\sigma = \sigma.$$

Observemos que $\sigma\tau \neq \tau\sigma$, por lo que Σ_3 es un ejemplo de grupo finito no abeliano. ∎

1.2 El orden de un elemento

La tabla siguiente contiene las potencias de la clase [3] en el grupo U_7:

n	0	1	2	3	4	5	6
3^n	1	3	2	6	4	5	1

A partir de $n = 6$ las potencias se repiten cícicamente: $3^7 = 3$, $3^8 = 2$, etc. En particular vemos que U_7 está formado por las 6 potencias distintas de 3, lo cual no era evidente. Estos hechos se entienden mejor en términos de algunos conceptos nuevos, el primero de los cuales es el siguiente:

Definición 1.3 Se dice que g tiene *orden finito* si existe un $m > 0$ tal que $g^m = 1$. En tal caso se define el *orden* de g como el menor número natural $m > 0$ que cumple esto, y se representa por $o(g)$. En caso contrario se dice que g tiene *orden infinito,* y se representa por $o(g) = \infty$. En particular, $o(1) = 1$.

Ejercicio: Probar que, en un producto, $o((g_1, \ldots, g_n)) = \text{mcm}(o(g_1), \ldots, o(g_n))$.

El teorema siguiente es [ITAl 3.19]:

Teorema 1.4 *Sea g un elemento de un grupo. Entonces:*

1. *Si $o(g) = d$, entonces $g^m = g^n$ si y sólo si $m \equiv n$ (mód d). En particular, $g^m = 1$ si y sólo si $d \mid m$.*
2. *Si $o(g) = \infty$, entonces $g^m = g^n$ si y sólo si $m = n$.*

Demostración: 1) Si $m = dc + r$, con $0 \leq r < d$, se cumple que

$$g^m = (g^d)^c g^r = g^r$$

y, como d es el menor natural no nulo tal que $g^d = 1$, se cumplirá $g^m = 1$ si y sólo si $r = 0$, es decir, si y sólo si $d \mid m$.

Más en general, se cumple $g^m = g^n$ si y sólo si $g^{m-n} = 1$, si y sólo si $d \mid m - n$, si y sólo si $m \equiv n$ (mód d).

2) Si $g^m = g^n$, con $n \leq m$, entonces $g^{m-n} = 1$, y tiene que ser $m - n = 0$ o, de lo contrario, el orden de g sería finito. ∎

Tal y como explicábamos en [ITAl], lo que expresa este teorema es que si un elemento tiene orden finito d, al calcular las potencias sucesivas de d obtenemos un ciclo en el que aparecen exactamente d elementos del grupo, empezando en $g^0 = 1$, y que vuelve a repetirse al llegar a $g^d = 1$. En cambio, si el orden es infinito, no hay potencias repetidas.

Ahora es claro que en un grupo finito todos los elementos tienen orden finito, pues es imposible que un elemento tenga sus (infinitas) potencias distintas dos a dos.

El orden de la clase de un número entero n en el grupo de unidades U_m se llama *orden de n módulo m*, y se representa por $o_m(n)$.

En estos términos hemos visto que $o_7(3) = 6$. Las tablas siguientes contienen los órdenes de los elementos de $\mathbb{Z}/6\mathbb{Z}$ y de U_7, respectivamente:

n	0	1	2	3	4	5
$o(n)$	1	6	3	2	3	6

n	1	2	3	4	5	6
$o_7(n)$	1	3	6	3	6	2

He aquí la tabla correspondiente a U_{28}:

n	1	3	5	9	11	13	15	17	19	23	25	27
$o_{28}(n)$	1	6	6	3	6	2	2	6	6	6	3	2

En [ITAl 3.21] demostramos que el orden de cualquier elemento de un grupo abeliano finito divide al orden del grupo. En 1.21 demostraremos que esto es cierto también para grupos no abelianos. Los valores de las tablas anteriores pueden deducirse con muy pocos cálculos teniendo en cuenta el teorema siguiente:

Teorema 1.5 *Si g es un elemento de un grupo y $o(g) = n$, entonces*

$$o(g^m) = \frac{n}{(m,n)}.$$

DEMOSTRACIÓN: Llamemos $d = (m,n)$. Entonces

$$(g^m)^{n/d} = g^{mn/d} = (g^n)^{m/d} = 1^{m/d} = 1,$$

lo que implica que $o(g^m) \mid n/d$. Por otro lado, si $k = o(g^m)$, tenemos que $(g^m)^k = 1$, luego $n \mid mk$, luego $n/d \mid (m/d)k$, luego $n/d \mid k = o(g^m)$, por lo que tiene que ser $o(g^m) = n/d$. ∎

Por ejemplo, en $\mathbb{Z}/6\mathbb{Z}$, como $o([1]) = 6$, tenemos que

$$o([4]) = o(4 \cdot [1]) = \frac{6}{(4,6)} = 3.$$

En U_7, una vez hemos comprobado que $o_7([3]) = 6$, tenemos igualmente que

$$o_7(4) = o_7(3^4) = \frac{6}{(4,6)} = 3.$$

Otra propiedad básica de los órdenes es la siguiente [ITAl 3.27]:

Teorema 1.6 *Sean g_1, g_2 elementos de un grupo con órdenes finitos primos entre sí. Si además conmutan, se cumple que $o(g_1g_2) = o(g_1)o(g_2)$.*

DEMOSTRACIÓN: Sea $m = o(g_1)$, $n = o(g_2)$. El hecho de que g_1 y g_2 conmuten implica que $(g_1g_2)^{mn} = g_1^{mn}g_2^{mn} = 1 \cdot 1 = 1$, luego $o(g_1g_2) \mid mn$.

Si $(g_1g_2)^k = 1$, entonces $g_1^k = g_2^{-k} = h$, luego por el teorema anterior $o(h) \mid m$ y $o(h) \mid n$. Como m y n son primos entre sí, concluimos que $o(h) = 1$, es decir, que $g_1^k = g_2^k = 1$, luego $m \mid k$ y $n \mid k$, luego $mn \mid k$. Esto prueba que el orden de g_1g_2 es exactamente mn. ∎

Las hipótesis del teorema son necesarias. Por ejemplo, en cualquier grupo, si $o(g) = n > 1$, entonces $o(g^{-1}) = n$, pero $o(gg^{-1}) = o(1) = 1 \neq n$. Un caso menos trivial lo podemos ver en U_{20}, donde $o_{20}(3) = o_{20}(13) = 4$, mientras que su producto es $3 \cdot 13 = 19$ y $o_{20}(19) = 2$.

El teorema también es falso en general si los elementos no conmutan. Por ejemplo, la tabla siguiente muestra los órdenes de las permutaciones de Σ_3:

g	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
$o(g)$	1	3	3	2	2	2

Por ejemplo, $o(\sigma\tau) = o(\tau) = 2$, mientras que $o(\sigma\tau\tau) = o(\sigma) = 3$.

Veamos un último hecho sobre órdenes:

Teorema 1.7 *Si los elementos no triviales de un grupo tienen todos orden* 2*, el grupo es abeliano.*

DEMOSTRACIÓN: Supongamos que G sólo tiene elementos no triviales de orden 2 y sean $a, b \in G$. Entonces $(ab)^2 = 1$, es decir, $abab = 1$. Multiplicando por a queda que $a^2bab = a$, es decir, $bab = a$, y multiplicando por b queda que $bab^2 = ab$, es decir, $ba = ab$, luego el grupo es abeliano. ∎

1.3 Homomorfismos de grupos

Introducimos ahora las aplicaciones que conservan la estructura de grupo:

Definición 1.8 Una aplicación $f : G \longrightarrow H$ entre dos grupos G y H es un *homomorfismo de grupos* si cumple $f(uv) = f(u)f(v)$ para todo $u, v \in G$.

La aplicación f es un *monomorfismo, epimorfismo* o *isomorfismo de grupos* si además es inyectiva, suprayectiva o biyectiva, respectivamente. Un isomorfismo de un grupo G en sí mismo es un *automorfismo* de G. Llamaremos $\operatorname{Aut} G$ al conjunto de todos los automorfismos de un grupo G.

Es fácil ver que la composición de homomorfismos de grupos es un homomorfismo y que la inversa de un isomorfismo de grupos es también un isomorfismo. En particular, resulta que $\operatorname{Aut} G$ es un grupo con la composición de aplicaciones.

Notemos que, en un grupo G, el elemento neutro es el único $g \in G$ que cumple $gg = g$. Como consecuencia, si $f : G \longrightarrow H$ es un homomorfismo de grupos, se cumple $f(g)f(g) = f(g)$, luego $f(1) = 1$. Además, como $f(g)f(g^{-1}) = f(1) = 1$, también se cumple que $f(g^{-1}) = f(g)^{-1}$.

Diremos que dos grupos G y H son *isomorfos* si existe un isomorfismo entre ellos, y lo representaremos por $G \cong H$. En tal caso G y H tienen las mismas propiedades definibles a partir de la estructura de grupo.

Ejemplo Las tablas de $\mathbb{Z}/6\mathbb{Z}$ y U_7 que hemos mostrado en la página 3 parecen muy distintas entre sí, pero esto es sólo una apariencia, ya que ambos grupos son isomorfos. Un isomorfismo $f : \mathbb{Z}/6\mathbb{Z} \longrightarrow U_7$ viene dado por $f([n]) = [3]^n$, es decir, por la tabla

$[n]$	0	1	2	3	4	5
$[3]^n$	1	3	2	6	4	5

En efecto, como $3 \in U_7$ tiene orden 6, el teorema 1.4 nos da que $[m] = [n]$ (en $\mathbb{Z}/6\mathbb{Z}$) si y sólo si $[3^m] = [3^n]$ (en U_7), por lo que f está bien definida (no depende del representante $[m]$ de la clase con el que se calcula la imagen). Hemos visto que es suprayectiva y, como ambos grupos tienen 6 elementos, tiene que ser también inyectiva.

Teniendo en cuenta que la notación en $\mathbb{Z}/6\mathbb{Z}$ es aditiva y en U_7 es multiplicativa, la condición para que f sea un homomorfismo es que

$$f([m] + [n]) = f([m])f([n])$$

o, explícitamente, que $[3]^{m+n} = [3]^m[3]^n$, lo cual es cierto.

Si escribiéramos las tablas de ambos grupos llamando $1, a, b, c, d, e$ a sus elementos, pero en el orden $0, 1, 2, 3, 4, 5$ en un caso y $1, 3, 2, 6, 4, 5$ en el otro, obtendríamos exactamente la misma tabla, de modo que no podríamos saber si corresponde a un grupo o al otro. Ésa es la "esencia" del concepto de isomorfismo: que si $f : G \longrightarrow H$ es un isomorfismo de grupos y damos el mismo nombre a cada elemento de G y a su imagen en H, es imposible saber si estamos operando en un grupo o en el otro.

Desde un punto de vista algebraico, $\mathbb{Z}/6\mathbb{Z}$ y U_7 son "el mismo grupo", y ambos tienen exactamente las mismas propiedades. Por ejemplo, hemos visto que ambos tienen dos elementos de orden 6, dos de orden 3 y uno de orden 2 (y podemos comprobar que estos elementos se corresponden por el isomorfismo que hemos definido). ∎

El grupo de Klein Tras la definición 1.2 hemos introducido el grupo de Klein como el producto $\{\pm 1\} \times \{\pm 1\}$ y hemos construido su tabla. En ella podemos observar que todos sus elementos cumplen $x^2 = 1$, es decir, que todos (salvo el neutro) tienen orden 2.

Supongamos en general que $V = \{1, a, b, c\}$ es un grupo de orden 4 cuyos elementos no triviales tienen todos orden 2. Esto significa que $a^2 = b^2 = c^2 = 1$. Además, $ab \neq 1$ (pues en caso contrario sería $a = b$), $ab \neq a$ (pues sería $b = 1$) y $ab \neq b$ (pues sería $a = 1$), luego necesariamente $ab = c$, e igualmente tiene que ser $ba = c$. En general, el producto de dos elementos no triviales de V es necesariamente el tercer elemento no trivial, luego la tabla de V es necesariamente ésta:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Es evidente que esta tabla define una operación con elemento neutro y respecto a la que todo elemento tiene un opuesto. Que sea asociativa es consecuencia de que no es ni más ni menos que la tabla del grupo de Klein (con otros nombres para sus elementos), y ya sabemos que el grupo de Klein es realmente un grupo. Esto se traduce en el teorema siguiente:

Teorema 1.9 *Todo grupo de orden* 4 *cuyos elementos no triviales sean de orden* 2 *es isomorfo al grupo de Klein* V_4.

Demostración: En general, si G y H son dos grupos de orden 4 cuyos elementos no triviales tienen orden 2, cualquier biyección $f : G \longrightarrow H$ que cumpla $f(1) = 1$ es un isomorfismo entre ellos, pues si $a, b \in G$, se tiene que cumplir que $f(ab) = f(a)f(b)$. Esto sucede trivialmente si $a = 1$ o $b = 1$, también si $a = b$, pues entonces es $f(a^2) = f(1) = 1 = f(a)^2$ y, por último, si $a \neq b$, hemos razonado que $ab = c$ es el tercer elemento no trivial de G, luego $f(ab) = f(c) = f(a)f(b)$, ya que también sabemos que $f(a)f(b)$ tiene que ser el tercer elemento no trivial de H, es decir, tiene que ser $f(c)$. ∎

Esto hace que, en realidad, es irrelevante que hayamos definido V_4 como el grupo $\{\pm1\}\times\{\pm1\}$. Lo único que importa es que V_4 es un grupo de orden 4 cuyos elementos no triviales tengan orden 2. Otro grupo que cumple esto es, por ejemplo, U_8, cuya tabla hemos mostrado al principio de este capítulo, y otro es $U_{12} = \{[1],[5],[7],[11]\}$, por lo que cualquiera de ellos puede ser considerado con el mismo derecho "el grupo de Klein".

El concepto de "isomorfismo de grupos" permite expresar la idea de que un grupo no es un conjunto concreto con una operación concreta, sino una forma de operar los elementos de un conjunto. Así, aunque la teoría de conjuntos nos obliga[1] a especificar un conjunto concreto al que llamar "grupo de Klein", conviene pensar que "el grupo de Klein" es cualquier grupo isomorfo al grupo de Klein, cualquier grupo de orden 4 tal que, al escribir su tabla llamando a sus elementos 1, a, b, c, sean éstos los que sean, obtenemos la tabla que hemos calculado más arriba. ∎

Los productos de grupos tienen asociados varios homomorfismos de interés. Por una parte tenemos las proyecciones: $\pi_i : G_1\times\cdots\times G_n \longrightarrow G_i$ que a cada n-tupla le asignan su componente i-ésima. Es evidente que son epimorfismos.

Por otra parte tenemos las inyecciones $\iota_i : G_i \longrightarrow G_1\times\cdots\times G_n$, dadas por $\iota_i(g) = (1,\ldots,g,\ldots 1)$, donde g se sitúa en la posición i-ésima. También es obvio que son monomorfismos.

Si $f : A \longrightarrow B$ es una aplicación biyectiva, podemos definir un isomorfismo $F : \Sigma_A \longrightarrow \Sigma_B$ entre los grupos simétricos asociados a los conjuntos A y B, que viene dado por $F(g) = f^{-1}\circ g\circ f$. Así, si A y B son conjuntos finitos, podemos afirmar que $\Sigma_A\cong\Sigma_B$ si y sólo si $|A| = |B|$. En particular, todo grupo de permutaciones de un conjunto finito es isomorfo a Σ_n para cierto n.

Por ejemplo, da igual hablar de las permutaciones del conjunto $\{a,b,c\}$ que del conjunto $\{1,2,3\}$. El isomorfismo entre ambos grupos se obtiene cambiando el nombre a los elementos. Por ejemplo, la permutación que envía el 1 al 2, el 2 al 3 y el 3 al 1 se corresponde con la que envía a a b, b a c y c a a.

1.4 Subgrupos y generadores

Definición 1.10 Si G es un grupo, un *subgrupo* de G es un grupo $H\subset G$ tal que el producto de dos elementos de H sea el mismo calculado en H o en G. Lo representaremos por $H\leq G$.

Notemos que si $H\leq G$ entonces el elemento neutro de H es el mismo que el de G, pues es el único elemento de H o de G que cumple $hh = h$. Igualmente, el inverso de un $h\in H$ es el mismo en H o en G, pues el inverso en h cumple también las condiciones para ser su inverso en G, y éste es único.

[1] Podríamos sortear esta obligación definiendo un "grupo" como una clase de equivalencia de grupos isomorfos, pero eso presenta ciertos inconvenientes técnicos y no es necesario en la práctica.

Por lo tanto, si $H \leq G$ entonces H es un subconjunto de G tal que el producto de dos elementos de H está en H, el neutro de G está en H y el inverso de cada elemento de H está en H. Recíprocamente, todo subconjunto de H que cumpla estas condiciones puede dotarse de forma única de estructura de grupo de modo que sea un subgrupo de G (estableciendo que el producto de dos elementos de H sea su producto en G). En la práctica conviene resumir estas condiciones en una sola:

Teorema 1.11 *Sea G un grupo y H un subconjunto no vacío de G. Entonces H es un subgrupo de G (con la restricción del producto de G) si y sólo si para todos los elementos $h_1, h_2 \in H$ se cumple $h_1 h_2^{-1} \in H$.*

DEMOSTRACIÓN: Obviamente un subgrupo debe cumplir esta condición. Si H la cumple, por ser no vacío existe $h \in H$, luego $1 = hh^{-1} \in H$. Además, si $h \in H$, entonces $h^{-1} = 1 \cdot h^{-1} \in H$, y si $h_1, h_2 \in H$, tenemos que $h_1, h_2^{-1} \in H$, luego $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$. Esto prueba que $H \leq G$. ∎

Notemos que si G es un grupo finito (o, más en general, un grupo cuyos elementos tengan todos orden finito), para que un subconjunto no vacío $H \subset G$ sea un subgrupo basta con que para todos los elementos $h_1, h_2 \in H$ se cumpla $h_1 h_2 \in H$, pues esto ya implica que si $h \in H$ entonces $h^n \in H$ para todo número natural n, y aplicándolo a $n = o(h) - 1$ tenemos que $h^{-1} \in H$.

Todo grupo G tiene como subgrupos el propio G y el subgrupo $1 = \{1\}$, llamado *subgrupo trivial* (y lo representaremos por 0 cuando usemos la notación aditiva). Los grupos 1 y G se llaman *subgrupos impropios* de G. Cualquier otro subgrupo es un *subgrupo propio.*

Observemos que hemos descrito los seis elementos del grupo Σ_3 en términos exclusivamente de dos de ellos, los que hemos llamado σ y τ. Esto se expresa diciendo que σ y τ forman un sistema generador de Σ_3.

Para dar una definición general de sistema generador observamos que, evidentemente, la intersección de toda familia de subgrupos de un grupo dado es de nuevo un subgrupo, lo cual nos permite definir el subgrupo generado por un conjunto:

Definición 1.12 Sea G un grupo y $X \subset G$. Llamaremos *subgrupo generado* por X a la intersección de todos los subgrupos de G que contienen a X. Lo representaremos mediante $\langle X \rangle$. Notemos que $\langle \varnothing \rangle = 1$.

Si $G = \langle X \rangle$ diremos que el conjunto X es un *generador* de G. Un grupo que admite un generador con un solo elemento es un grupo *cíclico.*

Teorema 1.13 *Sea G un grupo, X un subconjunto no vacío de G, llamemos $X^{-1} = \{x^{-1} \mid x \in X\}$ y sea g un elemento de G. Entonces:*

1. $\langle X \rangle = \{x_1 \cdots x_n \mid n \in \mathbb{N},\ x_1, \ldots, x_n \in X \cup X^{-1}\}$.
2. *Si G es finito* $\langle X \rangle = \{x_1 \cdots x_n \mid x_1, \ldots, x_n \in X\}$.
3. $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

DEMOSTRACIÓN: 1) Sea $H = \{x_1 \cdots x_n \mid n \in \mathbb{N},\ x_1, \ldots, x_n \in X \cup X^{-1}\}$. Tenemos que $\langle X\rangle$ es un grupo que contiene a los elementos de X, luego también a sus inversos y a los productos que pueden formarse entre ellos. Por lo tanto $H \subset \langle X\rangle$.

Por otro lado, H es un subgrupo de G, ya que no es vacío (claramente contiene a X), el producto de dos de sus elementos está claramente en H y el inverso de uno de sus elementos es $x_n^{-1} \cdots x_1^{-1} \in H$, pues si $x_i \in X$, entonces $x_i^{-1} \in X^{-1}$ y si $x_i \in X^{-1}$ entonces $x_i^{-1} \in X$. Por lo tanto, $\langle X\rangle \subset H$ y tenemos la igualdad.

2) Si G es finito (o, más en general, si todos sus elementos tienen orden finito) podemos razonar como en 1) partiendo de $H_0 = \{x_1 \cdots x_n \mid x_1, \ldots, x_n \in X\}$. La diferencia es que ahora (por la observación tras el teorema 1.11), para probar que H_0 es un subgrupo, basta probar que el producto de dos elementos de H_0 está en H_0.

3) Es consecuencia inmediata de 1). ∎

Combinando el teorema 1.4 con el último apartado del teorema anterior vemos que un elemento g de un grupo G tiene orden finito si y sólo si $|\langle g\rangle|$ es finito, y en tal caso $o(g) = |\langle g\rangle|$, pues hemos visto $\langle g\rangle$ está formado por las potencias de g y hay exactamente $o(g)$ potencias distintas. En particular, un grupo de orden finito n es cíclico si y sólo si tiene un elemento de orden n, pues el subgrupo generado por tal elemento será necesariamente el grupo completo.

Por ejemplo, es evidente que todos los grupos $\mathbb{Z}/n\mathbb{Z}$ son cíclicos, pues la clase 1 tiene orden n, luego genera todo el grupo. En cambio, hemos visto que U_7 es cíclico, mientras que U_{28} y Σ_3 no lo son, pues no tienen elementos de orden 12 y 6, respectivamente.

Ejemplos Los subgrupos cíclicos de $\mathbb{Z}/6\mathbb{Z}$ son

$$\langle 0\rangle = 0,\quad \langle 1\rangle = \langle 5\rangle = \mathbb{Z}/6\mathbb{Z},\quad \langle 2\rangle = \langle 4\rangle = \{0,2,4\},\quad \langle 3\rangle = \{0,3\}.$$

Los subgrupos cíclicos de U_7 son:

$$\langle 1\rangle = 1,\quad \langle 2\rangle = \langle 4\rangle = \{1,2,4\},\quad \langle 3\rangle = \langle 5\rangle = U_7,\quad \langle 6\rangle = \{1,6\}.$$

Los subgrupos cíclicos de Σ_3 son:

$$\langle 1\rangle = 1,\quad \langle \sigma\rangle = \langle \sigma^2\rangle = \{1,\sigma,\sigma^2\},$$

$$\langle \tau\rangle = \{1,\tau\},\quad \langle \sigma\tau\rangle = \{1,\sigma\tau\},\quad \langle \sigma^2\tau\rangle = \{1,\sigma^2\tau\}.$$

Los subgrupos cíclicos de U_{28} son

$$\langle 1\rangle = 1,\quad \langle 13\rangle = \{1,13\},\quad \langle 15\rangle = \{1,15\},\quad \langle 27\rangle = \{1,27\}$$

$$\langle 3\rangle = \langle 19\rangle = \{1,3,9,19,25,27\},\quad \langle 5\rangle = \langle 17\rangle = \{1,5,9,13,17,25\}$$

$$\langle 11\rangle = \langle 23\rangle = \{1,9,11,15,23,25\},\quad \langle 9\rangle = \langle 25\rangle = \{1,9,25\}.$$

Pero éstos no son los únicos subgrupos propios de U_{28}. Por ejemplo,

$$V = \{1, 13, 15, 27\}$$

es también un subgrupo, como se puede comprobar construyendo su tabla. Es un subgrupo de orden 4 cuyos elementos no triviales son todos de orden 2, luego es isomorfo al grupo de Klein. Vemos así que U_{28} es un grupo abeliano de orden 12 que tiene subgrupos de órdenes $1, 2, 3, 4, 6, 12$. En la sección siguiente demostraremos que el orden de un subgrupo divide necesariamente al orden del grupo. ∎

Núcleo e imagen Cada homomorfismo de grupos tiene asociados dos subgrupos de interés:

Definición 1.14 Si $f : G \longrightarrow H$ es un homomorfismo de grupos, $G_1 \leq G$ y $H_1 \leq H$, es fácil ver que $f[G_1] \leq H$ y que $f^{-1}[H_1] \leq G$. En particular se define el *núcleo* de f como el subgrupo $\mathrm{N}(f) = f^{-1}[1] = \{g \in G \mid f(g) = 1\} \leq G$ y la *imagen* de f como el subgrupo $\operatorname{Im} f = f[G] \leq H$.

Teorema 1.15 *Un homomorfismo de grupos $f : G \longrightarrow H$ es un epimorfismo si y sólo si $\operatorname{Im} f = H$ y es un monomorfismo si y sólo si $\mathrm{N}(f) = 1$.*

Demostración: La primera parte es inmediata por las definiciones. Si $\mathrm{N}(f) = 1$ y $f(g_1) = f(g_2)$, entonces

$$f(g_1 g_2^{-1}) = f(g_1) f(g_2)^{-1} = 1,$$

luego $g_1 g_2^{-1} \in \mathrm{N}(f)$, luego $g_1 g_2^{-1} = 1$, luego $g_1 = g_2$, lo que prueba que f es inyectiva. Recíprocamente, si f es un monomorfismo y $g \in \mathrm{N}(f)$, entonces $f(g) = 1 = f(1)$, luego $g = 1$. ∎

Ejemplo Consideremos el grupo multiplicativo $\{\pm 1\}$ y $S : \Sigma_3 \longrightarrow \{\pm 1\}$ dada por

$$S(1) = S(\sigma) = S(\sigma^2) = 1, \quad S(\tau) = S(\sigma\tau) = S(\sigma^2\tau) = -1.$$

La tabla siguiente muestra que se trata de un homomorfismo de grupos, pues todos los productos de permutaciones con imagen 1 son permutaciones con imagen 1 (el cuadrado superior izquierdo), los productos de permutaciones con imagen -1 tienen imagen $(-1)^2 = 1$ (el cuadrado inferior derecho) y los productos de permutaciones con imagen 1 y -1 tienen imagen $1(-1) = -1$:

		1			-1		
		1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
1	1	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
	σ	σ	σ^2	1	$\sigma\tau$	$\sigma^2\tau$	τ
	σ^2	σ^2	1	σ	$\sigma^2\tau$	τ	$\sigma\tau$
-1	τ	τ	$\sigma^2\tau$	$\sigma\tau$	1	σ^2	σ
	$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	1	σ^2
	$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	1

Claramente $\operatorname{Im} S = \{\pm 1\}$ y $\mathrm{N}(S) = \langle\sigma\rangle$. ∎

Ejemplo Si G es un grupo y $g \in G$, podemos definir un homomorfismo de grupos $f : \mathbb{Z} \longrightarrow G$ mediante $f(n) = g^n$.

Teniendo en cuenta que en $\mathbb{Z}$ usamos la notación aditiva, que f sea un homomorfismo equivale a la igualdad $f(m+n) = f(m)f(n)$, y esto es lo mismo que $g^{m+n} = g^m g^n$, que se cumple ciertamente. Claramente $\operatorname{Im} f = \langle g \rangle$, mientras que el teorema 1.4 se interpreta en este contexto como que $\mathrm{N}(f) = 1$ si g tiene orden infinito y $\mathrm{N}(f) = \langle n \rangle = n\mathbb{Z}$ si $o(g) = n$. ∎

Grupos cíclicos Los grupos cíclicos son los grupos más sencillos. El teorema siguiente recoge sus propiedades básicas:

Teorema 1.16 *Se cumplen los hechos siguientes:*

1. *Todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$.*
2. *Todo grupo cíclico de orden n es isomorfo a $\mathbb{Z}/n\mathbb{Z}$.*
3. *Todo grupo cíclico es abeliano.*
4. *Todo subgrupo de un grupo cíclico es cíclico.*
5. *Cada grupo cíclico finito tiene un único subgrupo de cada orden que divide al orden del grupo.*
6. *Si d divide al orden de un grupo cíclico, éste tiene exactamente $\phi(d)$ elementos de orden d.*

Demostración: Sea $G = \langle g \rangle$ un grupo cíclico.

1) Si G es infinito, entonces g tiene orden infinito y la aplicación $f : \mathbb{Z} \longrightarrow G$ dada por $f(n) = g^n$ es un isomorfismo de grupos. En efecto, en el ejemplo precedente hemos visto que es un homomorfismo de grupos de núcleo trivial, luego es un monomorfismo, y es suprayectiva por definición de grupo cíclico.

2) Si $|G| = o(g) = d$, la aplicación $f : \mathbb{Z}/d\mathbb{Z} \longrightarrow G$ dada por $f([m]) = g^m$ es un isomorfismo. En efecto, el teorema 1.4 nos da que $[m] = [n]$ si y sólo si $g^m = g^n$, lo que implica que f está bien definida, obviamente es suprayectiva y, como ambos grupos tienen d elementos, es biyectiva, y como en el ejemplo anterior se ve que es un homomorfismo de grupos.

3) Es consecuencia de los apartados anteriores, o también se comprueba directamente sin más que observar que dos elementos de G son de la forma g^m y g^n, por lo que $g^m g^n = g^{m+n} = g^{n+m} = g^n g^m$.

4) Sea $H \leq G$. Si G es infinito, no perdemos generalidad si suponemos que $G = \mathbb{Z}$. Ahora observamos que el hecho de que H sea un subgrupo se traduce en que si $m, n \in H$, entonces $m + n \in H$, y esto implica también que si $m \in H$ y $n \in \mathbb{Z}$ entonces $nm = m + \cdots + m \in H$, luego H es un ideal de $\mathbb{Z}$, y por [Al 3.2] sabemos que $\mathbb{Z}$ es un dominio de ideales principales, luego H es un ideal principal, es decir, $H = n\mathbb{Z}$, para cierto entero n, pero esto equivale a que $H = \langle n \rangle$, como subgrupo, luego es cíclico.

Si G es finito, consideramos el conjunto $H^* = \{n \in \mathbb{Z} \mid [n] \in H\}$, y es inmediato que H^* es un subgrupo de $\mathbb{Z}$, luego existe un $m \in \mathbb{Z}$ tal que $H^* = m\mathbb{Z}$, luego $[n] \in H$ si y sólo si $n \in m\mathbb{Z}$, si y sólo si $n = km$, para cierto $k \in \mathbb{Z}$, si y sólo si $[n] = k[m]$, para cierto $k \in \mathbb{Z}$, si y sólo si $[n] \in \langle[m]\rangle$, luego $H = \langle[m]\rangle$ es un grupo cíclico.

5) Si $|g| = n$ y $m \mid n$, entonces $o(g^{n/m}) = m$ por 1.5, luego $H = \langle g^{n/m}\rangle$ es un subgrupo de orden m. Vamos a ver que es el único. Si H^* es otro, sabemos que es cíclico, digamos $H^* = \langle g^k\rangle$. Sea $d = (k, n)$, de modo que, por 1.5, $n/d = m$ o, equivalentemente, $d = n/m$. Por la relación de Bezout, existen enteros tales que $d = uk + vn$, luego $g^d = (g^k)^u(g^n)^v = (g^k)^u$, luego $g^d \in H^*$, luego $H = \langle g^d\rangle \leq H^*$ y, como ambos grupos tienen el mismo número de elementos, $H = H^*$.

6) Si G es un grupo cíclico, sus elementos de orden d estarán en su único subgrupo de orden d, luego basta ver que todo grupo cíclico $G = \langle g\rangle$ de orden d tiene $\phi(d)$ elementos de orden d, lo cual se sigue del teorema 1.5. ∎

Es costumbre llamar C_n a cualquier grupo cíclico de orden n. Como dos cualesquiera son isomorfos entre sí, no importa cuál consideramos concretamente, del mismo modo que no importa a qué grupo en concreto llamamos V_4. Así, una forma de expresar que un grupo G es cíclico de orden n es decir que $G \cong C_n$.

Por ejemplo, ya conocemos dos grupos no isomorfos de orden 4, que son C_4 y V_4. No son isomorfos porque C_4 tiene un elemento de orden 4 y en V_4 todos los elementos no triviales tienen orden 2. Igualmente, C_6 y Σ_3 son dos grupos no isomorfos de orden 6. No son isomorfos porque uno es abeliano y el otro no.

Teorema 1.17 *Si C_n es un grupo cíclico de orden n, entonces* $\operatorname{Aut} C_n \cong U_n$.

Demostración: Sea $C_n = \langle g\rangle$, donde $o(g) = n$. Para cada $m \in \mathbb{Z}$, la aplicación $\alpha_m : C_n \longrightarrow C_n$ dada por $\alpha_m(x) = x^m$ es claramente un homomorfismo de grupos (esto es cierto para cualquier grupo abeliano). Si $(m, n) = 1$, entonces $\alpha_m(g) = g^m$ tiene orden n, por el teorema 1.5, luego $\operatorname{Im}\alpha_m$ contiene un elemento de orden m y, por consiguiente, $\operatorname{Im}\alpha_m = C_n$, es decir, que α_m es un epimorfismo. Pero una aplicación suprayectiva de un conjunto finito en sí mismo es también inyectiva, luego $\alpha_m \in \operatorname{Aut} C_n$.

Ahora observamos que si $m_1 \equiv m_2$ (mód m), entonces $\alpha_{m_1} = \alpha_{m_2}$, luego tenemos bien definida una aplicación $\alpha : U_n \longrightarrow \operatorname{Aut} C_n$ dada por $\alpha([m]) = \alpha_m$.

Se cumple que α es un homomorfismo de grupos, pues

$$\alpha([uv])(x) = x^{uv} = (x^u)^v = \alpha([v])(\alpha([u])(x)) = (\alpha[u] \circ \alpha[v])(x),$$

luego $\alpha([u][v]) = \alpha([u]) \circ \alpha([v])$.

Además α es un monomorfismo, pues si $\alpha([m]) = 1$, esto implica que

$$\alpha([m])(g) = g^m = g,$$

luego $m \equiv 1$ (mód n), luego $[m] = 1$ en U_n.

Por último, si $\phi : C_n \longrightarrow C_n$ es cualquier automorfismo, sea m tal que $\phi(g) = g^m$. Como tiene que ser $o(g^m) = o(g) = n$, el teorema 1.5 nos da que $(m, n) = 1$, luego $[m] \in U_m$ y $\alpha([m])(g) = g^m = \phi(g)$, luego $\alpha([m])(g^k) = \phi(g^k)$ para todo k, luego $\alpha([m]) = \phi$, y esto prueba que α es un isomorfismo. ∎

El grupo cuaternio Hasta ahora sólo conocemos un ejemplo de grupo no abeliano, a saber, el grupo de permutaciones Σ_3. En realidad es fácil ver que todos los grupos Σ_n para $n \geq 3$ son no abelianos, pero Σ_4 tiene ya 24 elementos, y estudiarlo sin disponer aún de la teoría oportuna sería muy farragoso. Mucho mayor es Σ_8, que tiene orden 40 320, pero vamos a estudiar uno de sus subgrupos, concretamente $Q_8 = \langle i, j\rangle$, donde

$$i = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 8 & 7 & 5 & 6 \end{pmatrix}, \quad j = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

Como se trata de un grupo finito, Q_8 está formado por todos los productos que podemos obtener multiplicando i, j cualquier número de veces en cualquier orden. Como máximo, podremos obtener 40 320 permutaciones, pero vamos a ver que son muchas menos. Una de ellas es

$$k = ij = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 6 & 5 & 3 & 4 & 2 & 1 \end{pmatrix}.$$

Ahora comprobamos que

$$i^2 = j^2 = k^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix} = -1,$$

donde la última igualdad es una definición, es decir, vamos a llamar -1 a esta permutación, que tiene la propiedad de que $(-1)^2 = 1$. Esto nos da las relaciones $i^4 = j^4 = k^4 = 1$, por lo que las tres permutaciones tienen orden 4 (su orden tiene que dividir a 4 y no es 2). Por otra parte, si llamamos

$$\begin{aligned} -i &= i^3 = i^2 \cdot i = i \cdot i^2 = (-1)i = i(-1) \\ -j &= j^3 = j^2 \cdot j = j \cdot j^2 = (-1)j = j(-1) \\ -k &= k^3 = k^2 \cdot k = k \cdot k^2 = (-1)k = k(-1) \end{aligned}$$

tenemos tres permutaciones más de Q_8, que son distintas de las cuatro que ya hemos encontrado y de la identidad. No hace falta calcularlas explícitamente, sino que podemos razonar así:

- Tiene que ser $-i \neq 1$, pues eso significaría $i^3 = 1$, pero i tiene orden 4. Igualmente $-j, -k$ son distintas de 1.
- Tiene que ser $-i \neq -1$, pues eso significaría $(-1)i = -1$, luego $i = 1$, que no es cierto. Igualmente $-i, -j, -k$ son distintas de ± 1.
- Tiene que ser $-i \neq -j$, pues eso implicaría $i = j$, que no es cierto, luego $-i, -j, -k$ son distintas entre sí.

- Tiene que ser $-i \neq i$, pues eso implicaría $-1 = 1$, lo cual es falso, e igualmente $-i, -j, -k$ son distintas de i, j, k, respectivamente.
- Tiene que ser $-i \neq j$, pues en tal caso $i(-1) = ij^2 = j$, luego $k = ij = j$, que ya hemos visto que no sucede. Por lo tanto, $\pm i, \pm j, \pm k$ son distintas entre sí.

Por lo tanto, hemos encontrado 8 permutaciones distintas en Q_8. Para probar que no hay más sólo necesitamos comprobar la relación

$$ji = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 5 & 6 & 4 & 3 & 1 & 2 \end{pmatrix} = -k.$$

En efecto, más explícitamente, tenemos que $ji = i^3 j$. Así, un elemento arbitrario de Q_8 se expresa como producto de permutaciones i, j, pero, cada vez que tenemos un producto ji, podemos pasar la j a la derecha mediante la relación anterior, hasta reducir el producto a uno de la forma $i^m j^n$. A su vez, como j tiene orden 4, podemos exigir que $n = 0, 1, 2, 3$, pero si $n = 2, 3$ podemos convertir $j^2 = i^2$ y así reducir $n = 0, 1$, y por último podemos reducir $m = 0, 1, 2, 3$, con lo que sólo hay 8 posibilidades para un elemento de Q_8. Explícitamente, la tabla de Q_8 es:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

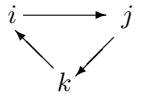
Todos los productos se pueden calcular operando explícitamente las permutaciones o bien a partir de las relaciones que hemos obtenido. Por ejemplo:

$$k(-i) = i \cdot j \cdot i(-1) = i \cdot i^3 \cdot j(-1) = j^3 = -j.$$

En la práctica, para operar en Q_8 basta recordar que -1 conmuta tanto con i como con j, luego conmuta con todos los elementos de Q_8, así como las relaciones

$$i^2 = j^2 = k^2 = -1, \quad (-1)^2 = 1,$$
$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad il = -j.$$

A su vez, las seis últimas relaciones se resumen en que el producto de dos de los tres elementos i, j, k es el tercero si el orden de los factores es el que indican las flechas:



y el tercero cambiado de signo si el orden es el contrario.

Los subgrupos cíclicos de Q_8 son:

$$\langle 1\rangle = 1, \quad \langle -1\rangle = \{\pm 1\},$$

$$\langle i\rangle = \langle -i\rangle = \{\pm 1, \pm i\}, \quad \langle j\rangle = \langle -j\rangle = \{\pm 1, \pm j\}, \quad \langle k\rangle = \langle -k\rangle = \{\pm 1, \pm k\}.$$

Así pues, Q_8 es un grupo no abeliano de orden 8 que tiene subgrupos de órdenes $1, 2, 4, 8$. ∎

1.5 Congruencias y cocientes

Del mismo modo que se define la congruencia módulo un ideal de un anillo, podemos definir la congruencia módulo un subgrupo de un grupo, pero si el grupo no es abeliano hay en realidad dos relaciones de congruencia que no tienen por qué coincidir:

Definición 1.18 Sea G un grupo y $H \leq G$. Diremos que $u, v \in G$ son *congruentes por la izquierda* módulo H (y lo representaremos $u \equiv_i v \pmod{H}$) si cumplen $v^{-1}u \in H$.

Diremos que u y v son *congruentes por la derecha* módulo H (y lo representaremos $u \equiv_d v \pmod{H}$) si cumplen $vu^{-1} \in H$.

Si G es abeliano, es evidente que ambas relaciones son la misma, y en notación aditiva se expresan así:

$$u \equiv v \pmod{H} \quad \text{si y sólo si} \quad u - v \in H.$$

Es muy fácil comprobar que ambas relaciones son de equivalencia y que la clase de equivalencia de un elemento $a \in G$ para la congruencia por la izquierda es el conjunto $aH = \{ah \mid h \in H\}$, mientras que la clase de equivalencia de a para la congruencia por la derecha es $Ha = \{ha \mid h \in H\}$.

Llamaremos $(G/H)_i$ y $(G/H)_d$ a los conjuntos cociente para las relaciones de congruencia módulo H por la izquierda y por la derecha, respectivamente.

Ejemplo Tomemos $G = \Sigma_3$ y $H = \{1, \tau\}$ (véase la página 4). Entonces

$$1H = \tau H = \{1, \tau\}, \quad \sigma H = \sigma\tau H = \{\sigma, \sigma\tau\}, \quad \sigma^2 H = \sigma^2\tau H = \{\sigma^2, \sigma^2\tau\},$$

$$H1 = H\tau = \{1, \tau\}, \quad H\sigma = H\sigma^2\tau = \{\sigma, \sigma^2\tau\}, \quad H\sigma^2 = H\sigma\tau = \{\sigma^2, \sigma\tau\},$$

por lo que

$$(G/H)_i = \{\{1, \tau\}, \{\sigma, \sigma\tau\}, \{\sigma^2, \sigma^2\tau\}\}, \quad (G/H)_d = \{\{1, \tau\}, \{\sigma, \sigma^2\tau\}, \{\sigma^2, \sigma\tau\}\},$$

con lo que vemos que los dos conjuntos cociente son distintos, luego las dos congruencias también lo son. ∎

El ejemplo anterior muestra que las relaciones de congruencia tienen una propiedad que no es casual: las clases de congruencia tienen todas el mismo número de elementos, tantos como el subgrupo H que las define.

En efecto, esto se debe a que, en general, la aplicación $H \longrightarrow aH$ dada por $h \mapsto ah$ es claramente biyectiva, al igual que lo es la aplicación $H \mapsto Ha$ dada por $h \mapsto ha$.

Así pues, todas las clases de congruencia (a izquierda o a derecha) respecto de un subgrupo H tienen el mismo cardinal que H.

En el caso de congruencias en un grupo finito G, esto ya implica que los cocientes $(G/H)_i$ y $(G/H)_d$ tienen el mismo número de elementos (concretamente, ambos tienen $|G|/|H|$ elementos), pero podemos definir explícitamente una biyección

$$(G/H)_i \longrightarrow (G/H)_d$$

mediante $Ha \mapsto a^{-1}H$.

En efecto, la aplicación es obviamente suprayectiva, y para ver que es inyectiva suponemos que $a^{-1}H = b^{-1}H$ y vamos a probar que $Ha = Hb$.

Tenemos que $a^{-1} = a^{-1}1 \in a^{-1}H = b^{-1}H$, luego existe $h \in H$ tal que $a^{-1} = b^{-1}h$, luego $a = h^{-1}b$, luego $a \in Hb$, luego $a \equiv_d b \,(\text{mód } H)$, luego $Ha = Hb$. Por consiguiente:

Definición 1.19 Si G es un grupo y $H \leq G$, se llama *índice* de H en G al cardinal

$$|G : H| = |(G/H)_i| = |(G/H)_d|.$$

Así, en un grupo finito G, cualquiera de los dos conjuntos cociente tiene $|G : H|$ clases de $|H|$ elementos cada una, luego tenemos probado un resultado fundamental:

Teorema 1.20 (Teorema de Lagrange) *Sea G un grupo finito*[2] *y $H \leq G$. Entonces $|G| = |G : H| \cdot |H|$. En particular el orden de todo subgrupo de G es un divisor del orden de G.*

En particular ahora podemos generalizar [ITAl 3.21]:

Teorema 1.21 *Si G es un grupo finito y g es un elemento de G, entonces $o(g) \mid |G|$.*

Basta tener en cuenta que $o(g) = |\langle g \rangle|$.

Veamos algunas consecuencias interesantes:

Teorema 1.22 *Todo grupo de orden 4 es isomorfo a C_4 o a V_4, según si tiene o no elementos de orden 4. En particular, todo grupo de orden 4 es abeliano.*

Demostración: Si un grupo de orden 4 tiene un elemento de orden 4, entonces es cíclico, es decir, isomorfo a C_4. En caso contrario, por el teorema anterior sus elementos no triviales tendrán orden 2, luego el grupo será isomorfo a V_4 por el teorema 1.9. ∎

[2]El lector familiarizado con la teoría de cardinales infinitos observará que la demostración que hemos dado vale igualmente si el grupo G es infinito.

Teorema 1.23 *Todo grupo de orden primo es cíclico.*

DEMOSTRACIÓN: Si G tiene orden primo y $g \in G$ no es trivial, necesariamente $|\langle g\rangle| = |G|$, luego $G = \langle g\rangle$. ∎

Tenemos, pues, que todo grupo de orden 1 es trivial, todo grupo de orden 2 es isomorfo a C_2, todo grupo de orden 3 es isomorfo a C_3, todo grupo de orden 4 es isomorfo a C_4 o a V_4 y todo grupo de orden 5 es isomorfo a C_5. Todos estos grupos son abelianos, por lo que todo grupo no abeliano tiene al menos 6 elementos, y Σ_3 es un ejemplo de grupo abeliano con 6 elementos.

Observemos también que Σ_3 no tiene más subgrupos propios que los subgrupos cíclicos que le hemos encontrado, ya que sus órdenes tienen que ser 2 o 3, luego tienen que ser cíclicos.

¿Grupos cociente? Si A es un anillo e I es un ideal de A, el conjunto cociente A/I tiene estructura de anillo con las operaciones definidas mediante

$$[a] + [b] = [a + b], \qquad [a][b] = [ab].$$

Es natural entonces preguntarse si los conjuntos cociente $(G/H)_i$ y $(G/H)_d$ adquieren estructura de grupo con la operación

$$[g_1][g_2] = [g_1 g_2]$$

o, más explícitamente, por ejemplo, para la congruencia por la derecha,

$$(Hg_1)(Hg_2) = Hg_1g_2.$$

En general la respuesta es negativa, como podemos ver en el ejemplo dado por $G = \Sigma_3$ y $H = \{1, \tau\}$, que hemos analizado antes. Por ejemplo, imaginemos que queremos multiplicar

$$(H\sigma)(H\tau) = H\sigma\tau.$$

El problema que nos aparece es que $H\tau = H1$, luego también tendríamos que poder multiplicar

$$(H\sigma)(H\tau) = (H\sigma)(H1) = H\sigma,$$

pero $H\sigma\tau \neq H\sigma$. Por lo tanto, al multiplicar dos clases multiplicando sus representantes podemos obtener clases distintas según qué representantes elijamos, luego no hay un criterio que permita asignar un producto a un par de clases.

En general, dado un grupo G y un subgrupo H, para que podamos definir una operación en el cociente $(G/H)_d$ mediante $(Hg_1)(Hg_2) = Hg_1g_2$, sin que el producto dependa de los representantes elegidos para hacer el cálculo, es necesario que si $g \in G$ y $h \in H$, puesto que $H1 = Hh$, obtengamos el mismo resultado al calcular

$$Hg^{-1} = (Hg^{-1})(H1) = (Hg^{-1})(Hh) = Hg^{-1}h,$$

pero esto equivale a que $g^{-1} \equiv_d g^{-1}h$ (mód H), o también a que $g^{-1}hg \in H$.

Así pues, una condición necesaria para que en el cociente $(G/H)_d$ podamos definir el producto de dos clases como la clase del producto de dos cualesquiera de sus representantes es que para todo $h \in H$ y todo $g \in G$ se cumpla que $g^{-1}hg \in H$. Es fácil modificar el argumento para llegar a la misma conclusión con $(G/H)_i$ en lugar de $(G/H)_d$. En la sección siguiente probaremos que esta condición necesaria es también suficiente. ∎

1.6 Subgrupos normales y grupos cociente

Los subgrupos normales de un grupo son los subgrupos en los que es posible dotar de estructura de grupo de forma natural a los conjuntos cocientes que determinan. Para caracterizarlos conviene introducir el concepto de automorfismo interno de un grupo:

Definición 1.24 Sea G un grupo y g, $h \in G$. Definimos el *conjugado* de h por g como el elemento

$$h^g = g^{-1}hg \in G.$$

Definimos la *conjugación* $\alpha_g : G \longrightarrow G$ como la aplicación dada por $\alpha_g(h) = h^g$.

Es fácil comprobar que α_g es un automorfismo de G. Más aún, la aplicación $\alpha : G \longrightarrow \operatorname{Aut} G$ dada por $\alpha(g) = \alpha_g$ es un homomorfismo de grupos. A la imagen de este homomorfismo, es decir, al subgrupo

$$\operatorname{Int} G = \{\alpha_g \mid g \in G\}$$

se le llama grupo de los *automorfismos internos* de G.

Es evidente que $h^g = h$ si y sólo si $gh = hg$, luego $\operatorname{Int} G = 1$ si y sólo si G es abeliano.

Si $A \subset G$, escribiremos $A^g = \alpha_g[A] = \{a^g \mid a \in A\}$. Notemos que si $H \leq G$, entonces $H^g \leq G$, pues es la imagen de H por un homomorfismo de grupos.

Teorema 1.25 *Sea G un grupo y H un subgrupo de G. Las siguientes condiciones son equivalentes:*

1. *La relación de congruencia módulo H por la izquierda coincide con la relación de congruencia módulo H por la derecha.*
2. *$gH = Hg$ para todo elemento $g \in G$.*
3. *$(G/H)_i = (G/H)_d$ (y entonces escribiremos simplemente G/H).*
4. *$H^g = H$ para todo elemento $g \in G$.*
5. *$H^g \subset H$ para todo elemento $g \in G$.*

DEMOSTRACIÓN: Teniendo en cuenta que gH y Hg son las clases de equivalencia de g por la izquierda y por la derecha módulo H, es claro que 1), 2) y 3) son equivalentes.

También es fácil probar que $gH = Hg$ equivale a que $H = g^{-1}Hg = H^g$. Sólo falta probar que 5) implica 4), pero esto es consecuencia de que $H^{g^{-1}} \subset H$ implica que $H \subset H^g$, luego de hecho $H = H^g$. ∎

Definición 1.26 Diremos que N es un *subgrupo normal* de un grupo G si cumple las condiciones del teorema anterior. Lo representaremos mediante $N \trianglelefteq G$.

Es inmediato que $1, G \trianglelefteq G$, así como que todo subgrupo de un grupo abeliano es normal. También es fácil ver que todo subgrupo de índice 2 es normal. La razón es que un subgrupo H con índice 2 en un grupo G da lugar a dos clases de congruencia, una es H (tanto por la izquierda como por la derecha) y la otra es $G \setminus H$, luego se cumple la condición 3) de 1.25.

También es claro que si $G = \langle X \rangle$, entonces para que $N \leq G$ sea un subgrupo normal basta con que $N^x = N$ para todo $x \in X$, y si G es finito basta con que $N^x \leq N$ para todo $x \in X$ (pues esto ya implica que $N^x = N$).

Al final de la sección anterior hemos visto que para que un conjunto cociente respecto de un subgrupo admita estructura de grupo, el subgrupo tiene que ser normal. Ahora probamos que la condición es suficiente:

Teorema 1.27 *Sea G un grupo y $N \trianglelefteq G$. Entonces el conjunto cociente G/N es un grupo con la operación dada por $(gN)(hN) = ghN$. El elemento neutro de G/N es $1N = N$. Si $g \in G$, se cumple que $(gN)^{-1} = g^{-1}N$. Si el grupo G es abeliano o cíclico, entonces G/N también lo es.*

DEMOSTRACIÓN: Hay que probar que la operación en G/N está bien definida, es decir, que si $gN = g'N$ y $hN = h'N$, entonces $ghN = g'h'N$.

Para ello observamos que $(gh)^{-1}g'h' = h^{-1}g^{-1}g'h' = h^{-1}h'h'^{-1}g^{-1}g'h'$.

Ahora, $h^{-1}h' \in N$ y $g^{-1}g' \in N$ porque por hipótesis son congruentes módulo N, y como N es normal, $h'^{-1}g^{-1}g'h' = (g^{-1}g')^{h'} \in N$, luego $(gh)^{-1}g'h' \in N$ y así $ghN = g'h'N$.

El resto del teorema es obvio. En todo caso, nótese que si $G = \langle g \rangle$, entonces $G/N = \langle gN \rangle$. ∎

Definición 1.28 Si G es un grupo y $N \trianglelefteq G$, definimos la *proyección canónica* como el homomorfismo $p : G \longrightarrow G/N$ dado por $p(g) = Ng$.

Claramente es un epimorfismo de grupos con núcleo N.

Ejemplos En Σ_3 tenemos que el subgrupo $N = \langle \sigma \rangle$ es normal, porque tiene índice 2, mientras que el subgrupo $H = \langle \tau \rangle$ no es normal, ya que

$$\tau^\sigma = \sigma^2\tau\sigma = \sigma^4\tau = \sigma\tau \notin H.$$

Igualmente se comprueba que no son normales $\langle \sigma\tau \rangle$ y $\langle \sigma^2\tau \rangle$.

El cociente es $\Sigma_3/N = \{N, N\tau\}$, que es un grupo cíclico de orden 2. Por lo tanto, es isomorfo al grupo $\{\pm 1\}$ y el isomorfismo $f : \Sigma_3/N \longrightarrow \{\pm 1\}$ es el dado por $f(N) = 1$, $f(N\tau) = -1$. Al componerlo con la proyección canónica:

$$\Sigma_3 \xrightarrow{p} \Sigma_3/N \xrightarrow{f} \{\pm 1\}$$

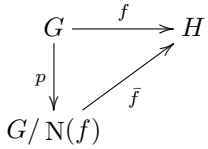
tenemos precisamente el homomorfismo S que habíamos definido en el ejemplo tras el teorema 1.15.

En Q_8 los subgrupos $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$ son normales porque tienen índice 2, pero en este caso el subgrupo $N = \{\pm 1\}$ también lo es, porque sus dos elementos conmutan con σ y con τ, por lo que $N^\sigma = N$ y $N^\tau = N$.

El cociente es $Q_8/N = \{N, Ni, Nj, Nk\}$, cuyas clases se operan como en Q_8, pero haciendo abstracción de los signos, es decir, todos los cuadrados valen 1, luego $Q_8/N \cong V_4$ es el grupo de Klein. ∎

Es inmediato comprobar que si $f : G \longrightarrow H$ es un homomorfismo de grupos y $N \trianglelefteq H$, entonces $f^{-1}[N] \trianglelefteq G$. En particular $\mathrm{N}(f) \trianglelefteq G$, y se cumple el análogo al teorema de isomorfía de anillos (con esencialmente la misma prueba):

Teorema 1.29 (Teorema de Isomorfía) *Sea $f : G \longrightarrow H$ un homomorfismo de grupos. Entonces $\mathrm{N}(f) \trianglelefteq G$, y la aplicación $\bar{f} : G/\mathrm{N}(f) \longrightarrow \operatorname{Im} f$ dada por $\bar{f}\big(g\,\mathrm{N}(f)\big) = f(g)$ es un isomorfismo de grupos que hace conmutativo el diagrama*



Es interesante analizar con detalle la situación. Para ello observamos que si $g_1, g_2 \in G$ la condición $f(g_1) = f(g_2)$ equivale a $f(g_1 g_2^{-1}) = 1$, es decir, a que $g_1 g_2^{-1} \in \mathrm{N}(f)$, o también a que $g_1 \equiv g_2$ (mód $\mathrm{N}(f)$).

Así pues, dos elementos $g_1, g_2 \in G$ son congruentes módulo $\mathrm{N}(f)$ si y sólo si ambos tienen la misma imagen por f. En otras palabras, las clases de equivalencia de $G/\mathrm{N}(f)$ agrupan los elementos de G con la misma imagen por f.

Esto lo ilustra el homomorfismo $S : \Sigma_3 \longrightarrow \{\pm 1\}$ del ejemplo que hemos analizado tras el teorema 1.15, cuyo núcleo $N = \{1, \sigma, \sigma^2\}$ está formado por los elementos con imagen 1 y la otra clase módulo N, es decir, $N\tau = \{\tau, \sigma\tau, \sigma^2\tau\}$ está formada por los elementos con imagen -1.

Ejemplo: El centro de un grupo Vamos a aplicar el teorema de isomorfía al homomorfismo $\alpha : G \longrightarrow \mathrm{Aut}(G)$ que a cada $g \in G$ le asigna el automorfismo interno α_g. Su núcleo está formado por los elementos $g \in G$ tales que $\alpha_g = 1$, es decir, tales que $\alpha_g(h) = h^g = h$ para todo $h \in G$, lo que equivale a que $gh = hg$. Esto nos lleva a la definición siguiente:

Definición 1.30 Llamaremos *centro* de un grupo G al conjunto $Z(G)$ de los elementos de G que conmutan con todos los elementos de G, de modo que G es abeliano si y sólo si $Z(G) = G$.

Hemos demostrado que $Z(G)$ es el núcleo del homomorfismo α (lo que en particular prueba que $Z(G) \trianglelefteq G$, aunque esto se comprueba trivialmente de forma directa). Por lo tanto, el teorema de isomorfía nos da que

$$G/Z(G) \cong \mathrm{Int}(G).$$

De paso, observamos que $\mathrm{Int}\, G \trianglelefteq \mathrm{Aut}\, G$.

En efecto, si $\phi \in \mathrm{Aut}\, G$ y $g \in G$, entonces, para todo $x \in G$, se cumple que

$$(\alpha_g)^\phi(x) = (\phi^{-1} \circ \alpha_g \circ \phi)(x) = \phi(\phi^{-1}(x)^g) = \phi(g^{-1}\phi^{-1}(x)g) =$$

$$\phi(g)^{-1}x\phi(g) = x^{\phi(g)} = \alpha_{\phi(g)}(x),$$

luego $(\alpha_g)^\phi = \alpha_{\phi(g)} \in \mathrm{Int}\, G$, lo que prueba que $(\mathrm{Int}\, G)^\phi \leq \mathrm{Int}\, G$, luego el subgrupo de los automorfismos internos de G es normal en el grupo de todos los automorfismos.

Es fácil ver que $Z(Q_8) = \{\pm 1\}$.

Teorema 1.31 *Si $n \geq 3$, entonces $Z(\Sigma_n) = 1$.*

Demostración: Sea $\sigma \in \Sigma_n$ tal que $\sigma \neq 1$. Esto significa que existen $i, j \in I_n$ tales que $\sigma(i) = j$, $i \neq j$. Como $n \geq 3$ existe un $k \in I_n$ distinto de i, j. Entonces $\sigma^{(jk)}(i) = k$, luego $\sigma^{(jk)} \neq 1$, luego σ no conmuta con (jk), luego $\sigma \notin Z(\Sigma_n)$. ∎

El teorema siguiente resulta útil:

Teorema 1.32 *Si un grupo G cumple que $G/Z(G)$ es cíclico, entonces G es abeliano, luego $|G : Z(G)|$ no puede ser un número primo.*

Demostración: Sea $G/Z(G) = \langle gZ(G)\rangle$. Entonces, todo $x \in G$ cumple que $xZ(G) = g^n Z(G)$, luego $x = g^n z$, con $z \in Z(G)$, pero es claro que dos elementos de esta forma conmutan, luego G es abeliano. ∎

Veamos algunas propiedades básicas de los subgrupos de los grupos cociente:

Teorema 1.33 *Sea G un grupo y $N \trianglelefteq G$.*

1. *Si $N \leq H \leq G$, entonces $H/N \leq G/N$.*
2. *Si $K \leq G/N$, entonces existe un subgrupo H de G tal que $N \leq H \leq G$ y $K = H/N$.*
3. *Si $N \leq H \leq G$, entonces $H/N \trianglelefteq G/N$ si y sólo si $H \trianglelefteq G$.*
4. *Las correspondencias descritas en los apartados 1) y 2) determinan una biyección entre los subgrupos de G/N y los subgrupos de G que contienen a N. Los subgrupos normales de G (que contienen a N) se corresponden con los subgrupos normales de G/N.*

DEMOSTRACIÓN: 1) Es inmediato. Los elementos de H/N son las clases hN con $h \in H$ y los de G/N son las clases gN con $g \in G$. La operación es la misma.

2) Sea $p : G \longrightarrow G/N$ el epimorfismo canónico dado por $p(g) = gN$. Definimos $H = p^{-1}[K] \leq G$. Como $N = p^{-1}[1N]$, claramente $N \leq H$. Así $H/N = \{hN \mid h \in H\} = p[H] = p\big[p^{-1}[K]\big] = K$.

3) Si $H/N \trianglelefteq G/N$, entonces al conjugar un elemento $h \in H$ por un elemento $g \in G$ se cumple $h^g N = (hN)^{gN} \in H/N$, luego $h^g \in H$ y así $H \trianglelefteq G$. El recíproco es análogo.

4) Si $H/N = H'/N$, entonces $H = p^{-1}[H/N] = p^{-1}[H'/N] = H'$, luego la correspondencia es inyectiva, y por 2) es suprayectiva. ∎

Ejemplo Podemos ilustrar el teorema anterior tomando $G = Q_8$ y $N = \{\pm 1\}$, de modo que $N \trianglelefteq G$. Si llamamos

$$N_1 = \langle i\rangle = \{\pm 1, \pm i\}, \quad N_2 = \langle j\rangle = \{\pm 1, \pm j\}, \quad N_3 = \langle k\rangle = \{\pm 1, \pm k\},$$

tenemos que $N \leq N_i \leq G$, luego $N_i/N \leq G/N$. Por ejemplo, para $i = 1$, tenemos que

$$N_1/N = \{N, Ni\} \leq \{N, Ni, Nj, Nk\} = G/N.$$

∎

Producto de subgrupos Si G es un grupo y A y B son subconjuntos de G, llamaremos $AB = \{ab \mid a \in A, b \in B\}$. En notación aditiva hablaremos de suma de subconjuntos y la representaremos $A + B$.

En general, el producto de dos subgrupos no tiene por qué ser un subgrupo. El teorema siguiente aclara la situación:

Teorema 1.34 *Sea G un grupo y H y K dos subgrupos de G.*

1. *$HK \leq G$ si y sólo si $HK = KH$.*
2. *Si $H \trianglelefteq G$ o $K \trianglelefteq G$, entonces $HK \leq G$.*
3. *Si $H \trianglelefteq G$ y $K \trianglelefteq G$, entonces $HK \trianglelefteq G$.*

DEMOSTRACIÓN: 1) Si $HK \leq G$ y $x \in HK$, entonces $x^{-1} \in HK$, luego es de la forma $x^{-1} = hk$, con $h \in H$ y $k \in K$. Por lo tanto $x = k^{-1}h^{-1} \in KH$. Igualmente se prueba la otra inclusión, luego $HK = KH$.

Si $HK = KH$, sean $x, y \in HK$. Entonces $x = hk$ e $y = h'k'$ con $h, h' \in H$ y $k, k' \in K$. Por lo tanto $xy^{-1} = hkk'^{-1}h'^{-1}$. El elemento $kk'^{-1}h'^{-1} \in KH = HK$, luego $kk'^{-1}h'^{-1} = h''k''$ para ciertos $h'' \in H$ y $k'' \in K$. Consecuentemente $xy^{-1} = hh''k'' \in HK$. Por el teorema 1.11 tenemos que $HK \leq G$.

2) Si $H \trianglelefteq G$ y $hk \in HK$, entonces $hk = kk^{-1}hk = kh^k \in KH^k = KH$ e igualmente se prueba la otra inclusión. Por lo tanto $HK = KH$ y por 1) $HK \leq G$.

3) Si $g \in G$, como la conjugación por g es un automorfismo de G, se cumple que $(HK)^g = H^g K^g = HK$. Por lo tanto $HK \trianglelefteq G$. ∎

El lector debe tener clara la diferencia entre que $HK = KH$ y que $hk = kh$ para todo $h \in H$ y todo $k \in K$. En el primer caso se dice que H y K *conmutan,* y en el segundo se dice que *conmutan elemento a elemento.* La segunda propiedad implica obviamente la primera, pero el recíproco no es cierto.

Ejemplo En Σ_3 podemos considerar los subgrupos $H = \{1, \tau\}$, $K = \{1, \sigma\tau\}$, de modo que

$$HK = \{1, \sigma^2, \tau, \sigma\tau\}, \quad KH = \{1, \sigma, \tau, \sigma\tau\},$$

por lo que $HK \neq KH$ y es claro que ninguno de los dos es un subgrupo de Σ_3 (pues 4 no divide a 6). Por otro lado, si $H = \{1, \sigma, \sigma^2\}$ y $K = \{1, \tau\}$, es fácil ver que $HK = KH = \Sigma_3$. Notemos que H y K conmutan, pero no conmutan elemento a elemento. ∎

Si G es abeliano se cumplen trivialmente todas las condiciones del teorema anterior y el producto de subgrupos es siempre un subgrupo.

Los teoremas de isomorfía Además del primer teorema de isomorfía, que ya hemos discutido, hay otros dos que son útiles en muchas ocasiones:

Teorema 1.35 (Segundo teorema de isomorfía) *Sea G un grupo, $H \leq G$ y $K \trianglelefteq G$. Entonces $HK/K \cong H/(H \cap K)$.*

Demostración: Consideremos la aplicación $f : H \longrightarrow HK/K$ dada por $f(h) = hK$. Es claro que se trata de un homomorfismo de grupos. Además es un epimorfismo, pues un elemento de HK/K es de la forma hkK con $h \in H$ y $k \in K$, pero $hkK = hK = f(h)$.

Un elemento $h \in H$ está en $\mathrm{N}(f)$ si y sólo si $h \in H$ y $hK = K$, si y sólo si $h \in H \cap K$, luego $\mathrm{N}(f) = H \cap K$ y por el teorema de isomorfía concluimos $HK/K \cong H/(H \cap K)$. ∎

Teorema 1.36 (Tercer teorema de isomorfía) *Consideremos un grupo G y dos subgrupos $K \trianglelefteq G$ y $K \leq H \trianglelefteq G$. Entonces $(G/K)/(H/K) \cong G/H$.*

Demostración: Un elemento de G/K es de la forma gK con $g \in G$, luego un elemento cualquiera de $(G/K)/(H/K)$ es de la forma $(gK)(H/K)$. Además $(gK)(H/K) = (1K)(H/K)$ si y sólo si $gK \in H/K$, es decir, si y sólo si $g \in H$.

Esto significa que la aplicación $f : G \longrightarrow (G/K)/(H/K)$ definida mediante $f(g) = (gK)(H/K)$ es un epimorfismo de núcleo H, luego por el teorema de isomorfía, $(G/K)/(H/K) \cong G/H$. ∎

El segundo teorema de isomorfía implica que si H y K son subgrupos de un grupo finito G y K es normal, entonces $|HK| = |H|\,|K|/|H \cap K|$. Vamos a probar que esto sigue siendo cierto aunque ninguno de los subgrupos sea normal y HK no sea un subgrupo.

Teorema 1.37 *Sea G un grupo finito y H, K dos subgrupos de G. Entonces*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

DEMOSTRACIÓN: Consideremos la aplicación $f : H \times K \longrightarrow HK$ dada por $f(h,k) = hk$. Obviamente es suprayectiva. Si $f(h,k) = f(h',k')$, entonces $hk = h'k'$, luego $u = (h')^{-1}h = k'k^{-1} \in H \cap K$.

Hemos probado que si $f(h,k) = f(h',k')$, entonces $(h',k') = (hu^{-1}, uk)$ para cierto $u \in H \cap K$. El recíproco es trivialmente cierto. Esto significa que para cada $hk \in HK$ se cumple que $f^{-1}[hk] = \big\{(hu^{-1}, uk) \;\big|\; u \in H \cap K\big\}$, luego $\big|f^{-1}[hk]\big| = |H \cap K|$.

En consecuencia, el número de elementos de $H \times K$ es igual al número de conjuntos de la forma $f^{-1}[hk]$ (que es $|HK|$) multiplicado por el número de elementos de cada uno de estos conjuntos (que es $|H \cap K|$), es decir, hemos probado que $|H|\,|K| = |HK|\,|H \cap K|$. ∎

Ejemplo: Grupos diédricos En el grupo $\Sigma_{\mathbb{Z}}$ de las permutaciones de $\mathbb{Z}$ consideramos las dadas por $\sigma(n) = n+1$ y $\tau(n) = -n$. Definimos el *grupo diédrico infinito* como $D_\infty = \langle \sigma, \tau \rangle$.

En primer lugar observamos que $\sigma^i(n) = n + i$, de donde se sigue que las potencias σ^i son distintas dos a dos, luego el orden de σ es infinito. Por el contrario, $\tau^2 = 1$, luego τ tiene orden 2.

Ahora observamos que $\sigma^\tau = \sigma^{-1}$ (lo que prueba, en particular, que D_∞ no es abeliano), pues

$$\sigma^\tau(i) = \tau(\sigma(\tau(i))) = \tau(\sigma(-i)) = \tau(-i+1) = i - 1 = \sigma^{-1}(i).$$

Por lo tanto, $(\sigma^n)^\tau = \sigma^{-n}$ o, en otros términos, $\tau\sigma^n = \sigma^{-n}\tau$. Esto hace que, aunque cada elemento de D_∞ se expresa en principio como producto de permutaciones $\sigma^{\pm 1}$ y τ (como por ejemplo $\sigma^{-1}\tau\sigma\sigma\tau\sigma^{-1}\sigma^{-1}\tau$), podemos intercambiar los factores hasta que todas las σ's queden a la izquierda, y así concluimos que

$$D_\infty = \{\sigma^n\tau^i \mid n \in \mathbb{Z},\ i = 0, 1\}.$$

Además, $(\sigma^n\tau^i)(0) = \tau^i(\sigma^n(0)) = \tau^i(n) = \pm n$, donde el signo depende de i, luego las permutaciones $\sigma^n\tau^i$ son distintas dos a dos.

Es fácil ver que las permutaciones σ^n son todas las permutaciones de $\mathbb{Z}$ que conservan el orden, mientras que las permutaciones $\sigma^n\tau$ son todas las permutaciones de $\mathbb{Z}$ que invierten el orden.

Observemos que todos los elementos σ^n tienen orden infinito, mientras que todos los $\sigma^n\tau$ tienen orden 2, porque, según las relaciones que hemos probado, $\sigma^n\tau\sigma^n\tau = \sigma^n\sigma^{-n}\tau\tau = 1$.

En particular, observemos que $\sigma\tau$ y τ son dos elementos de orden 2 cuyo producto $\sigma\tau\tau = \sigma$ tiene orden infinito. Esto muestra que hay que ser precavido al tratar de calcular el orden de un producto de dos elementos de un grupo. Más aún, es claro que $D_\infty = \langle \sigma\tau, \tau \rangle$, luego D_∞ es un grupo infinito generado por dos elementos de orden 2.

Hemos visto que $(\sigma^n)^\tau = \sigma^{-n}$ (y $(\sigma^n)^\sigma = \sigma^n$), lo que implica que $N_n = \langle\sigma^n\rangle$ es un subgrupo normal de D_∞.

A partir de aquí vamos a llamar σ_0 y τ_0 a las permutaciones que hasta ahora llamábamos σ y τ.

Definimos el *grupo diédrico de orden* $2n$ como $D_{2n} = D_\infty/\langle\sigma_0^n\rangle$. Si llamamos $\sigma = \sigma_0 N_n$, $\tau = \tau_0 N_n$, tenemos que $D_{2n} = \langle\sigma, \tau\rangle$, donde $\sigma^n = \tau^2 = 1$ y $\sigma^\tau = \sigma^{-1}$.

Notemos que σ tiene orden n, pues si $0 < i < n$ no puede suceder que $\sigma^i = 1$, ya que esto equivale a que $\sigma_0^i \in \langle\sigma_0^n\rangle$, lo cual es absurdo. Igualmente, τ tiene orden 2, ya que $\tau_0 \notin N_n$, pero $\tau_0^2 = 1 \in N_n$.

Como todo elemento de D_∞ se expresa como $\sigma_0^i\tau_0^j$, con $j = 0, 1$, es claro que todo elemento de D_{2n} se expresa como $\sigma^i\tau^j$, con $i = 0, \ldots, n-1$, $j = 0, 1$. Además la expresión es única, ya que si $\sigma^i\tau^j = \sigma^{i'}\tau^{j'}$ entonces $j = j'$, pues en caso contrario, si, por ejemplo, $j = 0$, $j' = 1$, tendríamos que $\tau = \sigma^{i-i'}$ y de aquí se sigue que $\tau_0 \in \langle\sigma_0\rangle$, contradicción. Así pues, $j = j'$, lo que implica que $\sigma^i = \sigma^{i'}$ y por lo tanto $i = i'$ (pues suponemos que los exponentes son menores que n).

En definitiva: $D_{2n} = \{1, \sigma, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \ldots \sigma^{n-1}\tau\}$ es realmente un grupo de orden $2n$, que contiene un subgrupo cíclico $N = \langle\sigma\rangle$ de orden n (normal, por tener índice 2) y los elementos restantes, de la forma $\sigma^i\tau$, tienen todos orden 2.

En particular, $D_2 = \{1, \tau\} \cong C_2$ y $D_4 = \{1, \sigma, \tau, \sigma\tau\} \cong V_4$ son grupos abelianos. Sin embargo, para $n \geq 3$, el grupo D_{2n} no es abeliano, pues cumple que $\sigma^\tau = \sigma^{-1} \neq \sigma$.

Observemos, por último, que

$$Z(D_{2n}) = \begin{cases} 1 & \text{si } n \text{ es impar,} \\ \langle\sigma^{n/2}\rangle & \text{si } n \text{ es par.} \end{cases}$$

En efecto, se cumple $\sigma^i\tau\sigma = \sigma\sigma^i\tau$ si y sólo si $\sigma^{i-1}\tau = \sigma^{i+1}\tau$, si y sólo si $\sigma^2 = 1$, lo cual no puede suceder si $n \geq 3$, luego $\sigma^i\tau \notin Z(D_{2n})$.

En cambio, $\sigma^i\tau = \tau\sigma^i$ si y sólo si $\sigma^i = \sigma^{-i}$, si y sólo si $\sigma^{2i} = 1$, lo cual, si $1 \leq i < n$, sólo puede ser si $n = 2i$, y en tal caso $\sigma^{n/2} \in Z(D_{2n})$, pues hemos visto que conmuta con τ, y obviamente conmuta con σ. ∎

El teorema siguiente nos permite identificar fácilmente un grupo diédrico:

Teorema 1.38 *Si $G = \langle\sigma, \tau\rangle$ es un grupo de orden $2n$ tal que $\sigma^n = \tau^2 = 1$ y $\sigma^\tau = \sigma^{-1}$, entonces $G \cong D_{2n}$.*

Demostración: Las relaciones $\tau\sigma = \sigma^{-1}\tau$ y $\tau\sigma^{-1} = \sigma\tau$ permiten reducir todo elemento de G a la forma $\sigma^i\tau^j$, con $0 \leq i < n$, $0 \leq j < 1$. Por lo tanto

$$G = \{1, \sigma, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \ldots \sigma^{n-1}\tau\}$$

y, como G tiene orden $2n$, estos $2n$ elementos tienen que ser distintos dos a dos.

Además el producto en G viene determinado por las relaciones:

$$\sigma^i\sigma^j = \sigma^{i+j}, \quad (\sigma^i\tau)\sigma^j = \sigma^{i-j}\tau, \quad (\sigma^i\sigma^j)\tau = \sigma^{i+j}\tau, \quad (\sigma^i\tau)(\sigma^j\tau) = \sigma^{i-j}.$$

Esto hace que si dos grupos $G = \langle\sigma,\tau\rangle$ y $G' = \langle\sigma',\tau'\rangle$ cumplen las condiciones del enunciado, la aplicación $f : G \longrightarrow G'$ dada por $f(\sigma^i\tau^j) = \sigma'^i\tau'^j$ es un isomorfismo de grupos. Como el grupo D_{2n} cumple las condiciones del enunciado, cualquier otro grupo que las cumpla es isomorfo a él. ∎

Observemos que Σ_3 cumple las condiciones de este teorema, luego $\Sigma_3 \cong D_6$. Más en general:

Teorema 1.39 *Si p es primo, todo grupo de orden $2p$ es isomorfo bien a C_{2p} o bien a D_{2p}.*

Demostración: Sea G un grupo de orden $2p$. Si $p = 2$, un grupo G de orden 4 es isomorfo a C_4 si tiene un elemento de orden 4 y, en caso contrario, sus elementos no triviales tendrán orden 2, luego G será isomorfo a $V_4 \cong D_4$ por el teorema 1.9. A partir de aquí suponemos que p es impar. Si G tiene un elemento de orden $2p$, entonces $G \cong C_{2p}$. Supongamos lo contrario, con lo que todos sus elementos no triviales tienen que tener orden 2 o p.

Veamos ahora que si G es abeliano, entonces tiene que tener elementos de orden 2 y elementos de orden p. En caso contrario, todos los elementos no triviales tendrían orden 2 o bien todos orden p, pero esto es imposible. En efecto, vamos a ver que si un grupo abeliano G tiene todos sus elementos no triviales de orden primo q, entonces el orden de G es potencia de q.

En caso contrario, podemos tomar un grupo G cuyo orden no sea potencia de q, con todos los elementos no triviales de orden q y de modo que $|G|$ sea el menor posible. En particular $G \neq 1$ (pues 1 es potencia de q). Sea $g \in G$ un elemento no trivial, luego de orden q. Entonces $N = \langle q\rangle \trianglelefteq G$ porque G es abeliano, luego G/N es un grupo abeliano cuyos elementos no triviales tienen todos orden q y $|G/N| < |G|$. Por la minimalidad de G, concluimos que $|G/N| = q^r$, luego $|G| = q^{r+1}$, contradicción.

Así pues, si G es abeliano, tiene elementos de orden 2 y de orden p, luego por el teorema 1.6 también tiene elementos de orden $2p$, que es el caso que ya habíamos excluido. Así pues, tenemos que G no es abeliano. Por el teorema 1.7 no puede ser que todos sus elementos tengan orden 2, luego hay al menos un elemento $\sigma \in G$ tal que $o(\sigma) = p$. Entonces $N = \langle\sigma\rangle \trianglelefteq G$, porque los subgrupos de índice 2 son normales.

Sea $\tau \in G \setminus N$. Entonces $o(\tau) = 2$, porque la alternativa es que $H = \langle\tau\rangle$ tenga orden p, pero la intersección $N \cap H$ tiene que tener orden 1 o p, pero si fuera p sería $N = N \cap H = H$, contradicción, luego $N \cap H = 1$, luego $|NH| = p^2 \leq p$ por el teorema 1.37, lo cual es imposible.

Por lo tanto τ tiene orden 2 y $|NH| = 2p$, es decir, $G = NH = \langle\sigma,\tau\rangle$. Como N es normal, $\sigma^\tau \in N$, luego $\sigma^\tau = \sigma^k$ para cierto k, pero

$$\sigma = \sigma^{\tau^2} = (\sigma^\tau)^\tau = (\sigma^k)^\tau = \sigma^{k^2},$$

luego $k^2 \equiv 1$ (mód p), luego $k \equiv \pm 1$ (mód p). Si fuera $k \equiv 1$ (mód p) tendríamos que $\sigma^\tau = \sigma$ y G sería abeliano, luego tiene que ser $\sigma^\tau = \sigma^{-1}$, y así llegamos a que G cumple las condiciones del teorema 1.38, luego $G \equiv D_{2n}$. ∎

En cambio, Q_8 es un grupo no abeliano de orden 8 que no es isomorfo al grupo D_8, pues en Q_8 sólo hay un elemento de orden 2, mientras que en D_8 hay cinco (los cuatro de la forma $\sigma^i\tau$ y σ^2).

Teorema 1.40 *Todo grupo no abeliano de orden* 8 *es isomorfo a* D_8 *o a* Q_8.

Demostración: Sea G un grupo no abeliano de orden 8. Sus elementos no triviales tienen que tener orden $2, 4, 8$, pero si hay un elemento de orden 8 entonces $G \cong C_8$ sería abeliano, y si todos los elementos fueran de orden 2 entonces G también sería abeliano por el teorema 1.7. Por lo tanto, tiene que haber un elemento $\sigma \in G$ de orden 4. El subgrupo $N = \langle\sigma\rangle$ tiene índice 2, luego es normal en G.

Supongamos ahora que exista $\tau \in G \setminus N$ de orden 2. Entonces $H = \langle\tau\rangle$ tiene orden 2 y $N \cap H = 1$, o de lo contrario sería $N \cap H = H$ y $\tau \in N$. El teorema 1.37 nos da que $|NH| = 8$, luego $G = NH = \langle\sigma, \tau\rangle$.

Como N es normal, $\sigma^\tau \in N$ y, como la conjugación es un automorfismo, σ^τ tiene que ser un generador de N, pero N tiene sólo dos generadores: σ y σ^{-1}, y no puede ser $\sigma^\tau = \sigma$, porque entonces G sería abeliano. Así pues, $\sigma^\tau = \sigma^{-1}$, luegl G cumple las condiciones del teorema 1.38 y concluimos que $G \cong D_8$.

La alternativa es que en $G \setminus N$ no haya elementos de orden 2, es decir, que todos sean de orden 4. Vamos a ver que en este caso $G \cong Q_8$, así que vamos a cambiar la notación y llamemos $i = \sigma$ y sea $j \in G \setminus N$, de modo que $N = \langle i\rangle$, $H = \langle j\rangle$ son dos subgrupos distintos de orden 4. El teorema 1.37 nos da ahora que

$$|NH| = \frac{4 \cdot 4}{|N \cap H|} \leq 8,$$

y $|N \cap H| \leq 2$, luego tiene que ser $|N \cap H| = 2$. Por lo tanto

$$N \cap H = \{1, i^2\} = \{1, j^2\}.$$

Llamemos $-1 = i^2 = j^2$. Como N y H son abelianos, vemos que -1 conmuta con i y con j. Como en el caso anterior concluimos que $j^i = j^{-1} = j^3$. Equivalentemente, $ji = ij^3$. Esto nos permite expresar cada elemento de G en la forma $i^m j^n$, donde $0 \leq m < 4$ y $0 \leq n < 2$, porque $j^2 = i^2$ y $j^3 = i^2 j$. En otros términos

$$G = \{1,\ i,\ i^2,\ i^3,\ j,\ ij,\ i^2j,\ i^3j\}$$

y, como G tiene orden 8, estos 8 elementos tienen que ser distintos dos a dos. Equivalentemente, llamando $-i = i^2 j = (-1)j$, etc., $G = \{\pm 1, \pm i, \pm j, \pm ij\}$, y la relación $i^j = -i$, o $ij = -ji$ permite concluir que el producto en G es exactamente el mismo de Q_8, luego $G \cong Q_8$. ∎

Veremos que todo grupo abeliano de orden 8 es isomorfo a uno de los grupos C_8, $C_2 \times C_4$ o $C_2 \times C_2 \times C_2$, con lo que hay exactamente 5 grupos de orden 8 no isomorfos entre sí.

Subgrupos característicos Algunos subgrupos poseen una propiedad relevante algo más fuerte que la normalidad:

Definición 1.41 *Un subgrupo H de un grupo G es característico si es invariante por automorfismos, es decir, si para todo $\alpha \in \mathrm{Aut}(G)$ se cumple que $\alpha[H] = H$.*

En particular, todo subgrupo característico es invariante por los automorfismos internos de G, luego es normal en G.

Es fácil ver que si H es característico en K y K es característico en G, entonces H es característico en G. Esto es falso si cambiamos "característico" por "normal", pero lo que sí que se cumple es que si H es característico en N y N es normal en G, entonces H es normal en G.

En efecto, para cada $g \in G$, el automorfismo interno $\alpha_g \in \mathrm{Aut}(G)$ se restringe a un automorfismo de N, luego $H^g = H$.

Si un grupo G tiene un único subgrupo de un determinado orden, éste es necesariamente característico en G (y es el caso de los subgrupos impropios 1 y G). Cualquier grupo que tenga una definición "canónica", en el sentido de que no dependa de la elección de elementos particulares de G, será característico. Por ejemplo, $Z(G)$ es siempre un subgrupo característico, puesto que un automorfismo transforma elementos que conmutan en elementos que conmutan.

En el apartado siguiente presentamos otro ejemplo de subgrupo característico de un grupo:

El subgrupo derivado En todo grupo hay un mínimo subgrupo normal con cociente abeliano:

Definición 1.42 Sea G un grupo. Llamaremos *subgrupo derivado* de G al subgrupo G' generado por los elementos de la forma $[x, y] = x^{-1}y^{-1}xy$, para todos los x, $y \in G$.

El elemento $[x, y]$ se llama *conmutador* de x, y. Su nombre se debe a que obviamente $xy = yx[x, y]$. En particular $[x, y] = 1$ si y sólo si $xy = yx$, es decir, si y sólo si x e y conmutan.

El teorema siguiente afirma que, como hemos anunciado, G' es el menor subgrupo normal de G cuyo cociente es abeliano:

Teorema 1.43 *Sea G un grupo. Entonces*

1. *$G' \trianglelefteq G$ y G/G' es un grupo abeliano.*
2. *Si $N \trianglelefteq G$, entonces G/N es abeliano si y sólo si $G' \leq N$.*

DEMOSTRACIÓN: 1) Es inmediato que si x, y, $g \in G$ entonces $[x,y]^g = [x^g, y^g]$. Los elementos de G' son productos de conmutadores, luego sus conjugados también, es decir, $G'^g \leq G'$, lo que prueba que G' es normal.

Claramente el cociente G/G' es abeliano, pues si xG', yG' son dos de sus elementos, tenemos que $x^{-1}y^{-1}xy \in G'$, luego $(xG')(yG') = (yG')(xG')$.

2) Si $G' \leq N$, entonces $G/N \cong (G/G')/(N/G')$, que es un grupo abeliano por ser un cociente de un grupo abeliano.

Si G/N es abeliano entonces para todo x, $y \in G$ se cumple $(xN)(yN) = (yN)(xN)$, luego $[x,y] = x^{-1}y^{-1}xy \in N$ y, como los conmutadores generan G', concluimos que $G' \leq N$. ∎

En particular un grupo G es abeliano si y sólo si $G' = 1$. Otra propiedad evidente es que si $H \leq G$, entonces $H' \leq G'$. El hecho de que G' sea el menor subgrupo que da cociente abeliano implica que, de hecho, G' es un subgrupo característico de G.

Ejemplos de subgrupos derivados Los ejemplos de grupos que hemos estudiado hasta ahora nos permiten identificar los subgrupos derivados de algunos grupos:

- Hemos visto que Σ_3 tiene un único subgrupo N de orden 3, que es normal (pues tiene índice 2) y su cociente es abeliano (porque tiene orden 2), luego $\Sigma_3' \leq N$ y, como el subgrupo derivado no puede ser trivial, ya que Σ_3 no es abeliano, tiene que ser $\Sigma_3' = N$.
- El grupo cuaternio Q_8 tiene un subgrupo normal N de orden 2, cuyo cociente tiene que ser abeliano (porque tiene orden 4), luego $Q_8' \leq N$ y, al igual que antes, como el derivado no puede ser trivial, tenemos que $Q_8' = N$.
- El mismo razonamiento se aplica al grupo diédrico D_8 y su único subgrupo normal de orden 2.Una forma de ver que es único es observar que cualquier subgrupo normal de orden 2 de D_8 tiene que ser igual a D_8'. ∎

Generalizando el último ejemplo tenemos:

Teorema 1.44 *Si $D_{2n} = \langle \sigma, \tau \rangle$ es el grupo diédrico de orden $2n$, su subgrupo derivado es $D_{2n}' = \langle \sigma^2 \rangle$.*

DEMOSTRACIÓN: Calculamos todos los conmutadores:

1. $[\sigma^i, \sigma^j] = 1$.
2. $[\sigma^i\tau, \sigma^j] = \sigma^i\tau\sigma^{-j}\sigma^i\tau\sigma^j = \sigma^i\tau\sigma^{i-2j}\tau = \sigma^{2j}$.
3. $[\sigma^i, \sigma^j\tau] = \sigma^{-i}\sigma^j\tau\sigma^i\sigma^j\tau = \sigma^{-2i}$.
4. $[\sigma^i\tau, \sigma^j\tau] = \sigma^i\tau\sigma^j\tau\sigma^i\tau\sigma^j\tau = \sigma^{i-j}\sigma^i\tau\sigma^j\tau = \sigma^{2(i-j)}$.

Esto prueba que $D_{2n}' \leq \langle \sigma^2 \rangle$ y el caso 2) para $j = 1$ muestra que $\sigma^2 \in D_{2n}'$, luego se da la igualdad. ∎

Notemos que si n es impar, entonces $D'_{2n} = \langle\sigma^2\rangle = \langle\sigma\rangle$, luego se cumple que $D_{2n}/D'_{2n} \cong C_2$, mientras que si n es par $D_{2n}/D'_{2n} \cong C_2 \times C_2$.

Ejercicio: Probar que $D'_\infty = \langle\sigma^2\rangle$.

Ejemplo Hemos definido el subgrupo derivado G' como el subgrupo generado por los conmutadores, no como el conjunto de todos los conmutadores. Conviene observar que, en general, el conjunto de todos los conmutadores de un grupo no es necesariamente un subgrupo.

Para probarlo consideremos un cuerpo k y llamemos G al conjunto de todas las matrices de la forma

$$(f(x), g(y), h(x,y)) = \begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix},$$

donde $f(x), g(y), h(x,y) \in k[x,y]$, que es un grupo con el producto usual[3] de matrices. Explícitamente:

$$(f_1(x), g_1(y), h_1(x,y))(f_2(x), g_2(y), h_2(x,y)) =$$

$$(f_1(x) + f_2(x), g_1(y) + g_2(y), h_1(x,y) + h_2(x,y) + f_1(x)g_2(y)).$$

El elemento neutro es $(0,0,0)$ (que corresponde a la matriz identidad) y el inverso de un elemento dado es

$$(f(x), g(y), h(x,y))^{-1} = (-f(x), -g(y), f(x)g(y) - h(x,y)).$$

Un cálculo rutinario muestra que el conmutador de dos elementos es

$$[(f_1(x), g_1(y), h_1(x,y)), (f_2(x), g_2(y), h_2(x,y))] = (0, 0, f_1(x)g_2(y) - f_2(x)g_1(y)).$$

En particular, $[(ax^k, 0, 0), (0, y^l, 0)] = (0, 0, ax^k y^l) \in G'$, y operando elementos de esta forma, para monomios cualesquiera, vemos que $(0, 0, h(x,y)) \in G'$, para cualquier polinomio $h(x,y)$, es decir, que G' es el subgrupo formado por todos los elementos de la forma $(0, 0, h(x,y))$.

Por último, vamos a ver que $(0, 0, x^2 + xy + y^2) \in G'$ no es un conmutador, lo que probará que G' no es, en este caso, el conjunto de todos los conmutadores de G.

En caso contrario existirían polinomios $f_1(x), f_2(x), g_1(y), g_2(y)$ tales que

$$f_1(x)g_2(y) - f_2(x)g_1(y) = x^2 + xy + y^2.$$

Pongamos que

$$f_1(x) = a_0 + a_1x + a_2x^2 + \cdots, \qquad f_2(x) = b_0 + b_1x + b_2x^2 + \cdots$$

[3]El producto de matrices lo definimos en [Al 4.32], pero podemos considerar la fórmula explícita dada como la definición del producto en G y comprobar que es una operación asociativa.

Entonces, viendo los dos miembros de la igualdad precedente como polinomios de $k[y][x]$, al igualar los términos independientes, los coeficientes de x y los de x^2 obtenemos

$$\begin{aligned} a_0g_2(y) - b_0g_1(y) &= 1, \\ a_1g_2(y) - b_1g_1(y) &= y, \\ a_2g_2(y) - b_2g_1(y) &= y^2. \end{aligned}$$

Sin embargo, estas ecuaciones son imposibles.[4] En efecto, de la primera ecuación se sigue que uno de los coeficientes a_0, b_0 no es nulo. Sin pérdida de generalidad podemos suponer que $a_0 \neq 0$, en cuyo caso

$$g_2(y) = a_0^{-1} + a_0^{-1}b_0g_1(y).$$

La segunda ecuación nos da entonces que

$$a_0^{-1}a_1 + (a_0^{-1}a_1b_0 - b - 1)g_1(y) = y,$$

de donde $a_1 = 0$, luego $g_1(y) = -b_1^{-1}y$ y $g_2(y) = a_0^{-1} + a_0^{-1}b_1^{-1}b_0y$, pero entonces la tercera ecuación es imposible, pues el miembro izquierdo es un polinomio de grado menor o igual que 1, y el miembro derecho tiene grado 2. ∎

El grupo del ejemplo anterior es infinito, y resulta natural preguntarse si puede suceder lo mismo en un grupo finito. La respuesta es afirmativa, pero puede probarse que el menor grupo en el que el subgrupo derivado no coincide con el conjunto de los conmutadores tiene 96 elementos. De hecho, hay dos grupos no isomorfos de orden 96 con esta propiedad. En la página 110 construiremos uno de ellos.

[4] El lector familiarizado con los conceptos básicos sobre espacios vectoriales, como [Al 4.29], tiene un argumento inmediato: las ecuaciones expresan que $1, y, y^2 \in \langle g_1(y), g_2(y)\rangle$, pero un subespacio vectorial de $k[y]$ de dimensión ≤ 2 no puede contener tres polinomios linealmente independientes.

Capítulo II

Grupos de permutaciones I

En este capítulo vamos a estudiar con más detalle los grupos simétricos Σ_n y sus subgrupos, si bien en la primera sección introduciremos el concepto más general de acción de un grupo sobre un conjunto que nos permitirá aplicar los resultados sobre grupos de permutaciones a grupos arbitrarios. Por ejemplo, demostraremos que todo grupo finito es isomorfo a un subgrupo de un grupo Σ_n.

2.1 Acciones de grupos

Si Ω es un conjunto y $\sigma \in \Sigma_\Omega$, no sólo podemos operar σ con otros elementos de Σ_Ω, sino que también tiene sentido aplicar σ a un elemento de Ω. La definición siguiente nos da un marco de trabajo general que incluye esta situación como un caso particular:

Definición 2.1 Una *acción* de un grupo G sobre un conjunto Ω es una aplicación $\Omega \times G \longrightarrow \Omega$ que cumple las propiedades siguientes (para todos los $a \in \Omega$ y todos los $g_1, g_2 \in G$):

1. $(ag_1)g_2 = a(g_1g_2)$.
2. $a1 = a$.

Cuando hablemos de un grupo G que *actúa* sobre un conjunto Ω, esto debe entenderse como que estamos considerando una cierta acción de G sobre Ω.

Por ejemplo, si $G \leq \Sigma_\Omega$, entonces G actúa sobre Ω mediante la acción dada por $a\sigma = \sigma(a)$.

En general, si un grupo G actúa sobre un conjunto Ω, no es necesario que G sea un subgrupo de Σ_Ω, pero a cada $g \in G$ le podemos asignar la aplicación $\tau_g : \Omega \longrightarrow \Omega$ dada por $\tau_g(a) = ag$.

Esta aplicación es inyectiva, pues si $\tau_g(a) = \tau_g(b)$, entonces $ag = bg$, luego, multiplicando por g^{-1}, queda que $a = b$, y τ_g también es suprayectiva, pues $\tau_g(ag^{-1}) = a$. Así pues, $\tau_g \in \Sigma_\Omega$.

Por consiguiente, tenemos una aplicación $\tau : G \longrightarrow \Sigma_\Omega$ que resulta ser un homomorfismo de grupos. En efecto, se trata de probar que $\tau_{gh} = \tau_g \circ \tau_h$, para lo cual tomamos $a \in \Omega$ y comprobamos que

$$\tau_{gh}(a) = agh = (ag)h = \tau_h(\tau_g(a)) = (\tau_g \circ \tau_h)(a).$$

Recíprocamente, todo homomorfismo $\tau : G \longrightarrow \Sigma_\Omega$ determina una acción de G en Ω dada por $ag = \tau_g(a)$ cuyo homomorfismo asociado es el propio τ. Por consiguiente, podemos identificar las acciones de un grupo G en un conjunto Ω con los homomorfismos $\tau : G \longrightarrow \Sigma_\Omega$.

Así pues, un grupo G actúa sobre un conjunto Ω cuando podemos asociar a cada elemento de G una permutación de Ω de modo que la asociación sea un homomorfismo de grupos (pero el homomorfismo τ no tiene por qué ser inyectivo, de manera que dos elementos de g pueden inducir en Ω la misma permutación).

El núcleo del homomorfismo τ se llama también *núcleo* de la acción, y una acción se dice *fiel* cuando su núcleo es trivial. Esto equivale a que el único elemento de G que deja invariantes a todos los elementos de Ω es 1 o también a que τ sea inyectiva, es decir, a que no haya dos elementos distintos en G que permuten igualmente los elementos de Ω.

Nota El concepto de acción que hemos definido es lo que, más precisamente, podemos llamar una *acción por la derecha* de un grupo G en un conjunto Ω. Una *acción por la izquierda* es una aplicación $G \times \Omega \longrightarrow \Omega$ que cumple las propiedades análogas:

$$g_1(g_2a) = (g_1g_2)a, \qquad 1a = a.$$

No es lo mismo, porque con una acción por la izquierda no podemos decir que la aplicación $\tau : G \longrightarrow \sigma_\Omega$ dada por $\tau_g(a) = ga$ sea un homomorfismo de grupos. Ahora se cumple que

$$\tau_{gh}(a) = gha = g\tau_h(a) = \tau_g(\tau_h(a)) = (\tau_h\tau_g)(a),$$

por lo que $\tau_{gh} = \tau_h\tau_g$. Así, τ es en este caso lo que se llama un *antihomomorfismo* de grupos, que invierte los productos en lugar de conservarlos.

No obstante, es fácil ver que si $G \times \Omega \longrightarrow \Omega$ es una acción por la izquierda de un grupo G en un conjunto Ω, podemos definir una acción por la derecha mediante $ag = g^{-1}a$, por lo que toda la teoría sobre acciones de grupos es aplicable también a las acciones por la izquierda. Por ejemplo, una acción por la izquierda determina (y está determinada por) un homomorfismo $\tau : G \longrightarrow \Sigma_\Omega$ dado por

$$\tau_g(a) = ag = g^{-1}a.$$

■

Es obvio que si un grupo G actúa sobre un conjunto Ω, todo $H \leq G$ actúa sobre Ω con la acción en la que, para cada $h \in H$, el elemento ah es el determinado por h como elemento de G. A esta acción la llamaremos *restricción* a H de la acción de G. Si la acción de G se corresponde con el homomorfismo τ, su restricción a H se corresponde con la restricción $\tau|_H$.

Podemos pensar que cuando un grupo G actúa sobre un conjunto Ω cada elemento $g \in G$ "transforma" cada elemento $a \in \Omega$ en otro $ag \in \Omega$, y podemos considerar todos los elementos de Ω por los que "pasa" uno dado a medida que actúan sobre él los distintos elementos de G. Esto se concreta mediante la definición siguiente:

Si un grupo G actúa sobre un conjunto Ω, definimos en Ω la relación dada por

$$a \sim b \quad \text{si y sólo si existe} \quad g \in G \text{ tal que } ag = b.$$

Es fácil ver que se trata de una relación de equivalencia. La clase de equivalencia de un elemento $a \in A$ recibe el nombre de *órbita* de a bajo G, y está formada por todos los elementos de Ω en que se puede transformar a mediante los elementos de G. La representaremos por Ω_a.

Una acción es *transitiva* si determina una única órbita, es decir, si cualquier elemento de Ω puede transformarse en cualquier otro mediante un elemento de G elegido convenientemente.

Por otra parte, si $a \in \Omega$, definimos el *estabilizador* de a como el conjunto $G_a = \{g \in G \mid ag = a\}$, es decir, el conjunto de elementos de G que dejan invariante a a. Es inmediato comprobar que $G_a \leq G$.

Entre estos conceptos existe una relación fundamental:

Teorema 2.2 *Sea G un grupo que actúa sobre un conjunto Ω y sea $a \in \Omega$. Entonces $|\Omega_a| = |G : G_a|$. En particular, si G es finito, el cardinal de las órbitas que determina en Ω divide al orden de G.*

DEMOSTRACIÓN: Definimos $f : (G/G_a)_d \longrightarrow \Omega_a$ mediante $f(G_a g) = ag$. La aplicación está bien definida, pues si $G_a g = G_a g'$, entonces $g'g^{-1} \in G_a$, luego $ag'g^{-1} = a$, luego $ag' = ag$.

La aplicación f es suprayectiva, pues todo $b \in \Omega_a$ es de la forma $b = ag$, para cierto $g \in G$, y también es inyectiva, pues si $f(G_a g) = f(G_a g')$, entonces $ag = ag'$, luego $ag'g^{-1} = a$, luego $g'g^{-1} \in G_a$, luego $G_a g' = G_a g$. Por lo tanto f es biyectiva, y así $|\Omega_a| = |(G/G_a)_d| = |G : G_a|$. ∎

Otro hecho elemental que conviene tener presente es que si dos elementos de un conjunto están en la misma órbita respecto a la acción de un grupo, entonces sus estabilizadores son subgrupos conjugados (en particular isomorfos):

Teorema 2.3 *Si un grupo G actúa sobre un conjunto Ω y tomamos $x \in \Omega$, $g \in G$, entonces $G_{xg} = G_x^g$.*

DEMOSTRACIÓN: Tenemos que $h \in G_{xg}$ si y sólo si $xgh = xg$, si y sólo si $xghg^{-1} = x$, si y sólo si $ghg^{-1} = h' \in G_x$, si y sólo si $h = h'^g \in G_x^g$. ∎

Veamos ahora un ejemplo de cómo podemos asociar una acción a un grupo arbitrario, aunque sus elementos no tengan nada que ver con permutaciones:

Conjugación Dado un grupo cualquiera G, el homomorfismo

$$G \longrightarrow \mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G) \leq \Sigma_G$$

hace que podamos considerar a la conjugación como una acción de G sobre el conjunto $\Omega = G$.

La relación de equivalencia en G asociada a esta acción se llama también conjugación, es decir, dos elementos $g_1, g_2 \in G$ son *conjugados* si existe un $g \in G$ tal que $g_1^g = g_2$.

La órbita de un elemento $g \in G$ respecto de la conjugación se llama *clase de conjugación* de g y se representa por

$$\mathrm{cl}(g) = \{g^x \mid x \in G\}.$$

El estabilizador de un $g \in G$ recibe el nombre de *centralizador* de g, y se representa por

$$C_G(g) = \{x \in G \mid g^x = g\} = \{x \in G \mid xg = gx\},$$

es decir, está formado por los elementos de G que conmutan con g. La relación general entre estabilizadores y órbitas afirma en este caso que

$$|\mathrm{cl}(g)| = |G : C_G(g)|.$$

Ejemplo Consideremos el grupo diédrico

$$D_8 = \{1,\ \sigma,\ \sigma^2,\ \sigma^3,\ \sigma^4,\ \tau,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau\}.$$

Obviamente $\mathrm{cl}(1) = \{1\}$, que se corresponde con que $C_{D_8}(1) = D_8$.

Es claro que $\langle\sigma\rangle \leq C_{D_8}(\sigma)$, pues $\langle\sigma\rangle$ es un grupo abeliano y todos sus elementos conmutan con σ.

Por otro lado, $\tau \notin C_{D_8}(\sigma)$, ya que $\sigma^\tau = \sigma^{-1} \neq \sigma$, luego el centralizador tiene que ser un subgrupo de D_8 con al menos 4 elementos y que no es D_8, luego tiene que ser $C_{D_8}(\sigma) = \langle\sigma\rangle$. Por consiguiente, la clase de conjugación tiene 2 elementos y, como $\sigma^\tau = \sigma^{-1}$, concluimos que $\mathrm{cl}(\sigma) = \{\sigma, \sigma^{-1}\}$.

En cambio, $(\sigma^2)^\tau = \sigma^{-2} = \sigma^2$, lo que se traduce en que $\langle\sigma\rangle \leq C_{D_8}(\sigma^2)$ y $\tau \in C_{D_8}(\sigma^2)$, lo que implica que $C_{D_8}(\sigma^2) = D_8$ (es un subgrupo con más de 4 elementos, luego tiene que tener 8). Esto significa que σ^2 conmuta con todos los elementos de D_8 y $\mathrm{cl}(\sigma^2) = \{\sigma^2\}$.

Ahora observamos que $\tau, \sigma^2 \in C_{D_8}(\tau)$, pues σ^2 está en todos los centralizadores, luego $C_{D_8}(\tau)$ tiene al menos 4 elementos, pero no es todo D_8, ya que $\sigma \notin C_{D_8}(\tau)$, luego $C_{D_8}(\tau) = \{1, \sigma^2, \tau, \sigma^2\tau\}$ y, como $\tau^\sigma = \sigma^3\tau\sigma = \sigma^2\tau$, concluimos que $\mathrm{cl}(\tau) = \{\tau, \sigma^2\tau\}$. Del mismo modo analizamos el caso restante, que nos permite completar la tabla siguiente:

$\mathrm{cl}(g)$	$C_{D_8}(g)$
$\{1\}$	D_8
$\{\sigma\}$	D_8
$\{\sigma, \sigma^3\}$	$\langle\sigma\rangle$
$\{\tau, \sigma^2\tau\}$	$\{1, \sigma^2, \tau, \sigma^2\tau\}$
$\{\sigma\tau, \sigma^3\tau\}$	$\{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$

■

Ejercicio: Calcular las clases de conjugación y los centralizadores de D_6, D_{10} y Q_8.

Los resultados que hemos obtenido sobre la conjugación nos dan un hecho elemental que, no obstante, tiene consecuencias muy interesantes:

Teorema 2.4 (Ecuación de clases) *Si G es un grupo finito no abeliano, existen elementos $x_1, \dots, x_n \in G$ tales que $C_G(x_i) \neq G$ y*

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(x_i)|.$$

DEMOSTRACIÓN: Sean $x_1, \dots, x_m$ un representante de cada clase de conjugación de G. Podemos suponer que las clases de $x_1, \dots, x_n$ tienen más de un elemento cada una, mientras que las de $x_{n+1}, \dots, x_m$ tienen un solo elemento. Pero $\mathrm{cl}(x) = \{x\}$ es equivalente a $x \in Z(G)$, luego tenemos que $Z(G) = \{x_{n+1}, \dots, x_n\}$. Ahora basta tener en cuenta que

$$|G| = \sum_{i=1}^{m} |\mathrm{cl}(x_i)| = |Z(G)| + \sum_{i=1}^{n} |\mathrm{cl}(x_i)| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(x_i)|,$$

donde $|G : C_G(x_i)| \neq 1$. ∎

Veamos una aplicación:

Si p es un número primo, un grupo finito es un *p-grupo* si su orden es potencia de p. La estructura de un p-grupo puede ser muy complicada, pero ahora podemos probar un hecho fundamental sobre ella:

Teorema 2.5 *Si p es un primo y G es un p-grupo, entonces $Z(G) \neq 1$.*

DEMOSTRACIÓN: Basta considerar la ecuación de clases para G, en la que p divide tanto a $|G|$ como a cada $|C_G(x_i)|$, luego $p \mid |Z(G)|$, y esto implica que $Z(G) \neq 1$. ∎

En particular:

Teorema 2.6 *Si p es primo, todo grupo de orden p o p^2 es abeliano.*

DEMOSTRACIÓN: Ya hemos visto en 1.23 que todo grupo de orden p es isomorfo a C_p, luego es abeliano. Si G tiene orden p^2, el teorema 1.32 nos da que $|Z(G)| \neq p$, y el teorema anterior nos da que $Z(G) \neq 1$, luego $Z(G) = G$. ∎

Así pues, todos los grupos de órdenes $1, 2, 3, 4, 5, 7, 9, 11, 13, 17, 19, 23, 25$ son abelianos.

Normalizadores y centralizadores Otra acción destacable que podemos asociar a un grupo G resulta de tomar como Ω el conjunto de todos los subgrupos de G y definiendo $\Omega \times G \longrightarrow G$ mediante $(H, g) \mapsto H^g$.

El estabilizador de un subgrupo se conoce como su normalizador:

Definición 2.7 Si G es un grupo y $H \leq G$, se define el *normalizador* de H en G como el subgrupo

$$N_G(H) = \{g \in H \mid H^g = H\}.$$

Se trata ciertamente de un subgrupo de G, cosa que se puede comprobar directamente sin dificultad, o bien podemos verlo como consecuencia de que $N_G(H)$ es, según acabamos de señalar, el estabilizador de H respecto de la acción por conjugación de G sobre los subgrupos de G.

De la definición se sigue trivialmente que $H \trianglelefteq N_G(H)$. De hecho, $N_G(H)$ es el mayor subgrupo de G en el cual H es normal.

La órbita de H en Ω es el conjunto de todos los subgrupos conjugados con H, por lo que el teorema 2.2 se particulariza en este caso a que el número de conjugados de un subgrupo H es el índice $|G : N_G(H)|$.

Notemos que si $H \leq G$ podemos definir $\alpha : N_G(H) \longrightarrow \mathrm{Aut}(H)$ mediante $\alpha_g(h) = h^g \in H^g = H$. Claramente se trata de un homomorfismo de grupos, pero hay que tener presente que su imagen no está necesariamente en $\mathrm{Int}(H)$. Los automorfismos internos de H son, por definición, los determinados por conjugación por elementos de H, pero la conjugación por un elemento de $N_G(H)$ que no esté en H no es necesariamente un automorfismo interno.

El núcleo de α está formado por los elementos $g \in N_G(H)$ que cumplen $\alpha_g(h) = h^g = h$, para todo $h \in H$, es decir, que cumplen $gh = hg$. Esto nos lleva a la definición siguiente:

Si G es un grupo y $H \leq G$, definimos el *centralizador* de H en G como el subgrupo

$$C_G(H) = \{g \in G \mid gh = hg \text{ para todo } h \in H\}.$$

Es fácil ver directamente que $C_G(H) \trianglelefteq N_G(H)$, o bien concluir que esto se cumple porque $C_G(H)$ es precisamente el núcleo del homomorfismo α que hemos definido más arriba. El teorema de isomorfía nos da que

$$N_G(H)/C_G(H) \cong \mathrm{Im}\,\alpha \leq \mathrm{Aut}(H).$$

Los centralizadores de elementos que habíamos definido previamente están relacionados con los centralizadores de subgrupos, pues $C_G(g) = C_G(\langle g \rangle)$.

Ejemplo Consideremos la acción por conjugación del grupo $G = D_8$ sobre el conjunto Ω de sus subgrupos. Entre ellos se encuentran:

- El subgrupo trivial, 1.
- Cinco subgrupos de orden 2:

$$Z(G) = \langle \sigma^2 \rangle, \quad \langle \tau \rangle, \quad \langle \sigma\tau \rangle, \quad \langle \sigma^2\tau \rangle, \quad \langle \sigma^3\tau \rangle.$$

- Tres subgrupos de orden 4:

$$\langle \sigma \rangle, \quad \langle \sigma^2, \tau \rangle, \quad \langle \sigma^2, \sigma\tau \rangle.$$

- G.

Notemos que los subgrupos de orden 4 distintos de $\langle\sigma\rangle$ son los de la forma $Z(G)H$, donde H varía en los cuatro subgrupos de orden 2 distintos de $Z(G)$, y son ciertamente subgrupos porque $Z(G)$ es un subgrupo normal y ambos son de tipo V_4. Es fácil convencerse de que no hay más.

Los subgrupos de orden $1, 4, 8$ son normales (los de orden 4 porque tienen índice 2), luego sus órbitas constan únicamente de ellos mismos, y lo mismo sucede con $\langle\sigma^2\rangle$.

Ahora, $N_G(\langle\tau\rangle) = N_G(\langle\sigma^2\tau\rangle) = \langle\sigma^2, \tau\rangle$, ya que $\langle\tau\rangle, \langle\sigma^2, \tau\rangle \lhd \langle\sigma^2, \tau\rangle$ (por tener índice 2) y no hay ningún subgrupo mayor en el que los dos subgrupos de orden 2 sean normales, ya que la única posibilidad sería G, y ninguno de ellos es normal en G. Análogamente, $N_G(\langle\sigma\tau\rangle) = N_G(\langle\sigma^3\tau\rangle) = \langle\sigma^2, \sigma\tau\rangle$.

Como los normalizadores tienen índice 2, concluimos que cada subgrupo tiene exactamente 2 conjugados en G (él mismo y otro). Como $\tau^\sigma = \sigma^{-1}\tau\sigma = \sigma^2\tau$, concluimos que las órbitas que G determina en Ω constan de un único subgrupo cada una excepto $\{\langle\tau\rangle, \langle\sigma^2\tau\rangle\}$ y $\{\langle\sigma\tau\rangle, \langle\sigma^3\tau\rangle\}$. ∎

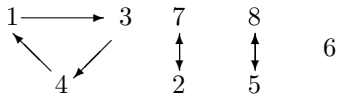
2.2 Los grupos simétricos

Pasamos ya al estudio de los grupos simétricos. Vamos a usar los conceptos que acabamos de introducir para obtener una descripción muy útil, tanto en la teoría como en la práctica, de las permutaciones de conjuntos finitos.

Ejemplo Consideremos la aplicación $g \in \Sigma_8$ dada por

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 4 & 1 & 8 & 6 & 2 & 5 \end{pmatrix}$$

donde —recordemos— esto significa que $g(1) = 3$, $g(2) = 7$, etc. La figura siguiente nos permite visualizarla mejor:



Las "agrupaciones" que vemos en la figura son precisamente las órbitas de la acción sobre I_8 del grupo $G = \langle g\rangle$. En efecto, tenemos que $1g = 3$ y $3g = 4$, luego $1g^2 = 4$, e igualmente $1g^3 = 1$, luego $1g^4 = 3$, y así vemos que cualquier elemento de G transforma el 1 en uno de los tres números $1, 3, 4$. Igualmente se razona con las demás, luego concluimos que la acción de G sobre I_8 determina cuatro órbitas, que son

$$\{1, 3, 4\}, \quad \{2, 7\}, \quad \{5, 8\}, \quad \{6\}.$$

∎

Ciclos Consideremos, en general, una permutación $g \in \Sigma_n$, sea $G = \langle g \rangle$ y sea $a \in I_n$. Entonces la órbita de a respecto de G es $\{ag^m \mid m \in \mathbb{Z}\}$. Ahora bien, como tiene que ser un conjunto finito, existen enteros $m_1 < m_2$ tales que $ag^{m_1} = ag^{m_2}$, luego $ag^{m_2-m_1} = a$. En suma, existe un número natural $m > 0$ tal que $ag^m = a$. Si m es el menor posible y k es cualquier número entero, entonces $k = mc + r$, con $0 \leq r < m$, y $ag^k = a(g^m)^c g^r = ag^r$. En suma, la órbita de a es en realidad $\{a, ag, \dots ag^{m-1}\}$, y tiene cardinal m, pues si $ag^i = ag^j$ con $0 \leq i < j < m$, entonces $ag^{j-i} = a$, con $j - i < m$, en contradicción con la minimalidad de m.

Así pues, al ir aplicando a un elemento a las potencias sucesivas de g vamos obteniendo elementos distintos

$$a \mapsto ag \mapsto ag^2 \mapsto \cdots \mapsto ag^{m-1} \mapsto a$$

hasta que, para un cierto m, se cumple $ag^m = a$, y a partir de ahí, si seguimos aplicando g, los elementos de la órbita se van repitiendo cíclicamente. El ejemplo anterior muestra varios casos concretos de esta situación:

$$1 \mapsto 3 \mapsto 4 \mapsto 1 \mapsto 3 \mapsto 4 \mapsto \cdots \qquad 2 \mapsto 7 \mapsto 2 \mapsto 7 \mapsto \cdots$$

$$5 \mapsto 8 \mapsto 5 \mapsto 8 \mapsto \cdots \qquad 6 \mapsto 6 \mapsto 6 \mapsto \cdots$$

Definición 2.8 Sea $g \in \Sigma_n$ una permutación, sea $G = \langle g \rangle$ y sea $a \in I_n$. Diremos que g es un *ciclo* si todas las órbitas que determina en I_n son triviales (en el sentido de que tienen un único elemento) excepto una. La *longitud* de un ciclo se define como el cardinal de su órbita no trivial. Los ciclos de longitud 2 se llaman *trasposiciones*.

En general, cuando hablemos de la órbita de un ciclo se entenderá que nos referimos a su órbita no trivial. Diremos que dos ciclos son *disjuntos* si sus órbitas lo son.

Si un ciclo g tiene órbita $\{a, ag, \dots, ag^{m-1}\}$, con $ag^m = a$, lo representaremos con la notación

$$g = (a, ag, \dots, ag^{m-1}).$$

Por ejemplo, el ciclo $(1, 3, 4) = (4, 1, 3) = (3, 4, 1) \in \Sigma_8$ es la permutación que cumple

$$1 \mapsto 3 \mapsto 4 \mapsto 1, \qquad 2 \mapsto 2, \quad 5 \mapsto 5, \quad 6 \mapsto 6, \quad 7 \mapsto 7, \quad 8 \mapsto 8.$$

Notemos que, en general, si g es un ciclo de longitud m y a es un elemento de su órbita, tenemos que $ag^m = a$, y entonces g^m fija a todos los elementos de la órbita de a, pues otro cualquiera es de la forma ag^i, y resulta que

$$ag^i g^m = ag^{m+i} = ag^m g^i = ag^i.$$

Por otra parte, como g fija a todos los elementos que no están en su órbita, lo mismo le sucede a g^m, y concluimos que $g^m = 1$. Por otra parte, si $0 < i < m$ tiene que ser $g^i \neq 1$, porque $ag^i \neq a$. Por lo tanto, la longitud de un ciclo no es ni más ni menos que el menor natural $m > 0$ tal que $g^m = 1$, es decir, su orden.

Teorema 2.9 *Sea $n > 0$ un número natural.*

1. *La longitud de un ciclo de Σ_n coincide con su orden.*

2. *Dos ciclos disjuntos conmutan.*

3. *Toda permutación de Σ_n distinta de 1 se expresa de forma única salvo el orden como producto de ciclos disjuntos dos a dos.*

4. *El orden de un producto de ciclos disjuntos es el mínimo común múltiplo de las longitudes de los ciclos.*

5. *Σ_n está generado por las trasposiciones.*

DEMOSTRACIÓN: 1) lo acabamos de probar. Para probar 2), consideramos un ciclo g de órbita A y otro g' de órbita A', con $A \cap A' = \varnothing$. Entonces, si $i \in I_n$, tenemos que

$$(gg')(i) = \begin{cases} g(i) & \text{si } i \in A, \\ g'(i) & \text{si } i \in A', \\ i & \text{si } i \in I_n \setminus (A \cup A'), \end{cases}$$

y esto no depende del orden, es decir, que $g'g$ es la misma permutación.

3) Dada $g \in \Sigma_n$, sean $A_1, \ldots, A_m$ sus órbitas no triviales. Es claro que $g[A_i] = A_i$, luego podemos definir $g_i \in \Sigma_n$ tal que $g_i|_{A_i} = g|_{A_i}$ y $g_i|_{I_n \setminus A_i}$ es la identidad. Claramente g_i es un ciclo de órbita A_i, y es fácil ver que $g = g_1 \cdots g_m$.

La unicidad se debe a que si $g = g_1 \cdots g_m$, donde los g_i son ciclos disjuntos de órbitas $A_1, \ldots, A_m$, entonces necesariamente $g_i|_{A_i} = g|_{A_i}$, de donde se sigue que $A_1, \ldots A_n$ son necesariamente las órbitas de g. Esto determina los g_i salvo el orden.

4) Sabemos que el orden de un ciclo es su longitud, luego si $g = g_1 \cdots g_m$ es una descomposición en ciclos disjuntos y r es el mínimo común múltiplo de sus longitudes, entonces $g_i^r = 1$, luego (teniendo en cuenta que los ciclos conmutan) $g^r = g_1^r \cdots g_m^r = 1$. Por otra parte, si $r' < r$, entonces existe un i tal que el orden de g_i no divide a r', luego $g_i^{r'} \neq 1$, pero si A_i es la órbita de g_i, tenemos que $g|_{A_i} = g_i|_{A_i}$, luego $g^{r'}|_{A_i} = g_i^{r'}|_{A_i} \neq 1$, luego $g^{r'} \neq 1$, luego r es el menor natural no nulo que cumple $g^r = 1$, es decir, el orden de g.

5) El hecho de que toda permutación se descomponga en producto de ciclos implica que los ciclos generan Σ_n, pero a su vez cada ciclo se puede expresar como producto de trasposiciones:

$$(a_1, \ldots, a_m) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_m),$$

luego las trasposiciones también son un generador. ∎

Ejemplo La descomposición en ciclos disjuntos de la permutación del ejemplo de la página 41 es

$$g = (1,3,4)(2,7)(5,8).$$

Es fácil operar con permutaciones cuando están expresadas como productos de ciclos disjuntos. Por ejemplo, para calcular el producto de $(2,5,7)(1,3)$ por $(1,3,4)(7,8)$, es decir,

$$(2,5,7)(1,3)(1,3,4)(7,8),$$

tomamos el 1, y vemos que al aplicar sucesivamente los cuatro ciclos obtenemos

$$1 \mapsto 1 \mapsto 3 \mapsto 4 \mapsto 4,$$

luego el producto empieza por un ciclo $(1,4,\ldots)$ Ahora calculamos

$$4 \mapsto 4 \mapsto 1 \mapsto 1,$$

luego cerramos el ciclo $(1,4)$. Pasamos al 2:

$$2 \mapsto 5 \mapsto 5 \mapsto 5 \mapsto 5,$$

luego tenemos $(1,4)(2,5,\ldots)$. Ahora partimos del 5:

$$5 \mapsto 7 \mapsto 7 \mapsto 7 \mapsto 8,$$

luego $(1,4)(2,5,8,\ldots)$. Pasamos al 8:

$$8 \mapsto 8 \mapsto 8 \mapsto 8 \mapsto 7,$$

luego $(1,4)(2,5,8,7,\ldots)$. Ahora:

$$7 \mapsto 2 \mapsto 2 \mapsto 2 \mapsto 2,$$

luego cerramos el ciclo $(1,4)(2,5,8,7)$. Falta estudiar el 3 y el 6, pero es fácil ver que quedan fijos, luego concluimos que

$$(2,5,7)(1,3)(1,3,4)(7,8) = (1,4)(2,5,8,7).$$

El cálculo de inversos es también muy simple, pues es claro que

$$(a_1,\ldots,a_n)^{-1} = (a_n,\ldots,a_1),$$

y, como los ciclos disjuntos conmutan, el inverso de un producto de ciclos disjuntos es el producto de los ciclos inversos. ∎

Observemos ahora la tabla siguiente, que contiene las potencias de un ciclo:

n	σ^n
1	$(1,2,3,4,5,6)$
2	$(1,3,5)(2,4,6)$
3	$(1,4)(2,5)(3,6)$
4	$(1,5,3)(2,6,4)$
5	$(6,5,4,3,2,1)$

En general:

Teorema 2.10 *Si $\sigma \in \Sigma_n$ es un ciclo de longitud k y $d = (k, m)$, entonces σ^m se descompone en producto de d ciclos disjuntos de longitud $o(\sigma^m) = k/d$.*

DEMOSTRACIÓN: Sea $G = \langle\sigma\rangle$, sea $H = \langle\sigma^m\rangle$ y sea Ω la única órbita no trivial de σ. Si $i \in \Omega$, su órbita respecto de la acción de G es

$$\Omega_i^G = \{ig \mid g \in G\},$$

que es la única órbita no trivial de σ, luego tiene longitud $k = |G|$. En particular, si $g_1, g_2 \in G$ son distintos, se cumple que $ig_1 \neq ig_2$. Por lo tanto, la órbita de i respecto de σ^m es

$$\Omega_i^H = \{ih \mid h \in H\}$$

está formada por $|H| = k/d$ elementos distintos, pues si $h_1 \neq h_2$ son elementos de H, se cumple que $ih_1 \neq ih_2$ (es un caso particular de lo anterior). Esto prueba que las órbitas respecto a σ^m de los elementos de Ω tienen todas longitud k/d (y las de índices de I_n que no estén en Ω son obviamente triviales), luego σ^m determina d órbitas no triviales de longitud k/d, luego se descompone en producto de d ciclos disjuntos de longitud k/d. ∎

Ejemplo: El grupo Σ_3 Observemos que $\Sigma_1 = 1$ y $\Sigma_2 = \{1, (1,2)\}$ es un grupo cíclico de orden 2. Consideremos ahora Σ_3, que es un grupo de orden 6. Sus elementos distintos de 1 pueden ser trasposiciones $(\circ,\circ)$ o ciclos de longitud 3: $(\circ,\circ,\circ)$. Analizando todos los casos posibles, vemos que

$$\Sigma_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (3,2,1)\}.$$

En particular vemos que Σ_3 tiene tres elementos de orden 2 y dos elementos de orden 3. Eso nos da los subgrupos cíclicos

$$\langle(1,2)\rangle = \{1, (1,2)\}, \quad \langle(1,3)\rangle = \{1, (1,3)\}, \quad \langle(2,3)\rangle = \{1, (2,3)\},$$
$$\langle(1,2,3)\rangle = \{1, (1,2,3), (3,2,1)\},$$

y no hay más subgrupos, pues cualquier subgrupo propio tiene que tener orden 2 o 3, luego tiene que ser cíclico. ∎

Ejemplo: El grupo Σ_4 El grupo Σ_4 tiene 24 elementos, la tabla siguiente recoge los tipos posibles y el número de permutaciones de cada tipo:

1	$(\circ,\circ)$	$(\circ,\circ)(\circ,\circ)$	$(\circ,\circ,\circ)$	$(\circ,\circ,\circ,\circ)$
1	6	3	8	6

Por ejemplo, para calcular el número de ciclos (a, b, c) de longitud 3 observamos que tenemos 4 posibilidades para elegir a, otras 3 para elegir b y otras 2 para elegir c, lo que nos da 24 posibilidades, pero como $(a, b, c) = (c, a, b) = (b, c, a)$, estamos contando tres veces cada ciclo, luego el número de ciclos es 8.

Ahora es claro ver que Σ_4 tiene 9 subgrupos C_2, y 4 subgrupos C_3 (porque cada uno tiene que contener dos ciclos de longitud 3) y 3 subgrupos C_4 (porque cada uno tiene que contener dos ciclos de longitud 4), y éstos son todos sus subgrupos cíclicos, pero hay muchos otros que no son cíclicos.

Por ejemplo, el estabilizador de cada $i = 1, 2, 3, 4$ (es decir, el conjunto de las permutaciones en cuya expresión en ciclos no aparece el índice i) es un subgrupo de Σ_4 isomorfo a Σ_3.

Es muy fácil identificar las permutaciones conjugadas:

Teorema 2.11 *Sea n un número natural no nulo.*

1. *Si $(a_1, \dots, a_m)$ es un ciclo en Σ_n y $\sigma \in \Sigma_n$, entonces*
$$(a_1, \dots, a_m)^\sigma = \big(\sigma(a_1), \dots, \sigma(a_m)\big).$$
2. *Dos permutaciones de Σ_n cuyas descomposiciones en producto de ciclos disjuntos sean $\sigma_1 \cdots \sigma_r$ y $\tau_1 \cdots \tau_s$ son conjugadas si y sólo si $r = s$ y (reordenando adecuadamente) la longitud de cada σ_i coincide con la de τ_i.*

Demostración: 1) En primer lugar,

$$\begin{aligned}\big((a_1, \dots, a_m)^\sigma\big)\big(\sigma(a_1)\big) &= \sigma\Big((a_1, \dots, a_m)\Big(\sigma^{-1}\big(\sigma(a_1)\big)\Big)\Big)\\ &= \sigma\big((a_1, \dots, a_m)(a_1)\big) = \sigma(a_2)\\ &= \big(\sigma(a_1), \dots, \sigma(a_m)\big)\big(\sigma(a_1)\big).\end{aligned}$$

Lo mismo vale para cualquier otro a_i. Si a es distinto de $\sigma(a_1), \dots, \sigma(a_m)$, entonces $\sigma^{-1}(a)$ es distinto de $a_1, \dots, a_m$, luego $(a_1, \dots, a_m)\big(\sigma^{-1}(a)\big) = \sigma^{-1}(a)$ y

$$\sigma\Big((a_1, \dots, a_m)\big(\sigma^{-1}(a)\big)\Big) = \sigma\big(\sigma^{-1}(a)\big) = a = \big(\sigma(a_1), \dots, \sigma(a_m)\big)(a).$$

Así pues $(a_1, \dots, a_m)^\sigma$ y $\big(\sigma(a_1), \dots, \sigma(a_m)\big)$ actúan igual sobre todos los elementos, luego son iguales.

2) Si $g \in \Sigma_n$, entonces $(\sigma_1 \cdots \sigma_r)^g = \sigma_1^g \cdots \sigma_r^g$, donde los σ_i^g son ciclos disjuntos (por el apartado anterior, si las órbitas de $\sigma_1, \dots, \sigma_r$ son $A_1, \dots, A_r$, entonces las órbitas de $\sigma_1^g, \dots, \sigma_r^g$ son $g[A_1], \dots, g[A_r]$). La unicidad de la descomposición hace que, $r = s$ y, salvo reordenación, $\sigma_i^g = \tau_i$, luego σ_i y τ_i tienen la misma longitud.

Respectivamente, si $r = s$ y la longitud de σ_i coincide con la de τ_i, digamos que $\sigma_i = (a_{i1}, \dots, a_{im_i})$, $\tau_i = (b_{i1}, \dots, b_{im_i})$, podemos tomar $g \in \Sigma_n$ que cumpla $g(a_{ij}) = b_{ij}$, y entonces, por el apartado anterior, $\sigma_i^g = \tau_i$, y concluimos que $(\sigma_1 \cdots \sigma_r)^g = \tau_1 \cdots \tau_r$. ∎

Ejemplos Ahora es inmediato que Σ_3 tiene tres clases de conjugación, a saber:

$$\{1\}, \qquad \{(1,2), (1,3), (2,3)\}, \qquad \{(1,2,3), (3,2,1)\}.$$

El centralizador de cada permutación coincide con el subgrupo que genera. Por ejemplo, el en caso de una trasposición, como la clase de conjugación tiene 3 elementos, el centralizador tiene que tener índice 3, luego orden 2, luego tiene que ser el subgrupo generado por la trasposición.

Consideremos ahora el caso de Σ_4. La tabla siguiente contiene un representante de cada clase de conjugación, junto con su centralizador y la estructura del mismo:

σ	$\mathrm{cl}(\sigma)$	$C_{\Sigma_4}(\sigma)$	
1	1	Σ_4	Σ_4
$(1,2)$	6	$\{1,(1,2),(3,4),(1,2)(3,4)\}$	V_4
$(1,2,3)$	8	$\langle(1,2,3)\rangle$	C_3
$(1,2,3,4)$	6	$\langle(1,2,3,4)\rangle$	C_4
$(1,3)(2,4)$	3	$\langle(1,2,3,4),(2,4)\rangle$	D_8

La segunda columna viene dada por la tabla de la página 45, y nos da el orden del centralizador. Para $\sigma = 1$ éste es obviamente Σ_4. En los casos de los ciclos de longitud 3 y 4 es inmediato que el centralizador tiene que tener también orden 3 o 4, respectivamente, por lo que tiene que constar exclusivamente del subgrupo generado por el ciclo.

En el caso de una transposición, el centralizador tiene que tener orden 4, y es obvio que $(3,4) \in C_{\Sigma_4}((1,2))$, pues dos ciclos disjuntos conmutan, lo que implica que el centralizador contiene a $\langle(1,2),(3,4)\rangle$, luego se tiene que dar la igualdad, y se trata de un grupo isomorfo a V_4, pues todos sus elementos no triviales tienen orden 2.

Por último, para el caso de un producto de trasposiciones, observando que $(1,3)(2,4) = (1,2,3,4)^2$, concluimos que $(1,2,3,4) \in C_{\Sigma_4}((1,3)(2,4))$. Esto nos da ya cuatro elementos del centralizador, y otros dos son, obviamente, $(1,3)$ y $(2,4)$, pues, ambas conmutan entre sí, luego también con su producto. Como el centralizador tiene que tener orden 8, necesariamente es

$$C_{\Sigma_4}((1,3)(2,4)) = \langle(1,2,3,4),(2,4)\rangle\,.$$

Explícitamente, sus elementos son los del subgrupo

$$D_8 = \{1,(1,2,3,4),(1,3)(2,4),(4,3,2,1),(2,4),(1,4)(2,3),(1,3),(1,2)(3,4)\}.$$

Notemos que, si llamamos $\sigma = (1,2,3,4)$, $\tau = (2,4)$, sólo tenemos que comprobar que las cuatro primeras permutaciones son las potencias de σ y que las segundas se obtienen multiplicándolas por τ, pues esto implica que estas 8 permutaciones están en el centralizador, y no puede haber más.

Es fácil ver que este grupo es isomorfo a D_8, por ejemplo, por el teorema 1.38. Así tenemos una representación de D_8 como grupo de permutaciones. No es la única posibilidad. Por ejemplo, el centralizador de $(1,2)(3,4) = (1,3,2,4)^2$ es

$$D_8' = \{1,(1,3,2,4),(1,2)(3,4),(4,2,3,1),(1,2),(1,3)(2,4),(3,4),(1,4)(2,3)\},$$

que es otro subgrupo de Σ_4 isomorfo a D_8. Observemos además que

$$V_4 = D_8 \cap D_8' = \{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$$

es otro subgrupo de Σ_4 isomorfo a V_4, pero es distinto de los centralizadores de las trasposiciones que hemos calculado antes (por ejemplo, porque no contiene ninguna trasposición). Además, este subgrupo cumple $V_4 \trianglelefteq \Sigma_4$, porque es la unión de dos clases de conjugación (la trivial y la formada por todos los productos de dos trasposiciones). Esto hace que al conjugar cualquier elemento de V_4 obtengamos otro de sus elementos. ∎

Veamos algunas aplicaciones del teorema 2.11:

Teorema 2.12 *Σ_n está generado por las trasposiciones $(i, i+1)$, para $1 \leq i < n$, y también por las trasposiciones $(1, i)$ para $1 < i \leq n$.*

Demostración: Por 2.9 sabemos que Σ_n está generado por las trasposiciones, luego basta ver que toda trasposición (i, j) se expresa como producto de las indicadas en el enunciado. Ahora bien, por ejemplo,

$$(1,5) = (2,5)^{(1,2)} = (3,5)^{(2,3)(1,2)} = (4,5)^{(3,4)(2,3)(1,2)} =$$

$$(1,2)(2,3)(3,4)(4,5)(3,4)(2,3)(1,2),$$

y es claro que del mismo modo podemos expresar cualquier (i, j) en producto de trasposiciones de números consecutivos.

Por otro lado, $(i, j) = (1, i)(1, j)(1, i)$, luego bastan las trasposiciones $(1, i)$ para generar todas las demás. ∎

Teorema 2.13 *Si p es primo, entonces Σ_p está generado por un p-ciclo cualquiera y una trasposición cualquiera.*

Demostración: Sea σ un p-ciclo y $\tau = (a, b)$ una trasposición y llamemos $H = \langle \sigma, \tau \rangle$. Como la órbita de σ recorre todos los índices, existe un k tal que $\sigma^k(a) = b$. Como $\sigma^k \in H$ y es también un p-ciclo (porque p es primo, luego todas sus potencias no triviales tienen orden p), basta probar que $\langle \sigma^k, \tau \rangle = \Sigma_p$. Equivalentemente, podemos suponer que $\sigma(a) = b$. Si $\sigma = (a, b, a_3 \ldots, a_p)$, sea $\rho \in \Sigma_p$ dada por $\rho(a) = 1$, $\rho(b) = 2$, $\rho(a_i) = i$. Entonces $\sigma^\rho = (1, \ldots, p)$ y $\tau^\rho = (1, 2)$, luego basta probar que $H^\rho = \langle (1, \ldots, p), (1, 2) \rangle = \Sigma_p$, pues en tal caso, conjugando por ρ^{-1} obtenemos que $H = \Sigma_p$. Equivalentemente, podemos suponer que $\sigma = (1, \ldots, p)$, $\tau = (12)$. Ahora bien, $(1, 2)^{\sigma^{i-1}} = (i, i + 1) \in H$, luego $H = \Sigma_p$ por el teorema anterior. ∎

Teorema 2.14 *Si $G \leq \Sigma_n$ es transitivo y está generado por transposiciones, entonces $G = \Sigma_n$.*

Demostración: Como G contiene transposiciones y cualquier transposición es conjugada con $(1, 2)$, cambiando G por un conjugado podemos suponer que $(1, 2) \in G$. Si $n = 2$ la conclusión es trivial, así que podemos suponer $n \geq 3$.

Por 2.12 basta probar que $(1, k) \in G$ para todo $1 < k \leq n$. Se cumple para $k = 2$, luego podemos suponer $3 \leq k \leq n$. Como G es transitivo, existe $g \in G$ tal que $g(1) = k$. Como g está generado por transposiciones, $g = \tau_1 \cdots \tau_r$,

donde cada $\tau_i \in G$ es una transposición. Sea $j_i = (\tau_1 \cdots \tau_i)(2)$, de modo que $j_r = k$. Podemos suponer que $j_{i-1} \neq j_i$, o de lo contrario podríamos eliminar τ_i. Entonces $\tau_i = (j_{i-1}, j_i)$, entendiendo que $j_0 = 2$. También podemos suponer que $j_i \neq 2$ para $i > 0$, pues en caso contrario podríamos suprimir $\tau_1 \cdots \tau_{i-1}$. Así pues:

$$g = (2, j_1)(j_1, j_2) \cdots (j_{r-1}, k).$$

Si ningún j_i es 1, entonces $g(1) = 1$ y $(1,2)^g = (1,k) \in G$. Si, por el contrario, $j_i = 1$, para cierto i (necesariamente $1 \leq i < r$), entonces será $\tau_{i+1} = (1, j_{i+1})$. Llamamos $h = \tau_{i+1} \cdots \tau_r \in G$, de modo que $h(1) = k$, $h(2) = 2$ y así $(1,2)^h = (k,2) \in G$ y a su vez $(2,k)^{(1,2)} = (1,k) \in G$. ∎

2.3 Grupos alternados

Vamos a ver ahora que cada grupo Σ_n tiene un único subgrupo de índice 2. Para probar su existencia necesitamos una definición un tanto técnica.

Si $\sigma \in \Sigma_n$ y $1 \leq i < j \leq n$, puede ocurrir que $\sigma(i) < \sigma(j)$, o bien que $\sigma(j) < \sigma(i)$. En el segundo caso diremos que σ *invierte* el par $\{i, j\}$. Diremos que una permutación es par o impar según si el número de pares que invierte es par o impar. Explícitamente:

Definición 2.15 Sea $n \geq 2$, sea $P_n = \big\{\{i,j\} \;\big|\; 1 \leq i < j \leq n\big\}$. Para cada permutación $\sigma \in \Sigma_n$ y cada $b = \{i,j\}$ con $1 \leq i < j \leq n$, sea

$$\epsilon(\sigma, b) = \begin{cases} 1 & \text{si } \sigma(i) < \sigma(j), \\ -1 & \text{si } \sigma(j) < \sigma(i). \end{cases}$$

Llamaremos *signatura* de σ a

$$\operatorname{sig}\sigma = \prod_{b \in P_n} \epsilon(\sigma, b) \in \{1, -1\}.$$

Las permutaciones de signatura 1 se llaman *permutaciones pares.* Las de signatura -1 se llaman *impares.*

Teorema 2.16 *Sea $n \geq 2$. Entonces la aplicación* $\operatorname{sig} : \Sigma_n \longrightarrow \{-1, 1\}$ *es un homomorfismo de grupos.*

Demostración: Sean σ, $\tau \in \Sigma_n$ y sea $b \in P_n$. Es fácil comprobar que $\epsilon(\sigma\tau, b) = \epsilon(\sigma, b)\epsilon\big(\tau, \sigma[b]\big)$. Como la aplicación $P_n \longrightarrow P_n$ dada por $b \mapsto \sigma[b]$ es biyectiva, se cumple que

$$\operatorname{sig}(\sigma\tau) = \prod_{b \in P_n} \epsilon(\sigma\tau, b) = \prod_{b \in P_n} \epsilon(\sigma, b)\epsilon\big(\tau, \sigma[b]\big)$$

$$= \prod_{b \in P_n} \epsilon(\sigma, b) \prod_{b \in P_n} \epsilon\big(\tau, \sigma[b]\big) = \prod_{b \in P_n} \epsilon(\sigma, b) \prod_{b \in P_n} \epsilon(\tau, b) = (\operatorname{sig}\sigma)(\operatorname{sig}\tau).$$

∎

Este teorema nos da una interpretación sencilla y operativa de la signatura de una permutación. Consideremos, por ejemplo, la trasposición $(1,2) \in \Sigma_n$. Es claro que $\epsilon\big((1,2),b\big) = -1$ si y sólo si $b = \{1,2\}$, luego $\operatorname{sig}(1,2) = -1$. Más aún, todas las trasposiciones son conjugadas (por el teorema 2.11), y obviamente

$$\operatorname{sig}(\sigma^\tau) = (\operatorname{sig}\sigma)^{\operatorname{sig}\tau} = \operatorname{sig}\sigma,$$

pues $\{+1,-1\}$ es un grupo abeliano. Esto implica que todas las trasposiciones tienen signatura -1. Si unimos esto al teorema anterior y al teorema 2.9, tenemos probado el teorema siguiente:

Teorema 2.17 *Una permutación es par o impar si y sólo si se descompone en un número par o impar de trasposiciones, respectivamente.*

No podíamos tomar esto como definición porque requiere probar que una misma permutación no puede descomponerse a la vez en producto de un número par y de un número impar de trasposiciones, cosa que ha quedado probada implícitamente.

Es fácil reconocer la signatura de una permutación descompuesta en ciclos. Según la prueba de 2.9 5), un ciclo de longitud m se descompone en $m-1$ trasposiciones, luego un ciclo es par si y sólo si su longitud es impar.

Definición 2.18 Llamaremos *grupo alternado* de grado n al grupo A_n formado por las permutaciones pares de Σ_n, es decir, al núcleo del homomorfismo sig.

Teorema 2.19 *Si $n \geq 3$, el grupo A_n está generado por los ciclos de longitud 3 y, más precisamente, por los ciclos $(1,2,i)$, para $3 \leq i \leq n$.*

Demostración: Consideremos un producto de dos trasposiciones. Ha de ser de la forma $(a,b)(c,d)$ o bien de la forma $(a,b)(a,c)$, pero

$$(a,b)(c,d) = (a,b,c)(c,a,d), \qquad (a,b)(a,c) = (a,b,c),$$

luego toda permutación par se expresa como producto de ciclos de longitud 3.

Finalmente observamos que el subgrupo generado por los ciclos $(1,2,i)$ contiene a $(1,2,i)(1,2,i) = (1,i,2)$, y también a $(1,2,j)(1,2,i)(1,j,2) = (1,i,j)$, y también a $(1,i,j)(1,k,i) = (i,j,k)$, luego contiene todos los ciclos de longitud 3 y, por consiguiente, es A_n. ∎

Teorema 2.20 *Si $n \geq 2$, entonces A_n es el único subgrupo de índice 2 de Σ_n.*

Demostración: Por el teorema de isomorfía, $\Sigma_n/A_n \cong \{1,-1\}$, luego $|\Sigma_n : A_n| = 2$, es decir, $|A_n| = n!/2$. Notemos que esto vale en realidad para $n \geq 2$, pues en $\Sigma_1 = 1$ no hay permutaciones impares.

Supongamos ahora que $N \leq \Sigma_n$ es cualquier subgrupo de índice 2 (y por consiguiente es normal). El cociente Σ_n/N es isomorfo a $\{\pm 1\}$. Componiendo el epimorfismo canónico en el cociente con este isomorfismo obtenemos un epimorfismo $f : \Sigma_n \longrightarrow \{\pm 1\}$ de núcleo N.

Si $\sigma, \tau \in \Sigma_n$ son dos trasposiciones, sabemos que son conjugadas, es decir, existe $\rho \in \Sigma_n$ tal que $\tau = \sigma^\rho$, luego $f(\tau) = f(\sigma)^{f(\rho)} = f(\sigma)$, donde usamos que $\{\pm 1\}$ es un grupo abeliano.

Como las trasposiciones generan Σ_n, sus imágenes por p tienen que generar la imagen $\{\pm 1\}$, pero todas tienen la misma imagen, luego $f(\sigma) = -1$, para toda trasposición σ, luego $f(\sigma) = 1$ para toda permutación par, lo que significa que $A_n \leq N$, luego $A_n = N$. ∎

Claramente $A_2 \cong 1$, $A_3 \cong C_3$, mientras que

$$A_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),$$

$$(1,2,3), (3,2,1), (1,2,4), (4,2,1), (1,3,4), (4,3,1), (2,3,4), (4,3,2)\}$$

es un grupo no abeliano de orden 12 y no es isomorfo a D_{12}, pues no tiene elementos de orden 6. Más aún, no tiene subgrupos de orden 6.

En efecto, si $H \leq A_4$ fuera un subgrupo de orden 6, sería isomorfo a C_6 o a D_6, y en ambos casos contendría un único subgrupo de orden 3, pero A_4 tiene cuatro subgrupos de orden 3, luego uno de ellos, digamos K, tendría que cumplir que $H \cap K = 1$, pero entonces $|HK| = 18$ y HK no cabría en A_4.

Así pues, no es cierto que un grupo tenga que tener subgrupos de cualquier orden que divida al orden del grupo.

Es fácil determinar todos los subgrupos de A_4: además de los subgrupos impropios, tiene 4 subgrupos C_4, otros 3 subgrupos C_2 y un único subgrupo de orden 4, a saber,

$$V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\},$$

que es único porque no hay más elementos de orden 2 y no hay de orden 4. Notemos que, como $V_4 \trianglelefteq \Sigma_4$, también $V_4 \trianglelefteq A_4$.

Los grupos alternados tienen una propiedad que más adelante veremos que tiene su relevancia:

Definición 2.21 Un grupo es *simple* si sus únicos subgrupos normales son los impropios.

Ejercicio: Probar que los grupos simples abelianos son los cíclicos de orden primo.

Acabamos de ver que A_4 no es simple. Sin embargo:

Teorema 2.22 *Si $n \geq 5$ entonces el grupo alternado A_n es un grupo simple no abeliano.*

Demostración: En primer lugar observamos que si un subgrupo $N \trianglelefteq A_n$ contiene un ciclo de longitud 3, entonces $N = A_n$.

En efecto, sea $(a, b, c) \in N$. Si σ es cualquier otro ciclo de longitud 3, por el teorema 2.11 existe una permutación $\tau \in \Sigma_n$ tal que $(a, b, c)^\tau = \sigma$.

Si $\tau \in A_n$ entonces $\sigma = (a,b,c)^\tau \in N^\tau = N$.

Si τ es impar, $(a,b,c) = (c,b,a)^{-1} = (c,b,a)^{(a,c)}$, y $\sigma = (c,b,a)^{(a,c)\tau}$, donde ahora la permutación $(a,c)\tau$ es par y, como $(c,b,a) = (a,b,c)^{-1} \in N$, concluimos igualmente que $\sigma \in N$.

Por lo tanto N contiene a todos los ciclos de longitud 3, que generan A_n, luego $N = A_n$.

Por lo tanto, basta probar que si N es un subgrupo normal no trivial de A_n entonces contiene un ciclo de longitud 3.

Distinguimos varios casos:

1. Si N contiene una permutación que, descompuesta en ciclos disjuntos, tiene al menos un ciclo de longitud ≥ 4, digamos $\sigma = (123\cdots r)\tau$, entonces

   $$\sigma^{-1}\sigma^{(123)} = (124) \in N.$$

   A partir de aquí podemos suponer que los elementos de N se descomponen en ciclos disjuntos de longitud a lo sumo 3.

2. Si N contiene un elemento que contiene dos ciclos disjuntos de longitud 3, digamos $\sigma = (123)(456)\tau \in N$, entonces

   $$\sigma^{-1}\sigma^{(124)} = (12534) \in N$$

   y se puede aplicar el caso anterior. A partir de aquí podemos suponer que los elementos de N contienen a lo sumo un ciclo de longitud 3.

3. Si N contiene un elemento que contiene un único ciclo de longitud 3, digamos $\sigma = (123)\tau$, donde τ es producto de trasposiciones disjuntas, luego tiene orden 2, entonces

   $$(123)\tau(123)\tau = (132) \in N.$$

4. Finalmente, si N contiene sólo productos de trasposiciones disjuntas, por ejemplo $\sigma = (12)(34)\tau$, entonces

   $$\sigma\sigma^{(123)} = (13)(24) \in N.$$

   Ahora usamos que $n \geq 5$, lo que nos permite considerar

   $$(13)(24)((13)(24))^{(135)} = (153) \in N.$$

El hecho de que A_n es no abeliano para $n \geq 5$ es consecuencia inmediata de que A_n contiene a A_4, que es un grupo no abeliano. ∎

Como primera aplicación:

Teorema 2.23 *Si $n \geq 5$, el único subgrupo normal propio de Σ_n es A_n.*

DEMOSTRACIÓN: Sea $N \trianglelefteq \Sigma_n$. Entonces $N \cap A_n \trianglelefteq A_n$, luego por el teorema anterior tenemos que $N \cap A_n = A_n$ o bien $N \cap A_n = 1$. En el primer caso $A_n \leq N$ y, como $|\Sigma_n : A : n| = 2$, tiene que ser $N = A_n$ o bien $N = \Sigma_n$.

En el segundo caso, o bien $N = 1$, o bien $\Sigma_n = NA_n$ y el teorema 1.37 nos da que $|N||A_n| = |\Sigma_n|$, luego $|N| = 2$, pero entonces[1] $N \leq Z(\Sigma_n) = 1$ y tenemos una contradicción. ∎

Conjugación en A_n Hemos visto que dos permutaciones son conjugadas en Σ_n si y sólo si tienen descomposiciones en ciclos disjuntos del mismo tipo, pero en tal caso no tienen por qué ser conjugadas en A_n. Consideremos, por ejemplo, el ciclo $(1,2,3) \in A_4$, que tiene 8 conjugados en Σ_4, luego su centralizador tiene orden 3, luego

$$C_{\Sigma_4}((1,2,3)) = \langle (1,2,3) \rangle .$$

Como el centralizador consta únicamente de permutaciones pares, resulta que

$$C_{A_4}((1,2,3)) = C_{\Sigma_4}((1,2,3)) \cap A_4 = \langle (1,2,3) \rangle ,$$

pero esto hace que el índice $|A_4 : C_{A_4}((1,2,3))|$ ya no sea 8, sino 4, por lo que concluimos que $(1,2,3)$ tiene únicamente 4 conjugados en A_4. Y lo mismo vale para cualquier otro ciclo de longitud 3, de modo que la clase de conjugación de los 8 ciclos de longitud 3 en Σ_4 se descompone en unión de dos clases de conjugación en A_4, con 4 ciclos cada una. Calculando algunos conjugados podemos ver que estas clases son:

$$\{(1,2,3),(2,1,4),(3,1,4),(4,3,2)\}, \quad \{(3,2,1),(4,1,2),(4,1,3),(2,3,4)\}.$$

Concretamente, vemos que cada ciclo ha dejado de ser conjugado con su inverso. La conjugación $(1,2,3)^{(3,1)} = (3,2,1)$ no puede hacerse con exponente en A_4.

No ocurre lo mismo con la clase de conjugación de $(1,3)(2,4)$, que está formada por 3 permutaciones y, consecuentemente, el centralizador

$$C_{\Sigma_4}((1,3)(2,4)) = \langle (1,2,3,4), (2,4) \rangle$$

tiene orden 8, y hemos visto que es un grupo diédrico. Ahora el centralizador contiene permutaciones impares, por lo que

$$C_{A_4}((1,3)(2,4)) = C_{\Sigma_4}((1,3)(2,4)) \cap A_4 = V_4,$$

pues ciertamente V_4 está en la intersección y ésta no puede ser mayor, ya que entonces sería todo D_8. El efecto es que ahora $|A_4 : C_{A_4}((1,3)(2,4))| = 3$, por lo que $(1,3)(2,4)$ sigue teniendo 3 conjugados en A_4, luego su clase de conjugación en A_4 es la misma que en Σ_4.

Es claro entonces que A_4 tiene 4 clases de conjugación, de cardinales $1,3,4,4$. Las dos primeras son también clases de conjugación en Σ_4 y las dos últimas resultan de la escisión en dos de la clase de conjugación de los ciclos de longitud 3 en Σ_4.

[1] En general, si $N = \{1, n\}$ es un subgrupo normal de un grupo G, tenemos que $n^g = n$ para todo $g \in G$, lo que equivale a que $n \in Z(G)$.

Notemos en general que si $H \leq \Sigma_n$,

$$H/(H \cap A_n) \cong HA_n/A_n \leq \Sigma_n/A_2,$$

el índice $|H : H \cap A_n|$ tiene que ser 1 o 2, luego si $|H|$ es impar tiene que ser $H \cap A_n = H$, es decir, que $H \leq A_n$. Luego las clases de conjugación en Σ_n de las permutaciones de A_n cuyo centralizador en Σ_n tiene orden impar se escinden en dos clases de conjugación en A_n. Por ejemplo, el lector puede comprobar que la tabla siguiente sobre Σ_6 y A_6 es correcta:

σ	$\lvert\mathrm{cl}_{\Sigma_6}(\sigma)\rvert$	$\lvert C_{\Sigma_6}(\sigma)\rvert$	$\lvert C_{A_6}(\sigma)\rvert$	$\lvert\mathrm{cl}_{A_6}(\sigma)\rvert$
1	1	720	360	1
(12)(34)	45	16	8	45
(123)	40	18	8	$20+20$
(123)(456)	40	18	9	$20+20$
(12)(3456)	90	8	4	90
(12345)	144	5	5	$72+72$
(12)	15	48		
(12)(34)(56)	15	48		
(12)(345)	120	6		
(123456)	120	6		

Vemos que en Σ_6 hay 10 clases de conjugación, mientras que en A_6 hay 9.

Por ejemplo, para calcular el número de permutaciones de tipo (12)(34)(56) hacemos

$$\frac{\frac{6\cdot5}{2}\cdot\frac{4\cdot3}{2}\cdot\frac{2\cdot1}{2}}{6} = 15,$$

pues tenemos 6 opciones para elegir el primer índice y 5 para el segundo, pero como (12) = (21), estas 30 opciones dan en realidad 15 trasposiciones. Para elegir la segunda trasposición tenemos 4 opciones para el primer índice y 3 para el segundo, pero nuevamente hay que dividir entre 2, y lo mismo sucede con la tercera. Además, las 90 permutaciones así obtenidas no son distintas, sino que cualquiera de las 6 permutaciones posibles de las tres trasposiciones da lugar a la misma permutación, luego hay que dividir el resultado entre 6.

Para saber si los centralizadores se reducen o no al pasar a A_6 sólo hay que ver si, en caso de tener orden par, contienen alguna permutación impar. Por ejemplo, el centralizador de (123)(456) contiene la permutación impar (14)(25)(36), que intercambia los ciclos sin alterar la permutación, luego su intersección con A_6 tiene la mitad de elementos.

Ejercicio: Construir una tabla análoga para Σ_5 y A_5.

2.4 El teorema de Cayley

En el capítulo anterior hemos definido el grupo Q_8 como un subgrupo de Σ_8 generado por dos permutaciones cuidadosamente elegidas. ¿Por qué precisamente ésas? ¿Cómo puede uno saber que esas permutaciones precisamente generan un subgrupo de orden 8? La respuesta está en el teorema de Cayley,

que vamos a demostrar en esta sección. En realidad demostraremos una versión más general del teorema clásico de Cayley. Para ello necesitamos introducir un concepto:

Definición 2.24 Si G es un grupo y $H \leq G$, el *núcleo normal* de H en G es el subgrupo generado por (la unión de) todos los subgrupos normales de G contenidos en H. Lo representaremos por $\mathrm{nn}_G(H)$.

Notemos que $\mathrm{nn}_G(H) \leq H$ y $\mathrm{nn}_G(H) \trianglelefteq G$. De hecho, es el mayor subgrupo normal de G contenido en H.

En efecto, si $n \in \mathrm{nn}_G(H)$ y $g \in G$, entonces $n = n_1 \cdots n_k$, donde, para cada índice i, existe un subgrupo $N_i \trianglelefteq G$ de modo que $n_i \in N_i \leq H$. Por lo tanto, $n^g = n_1^g \cdots n_k^g$, con $n_i^g \in N_i$, luego $n^g \in \mathrm{nn}_G(H)$.

Hay otra caracterización útil del núcleo normal:

$$\mathrm{nn}_G(H) = \bigcap_{g \in H} H^g.$$

En efecto, como $\mathrm{nn}_G(H) \leq H$, también $\mathrm{nn}_G(H) = \mathrm{nn}_G(H)^g \leq H^g$, luego $\mathrm{nn}_G(H) \leq \bigcap_{g \in H} H^g$. Por otro lado, $\bigcap_{g \in H} H^g \leq H^1 = H$ y, si $u \in G$,

$$\Big(\bigcap_{g \in H} H^g\Big)^u = \bigcap_{g \in H} H^{gu} = \bigcap_{g \in H} H^g,$$

pues, cuando g recorre G, lo mismo le sucede a gu. Esto prueba que la intersección es un subgrupo normal de G contenido en H, luego $\bigcap_{g \in H} H^g \leq \mathrm{nn}_G(H)$ y tenemos la igualdad.

Teorema 2.25 (de Cayley) *Sea G un grupo y $H \leq G$. Sea $\Omega = G/H$ el conjunto de clases de congruencia por la derecha. Entonces G actúa sobre Ω por multiplicación, es decir, $(Hg_1)g_2 = H(g_1g_2)$ y el núcleo de la acción $G \longrightarrow \Sigma_\Omega$ es el núcleo normal de H en G.*

Demostración: Notemos que la definición $(Hg_1)g_2 = H(g_1g_2)$ no depende de la elección del representante de la clase Hg_1, pues si $Hg_1 = Hg_1'$, entonces $g_1 = hg_1'$, para cierto $h \in H$, luego $g_1g_2 = hg_1'g_2$, luego $H(g_1g_2) = H(g_1'g_2)$. Por lo tanto, la acción de G en Ω está bien definida.

Sea $\alpha : G \longrightarrow \Sigma_\Omega$ el homomorfismo asociado a la acción, es decir, el dado por $\alpha_{g_2}(Hg_1) = H(g_1g_2)$. Se cumple que $g_2 \in \mathrm{N}(\alpha)$ si y sólo si, para todo $g_1 \in G$, se cumple que $Hg_1g_2 = Hg_1$, lo que equivale a que $g_1g_2g_1^{-1} \in H$, o también a que $g_2 \in H^{g_1}$, para todo $g_1 \in G$, o también a que $g_2 \in \mathrm{nn}_G(H)$. ∎

Por lo tanto, si $\mathrm{nn}(H) = 1$ (en particular si $H = 1$), tenemos que G es isomorfo a un subgrupo de Σ_Ω. El caso $H = 1$ es el caso clásico del teorema de Cayley, y conviene enunciarlo explícitamente:

Teorema 2.26 (de Cayley) *Todo grupo G actúa sobre sí mismo por multiplicación por la derecha, es decir, tomando $\Omega = G$ y la acción $\Omega \times G \longrightarrow \Omega$ dada por el producto en G. Esta acción determina un monomorfismo $G \longrightarrow \Sigma_G$.*

Así pues, todo grupo G es isomorfo a un subgrupo de Σ_G.

Ejemplos Imaginemos que conocemos la tabla del grupo Q_8:

		1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	1	-1	i	$-i$	j	$-j$	k	$-k$
2	-1	-1	1	$-i$	i	$-j$	j	$-k$	k
3	i	i	$-i$	-1	1	k	$-k$	$-j$	j
4	$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
5	j	j	$-j$	$-k$	k	-1	1	i	$-i$
6	$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
7	k	k	$-k$	j	$-j$	$-i$	i	-1	1
8	$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

si numeramos sus elementos como indica la primera columna de la tabla, entonces la multiplicación por i y por j se corresponden precisamente con las permutaciones

$$i = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ i & -i & -1 & 1 & -k & k & j & -j \\ 3 & 4 & 2 & 1 & 8 & 7 & 5 & 6 \end{pmatrix},$$

$$j = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ j & -j & k & -k & -1 & 1 & -i & i \\ 5 & 6 & 7 & 8 & 2 & 1 & 4 & 3 \end{pmatrix}$$

que tomamos como definición en el capítulo anterior. (Por ejemplo, $j \cdot i = -k$ se corresponde con $i(5) = 8$.) En términos de ciclos disjuntos son

$$i = (1,3,2,4)(5,8,6,7), \qquad j = (1,5,2,6)(3,7,4,8).$$

Así pues, definamos como definamos Q_8, estas permutaciones son las imágenes de los elementos i, j por el monomorfismo dado por el teorema anterior, luego el subgrupo de Σ_8 que generan tenía que ser isomorfo a Q_8.

Del mismo modo podríamos encontrar un subgrupo de Σ_8 isomorfo a D_8, pero podemos encontrar uno en Σ_4 tomando $H = \langle 1, \tau \rangle \leq D_8$, que es un subgrupo con núcleo normal trivial, por lo que el homomorfismo

$$D_8 \longrightarrow \Sigma_{D_8/H} \cong \Sigma_4$$

asociado a la acción de D_8 sobre D_8/H es un monomorfismo. Concretamente,

$$D_8/H = \{H1, H\sigma, H\sigma^2, H\sigma^3\}$$

y la acción es

		σ	τ
1	$H1$	$H\sigma$	$H1$
2	$H\sigma$	$H\sigma^2$	$H\sigma^3$
3	$H\sigma^2$	$H\sigma^3$	$H\sigma^2$
4	$H\sigma^3$	$H1$	$H\sigma$

con lo que σ y τ se corresponden con las permutaciones

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1,2,3,4), \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2,4),$$

que ciertamente generan uno de los tres subgrupos de Σ_4 isomorfos a D_8. ∎

Veamos algunas de aplicaciones, la primera de las cuales generaliza el hecho de que los subgrupos de índice 2 son normales:

Teorema 2.27 *Sea G un grupo finito y H un subgrupo tal que $|G:H| = p$ sea el menor primo que divide a $|G|$. Entonces $H \trianglelefteq G$.*

Demostración: Sea $\Omega = (G/H)_d$ y $\tau : G \longrightarrow \Sigma_\Omega$ el homomorfismo asociado a la acción por multiplicación. Sea $N = \mathrm{N}(\tau) \trianglelefteq G$. Se cumple que $N \leq H \leq G$. Por el teorema de isomorfía G/N es isomorfo a un subgrupo de Σ_Ω, luego $|G:N| \mid p!$, pero también $|G:N| \mid |G|$ y p es el menor primo que divide a $|G|$. Es claro entonces que $|G:N| = p$ (no puede ser $|G:N| = 1$ porque $p = |G:H| \mid |G:N|$). Ahora bien, si $N \leq H \leq G$ y los dos tienen índice p, tiene que ser $H = N \trianglelefteq G$. ∎

La segunda es una condición suficiente para que un grupo tenga un subgrupo de índice 2:

Teorema 2.28 *Todo grupo G de orden $2n$, donde n es impar, tiene un subgrupo de orden 2 y otro de índice 2.*

Demostración: Si G no tuviera elementos de orden 2, podríamos agrupar los elementos no triviales de G en parejas (g, g^{-1}), con lo que (contando el neutro) el grupo G tendría un número impar de elementos.

Ahora consideramos el monomorfismo $G \longrightarrow \Sigma_G \cong \Sigma_{2n}$ dado por el teorema de Cayley. Si $g \in G$ tiene orden 2, su imagen es una permutación que se descompone en producto de n transposiciones (h, hg), luego es una permutación impar. Esto significa que la imagen G^* de G no está contenida en A_{2n}, luego $G^* A_{2n} = \Sigma_{2n}$, luego

$$(2n)! = \frac{2n\,(2n)!/2}{|G^* \cap A_{2n}|},$$

luego $G^* \cap A_{2n}$ es un subgrupo de G^* de orden n, es decir, de índice 2, y $G \cong G^*$ también tendrá un subgrupo de índice 2. ∎

Teorema 2.29 *Un grupo finito simple no abeliano no puede tener subgrupos de índice $2, 3, 4$.*

DEMOSTRACIÓN: Sea G un grupo finito simple no abeliano y supongamos que H es un subgrupo de índice $2, 3, 4$. El homomorfismo $G \longrightarrow \Sigma_{|G:H|}$ dado por el teorema de Cayley tiene que ser un monomorfismo, pues su núcleo es un subgrupo normal contenido en $H < G$. Por lo tanto, G es isomorfo a un subgrupo de Σ_2, Σ_3 o Σ_4, pero ninguno de estos grupos contiene un subgrupo simple no abeliano. ∎

Teorema 2.30 *Si $n \geq 5$, todo subgrupo propio de A_n tiene índice mayor o igual que n.*

DEMOSTRACIÓN: Sea $|A_n : H| = m$, sea $\Omega = (A_n/H)_d$ y $\tau : A_n \longrightarrow \Sigma_\Omega$ el homomorfismo asociado a la acción por multiplicación. Como A_n es simple tiene que ser un monomorfismo, luego $n!/2 \leq m!$, luego $m \leq n$. ∎

2.5 Automorfismos de los grupos simétricos

Hemos visto en 1.31 que, para $n \geq 3$, se cumple que $Z(\Sigma_n) = 1$, lo que nos da un isomorfismo $\Sigma_n \longrightarrow \mathrm{Int}(\Sigma_n) \leq \mathrm{Aut}(\Sigma_n)$. El teorema siguiente nos da una caracterización de los automorfismos internos:

Teorema 2.31 *Un automorfismo $f : \Sigma_n \longrightarrow \Sigma_n$ es interno si y sólo si transforma trasposiciones en trasposiciones.*

DEMOSTRACIÓN: El teorema 2.11 nos da que los automorfismos internos transforman trasposiciones en trasposiciones. Recíprocamente, supongamos que un automorfismo f cumple esta propiedad. Sea $f((1,r)) = (a_r, b_r)$, para $r \geq 2$. Entonces, si $r \geq 3$, tenemos que

$$f((1,2)(1,r)) = (a_2, b_2)(a_r, b_r),$$

pero $(1,2)(1,r) = (1,r,2)$ tiene orden 3, luego las trasposiciones (a_2, b_2) y (a_r, b_r) no pueden ser disjuntas, con lo que, o bien $a_r = a_2, b_2$, o bien $b_r = a_2, b_2$. Cambiando a_r por b_r si es preciso, no perdemos generalidad si suponemos que $a_r = a_2, b_2$. Vamos a probar que, o bien $a_r = a_2$ para todo $r \geq 3$, o bien $a_r = b_2$ para todo $r \geq 3$.

En caso contrario, tendríamos que $a_r = a_2$, $a_s = b_2$ con $2 < r < s$. Como $(1,r)(1,s)$ tiene orden 2, lo mismo debería suceder con

$$f((1,r)(2,s)) = (a_r, b_r)f((1,2)(1,s)(1,2)) = (a_r, b_r)(a_2, b_2)(a_s, b_s)(a_2, b_2) =$$

$$(a_2, b_r)(a_2, b_2)(b_2, b_3)(a_2, b_2) = (a_2, b_r, b_s),$$

pero vemos que la imagen tiene orden 3 y tenemos una contradicción.

Si fuera $a_r = b_2$ para todo $r \geq 3$, cambiando a_2 por b_2 si es preciso, no perdemos generalidad si suponemos que $a_r = a_2$ para todo $r \geq 2$. Equivalentemente, tenemos que $f(1,r) = (a_2, b_r)$, para todo $r \geq 2$.

Como f es biyectiva, esto requiere que todos los b_r sean distintos entre sí y distintos de a_2, luego podemos definir una permutación $x \in \Sigma_n$ mediante $x(1) = a_2$, $x(r) = b_r$, para $r \geq 2$.

Esto hace que $f(1,r) = (a_2, b_r) = (1,r)^x$, luego f coincide con el automorfismo interno determinado por x sobre las trasposiciones $(1,r)$ y, como, por 2.12, éstas generan Σ_n, concluimos que f es dicho automorfismo interno. ∎

Como consecuencia:

Teorema 2.32 *Si $n \neq 2, 6$, entonces* $\mathrm{Aut}(\Sigma_n) = \mathrm{Int}(\Sigma_n) \cong \Sigma_n$.

Demostración: Tomemos $f \in \mathrm{Aut}(\Sigma_n)$. Entonces, $f((1,2))$ tiene orden 2, luego tiene que ser un producto de k trasposiciones, con $2k \leq n$. Pero como f tiene que transformar la clase de conjugación de las trasposiciones en otra clase de conjugación, concluimos que f hace corresponder las trasposiciones con los productos de k trasposiciones, para un mismo k fijo.

Trasposiciones hay $n(n-1)/2$, mientras que productos de k trasposiciones hay

$$\frac{n(n-1)\cdots(n-2k+1)}{2^k k!}.$$

Por lo tanto, se tiene que dar la igualdad

$$\frac{n(n-1)\cdots(n-2k+1)}{2^k k!} = \frac{n(n-1)}{2},$$

que equivale a

$$2^{k-1}k! = (n-2)\cdots(n-2k+1).$$

Como $2k \leq n$, en particular

$$2^{k-1}k! \geq (2k-2)\cdots 3\cdot 2\cdot 1 = (2k-2)!$$

Ahora, una simple inducción prueba que si $k \geq 4$ se cumple $2^{k-1}k! < (2k-2)!$ En efecto, se cumple para $k = 4$ y, si vale para k, tenemos que

$$(2(k+1)-2)! = (2k)! = 2k(2k-1)(2k-2)! > 2(k+1)2^{k-1}k! = 2^k(k+1)!$$

Por lo tanto, para que se dé la igualdad requerida, tiene que ser $k = 1, 2, 3$.

Si $k = 2$, la igualdad es $(n-2)(n-3) = 4$, lo cual no se cumple para ningún valor de n. Si $k = 3$ la igualdad es $(n-2)(n-3)(n-4)(n-5) = 24$, pero $6 = 2k \leq n$ y si $n > 6$ el miembro izquierdo es mayor que $5\cdot 4\cdot 3\cdot 2 = 120$, luego no se puede dar la igualdad. Como hemos exceptuado $n = 6$, la única posibilidad es $k = 1$, en cuyo caso f es interno por el teorema anterior. ∎

La situación en el caso $n = 2$ es obvia: tenemos que $\Sigma_2 \cong C_2$, por lo que $\mathrm{Aut}(\Sigma_2) = 1$. Sin embargo, el caso peculiar es $n = 6$, pues en este caso tenemos que $\mathrm{Int}(\Sigma_6) \cong \Sigma_6$ y el teorema anterior abre la posibilidad a que Σ_6 tenga automorfismos no internos. Vamos a ver que así es, para lo cual nos apoyaremos en el hecho siguiente:

Teorema 2.33 *Σ_6 contiene un subgrupo transitivo isomorfo a Σ_5.*

DEMOSTRACIÓN: Consideramos el conjunto Ω de los subgrupos de orden 5 de Σ_5. Puesto que hay 24 ciclos de longitud 5, cada subgrupo tiene 4 de ellos y dos subgrupos de orden 5 tienen intersección trivial, concluimos que $|\Omega| = 6$. El grupo Σ_5 actúa sobre Ω por conjugación, y el teorema 2.11 implica que la acción es transitiva. Tenemos entonces un homomorfismo de grupos $\rho : \Sigma_5 \longrightarrow \Sigma_6$ cuya imagen es transitiva, y tiene que ser un monomorfismo, pues su núcleo N no puede ser ni A_5 ni Σ_5 (si fuera A_5 tendríamos que Σ_5/A_5 sería un grupo de orden 2 actuando transitivamente sobre un conjunto de 6 elementos, lo cual es absurdo). ∎

Sea ahora $K \leq \Sigma_6$ el subgrupo dado por el teorema anterior y consideremos la acción de Σ_6 sobre $\Omega = (\Sigma_6/K)_d$ por multiplicación. Ésta determina un homomorfismo $\tau : \Sigma_6 \longrightarrow \Sigma_\Omega \cong \Sigma_6$, que es un automorfismo por 2.30. Vamos a probar que no es un automorfismo interno.

Más precisamente, la tabla siguiente muestra representantes de las distintas clases de conjugación no triviales de Σ_6 junto con su número de elementos, y vamos a probar que τ intercambia las clases que están en el mismo recuadro y deja fijas las que están en solas en su recuadro.

$(1,2,3)(4,5)$	120	$(1,2,3)$	40	$(1,2)$	15
$(1,2,3,4,5,6)$	120	$(1,2,3)(4,5,6)$	40	$(1,2)(3,4)(5,6)$	15
$(1,2,3,4)(5,6)$	90	$(1,2,3,4)$	90		
$(1,2)(3,4)$	45	$(1,2,3,4,5)$	144		

Para ello sea $\sigma = (1,2,3)(4,5)$ o bien $\sigma = (1,2,3)$ y supongamos que $\tau(\sigma)$ es del mismo tipo. En ambos casos esto implica que $\tau(\sigma)$ tiene un punto fijo, lo que a su vez se interpreta como que existe un $\xi \in \Sigma_6$ tal que $K\xi^{-1}\sigma = K\xi^{-1}$, luego $\sigma^\xi \in K$, luego existe un $\sigma' \in \Sigma_5$ tal que $\rho(\sigma') = \sigma^\xi$.

El hecho de que $\rho(\sigma')$ tenga un punto fijo en Σ_6 se interpreta como que σ', respecto de la acción por conjugación de Σ_5 sobre sus subgrupos de orden 5, fija a uno de ellos, digamos P, de modo que $P^{\sigma'} = P$. El orden de σ' es el mismo que el de σ (es decir, 6 en el primer caso y 3 en el segundo), pero en el primer caso podemos cambiar σ' por σ'^2 y así en ambos casos tenemos un $\sigma' \in \Sigma_5$ de orden 3 que cumple $P^{\sigma'} = P$.

Esto implica que la conjugación por σ' es un automorfismo de P de orden divisor de 3, pero $\mathrm{Aut}(P) \cong C_4$, luego tiene que ser la identidad, luego, si μ es un ciclo de longitud 5 que genera P, tenemos que $\sigma' \in C_{\Sigma_5}(\mu)$, pero esto es imposible, porque μ tiene 24 conjugados en Σ_5, luego $|C_{\Sigma_5}(\mu)| = 5$ y así el centralizador no puede tener elementos de orden 3.

Con esto hemos probado que τ intercambia las clases de conjugación de los dos primeros recuadros de la tabla. Esto ya implica que no es un automorfismo interno de Σ_6, y entonces el teorema 2.31 nos da que también intercambia las clases de conjugación del tercer recuadro. Obviamente tiene que fijar a las clases de la última fila de la tabla anterior, pues no hay otras del mismo cardinal con las que se puedan intercambiar, y sólo falta probar que fija las dos clases de conjugación de la penúltima fila, en lugar de intercambiarlas. Ello se debe a que una está formada por permutaciones pares y la otra por permutaciones impares,

mientras que τ conserva la paridad (porque transforma las trasposiciones en permutaciones impares). Con esto casi hemos probado el teorema siguiente:

Teorema 2.34 $|\operatorname{Aut}(\Sigma_6) : \operatorname{Int}(\Sigma_6)| = 2$, *luego* $|\operatorname{Aut}(\Sigma_6)| = 1\,140$.

DEMOSTRACIÓN: Hemos probado que $\operatorname{Int}(\Sigma_6) < \operatorname{Aut}(\Sigma_6)$, y en la demostración de 2.32 hemos visto que cualquier automorfismo de Σ_6 que no sea interno transforma las trasposiciones en productos de tres trasposiciones, luego si $f, g \in \operatorname{Aut}(\Sigma_6)$ no son internos, la composición fg^{-1} transforma trasposiciones en trasposiciones, luego es un automorfismo interno por el teorema 2.31. Esto prueba que $\operatorname{Aut}(\Sigma_6)/\operatorname{Int}(\Sigma_6) \cong C_2$. ∎

En particular, todo $f \in \operatorname{Aut}(\Sigma_6)$ que no sea un automorfismo interno es de la forma $f = \tau g$, donde g es un automorfismo interno, y podemos concluir que f transforma las trasposiciones en productos de tres trasposiciones y los ciclos de longitud 3 en productos de dos ciclos de longitud 3.

Así pues Σ_6 es el único grupo simétrico no abeliano que tiene automorfismos externos, o que no es isomorfo a su grupo de automorfismos.

Veamos ahora que con A_n tenemos una situación similar. Si $n \geq 4$, como $Z(A_n) = 1$, tenemos igualmente el isomorfismo $A_n \longrightarrow \operatorname{Int}(A_n)$, pero ahora, como $A_n \trianglelefteq \Sigma_n$, cada $\sigma \in \Sigma_n$ induce un automorfismo de A_n por conjugación, no necesariamente interno.

Tenemos, pues, un homomorfismo $\Sigma_n \longrightarrow \operatorname{Aut}(\Sigma_n) \longrightarrow \operatorname{Aut}(A_n)$ que es inyectivo (para $n \geq 4$) pues su núcleo N tiene que cumplir $N \cap A_n = 1$, lo que es imposible para $n \geq 5$ por 2.23, y para $n = 4$ el grupo N tendría que tener orden 2 y estar generado por una permutación impar, luego tendría que ser una trasposición, pero los subgrupos generados por trasposiciones no son normales.

Teorema 2.35 *Un automorfismo $f : A_n \longrightarrow A_n$ (con $n \geq 3$) es la restricción de un automorfismo interno de Σ_n si y sólo si transforma ciclos de longitud* 3 *en ciclos de longitud* 3.

DEMOSTRACIÓN: Obviamente las restricciones de automorfismos internos transforman ciclos en ciclos de la misma longitud. Supongamos que f tiene esta propiedad y llamemos $u_i = (1, 2, i)$, $v_i = f(u_i)$, para $i \geq 3$.

Si $i \neq j$, entonces $u_i u_j = (1, 2, i)(1, 2, j) = (1, j)(2, i)$, que tiene orden 2, luego $v_i v_j$ también tiene orden 2. Observemos ahora que (si letras distintas representan índices distintos):

1. $(x, y, z)(x', y', z')$ tiene orden 3.
2. $(x, y, z)(x', y', z) = (x, y, x', y', z)$ tiene orden 5.
3. $(x, y, z)(x, y, z') = (x, z')(y, z)$ tiene orden 2.
4. $(x, y, z)(y, x, z') = (y, z, z')$ tiene orden 3.
5. $(x, y, z)(x, y, z) = (z, y, x)$ tiene orden 3.
6. $(x, y, z)(x, z, y) = 1$ tiene orden 1.

Por lo tanto, v_3v_4 tienen que estar en el caso 3., es decir, $v_3 = (a_1, a_2, c)$, $v_4 = (a_1, a_2, d)$. Supongamos ahora que, para un $i \geq 5$, se cumpliera que v_i fija a a_1. Entonces, com v_3v_i tiene orden 2, tendría que ser $v_i = (a_2, c, x)$ y, como v_4v_i tiene orden 2, tendría que ser $v_i = (a_2, d, x')$, lo cual es imposible.

Así pues, v_i no fija a a_1, e igualmente se concluye que no fija a a_2, luego, para que v_3v_i tenga orden 2, tiene que ser $v_i = (a_1, a_2, a_i)$. Como f es biyectiva, los a_i tienen que ser distintos entre sí, por lo que podemos definir $x \in \Sigma_n$ mediante $x(i) = a_i$, y entonces

$$u_i^x = (1, 2, i)^x = (a_1, a_2, a_i) = v_i = f(u_i),$$

luego f coincide con la restricción del automorfismo interno de Σ_n determinado por x sobre todos los ciclos $(1, 2, i)$ y, como, por 2.19 estos ciclos generan A_n, tenemos la conclusión. ∎

Teorema 2.36 *Si $n \neq 2, 3, 6$, entonces* $\mathrm{Aut}(A_n) \cong \mathrm{Aut}(\Sigma_n) \cong \Sigma_n$.

Demostración: Si $f \in \mathrm{Aut}(A_n)$, tenemos que $f((1, 2, 3))$ tiene orden 3, luego tiene que ser producto de k ciclos de longitud 3, con $3k \leq n$. En particular, si $n = 4$ tiene que ser $k = 1$ y f es la restricción de un automorfismo interno de Σ_n por el teorema anterior. Si $n \geq 6$, como f transforma clases de conjugación en clases de conjugación, tiene que transformar cada ciclo de longitud 3 en un producto de k ciclos de longitud 3. Al igualar el número de permutaciones de cada tipo obtenemos

$$\frac{n(n-1)\cdots(n-3k+1)}{3^k k!} = \frac{n(n-1)(n-2)}{3},$$

que equivale a

$$3^{k-1}k! = (n-3)\cdots(n-3k+1).$$

Como $3k \leq n$, tenemos que

$$3^{k-1}k! \geq (3k-3)!$$

pero para $k \geq 3$ se cumple la desigualdad opuesta. Razonando inductivamente, vemos que se cumple para $k = 3$ y, si $3^{k-1}k! < (3k-3)!$, entonces

$$(3(k+1)-3)! = (3k)! = 3k(3k-1)(3k-2)(3k-3)! \geq 3(k+1)(3k-2)!$$

$$> 3(k+1)3^{k-1}k! = 3^k(k+1)!$$

Por consiguiente, tiene que ser $k = 1, 2$. Si $k = 2$ tenemos

$$6 = (n-3)(n-4)(n-5),$$

lo cual es imposible si $n \geq 7$, pues entonces el miembro derecho es mayor o igual que $4 \cdot 3 \cdot 2 = 24$. Como hemos exceptuado $n = 6$, tiene que ser $k = 1$, y el teorema anterior nos da que f es la restricción de un automorfismo interno de Σ_n, luego el monomorfismo $\Sigma_n \longrightarrow \mathrm{Aut}(A_n)$ es un isomorfismo. ∎

Como $A_2 \cong C_2$ y $A_3 \cong C_3$, es claro que $\mathrm{Aut}(A_2) = 1$ y $\mathrm{Aut}(A_3) \cong C_2$.

En el caso excepcional $n = 6$, seguimos teniendo un monomorfismo

$$\Sigma_6 \longrightarrow \mathrm{Aut}(\Sigma_6) \longrightarrow \mathrm{Aut}(A_6)$$

que nos permite identificar a $\Sigma_6 \leq \mathrm{Aut}(A_6)$ con el grupo de los automorfismos de A_6 determinados por la conjugación por un elemento de Σ_6. Ahora bien, si $f \in \mathrm{Aut}(\Sigma_6)$ no es interno, hemos probado que transforma ciclos de longitud 3 en productos de dos ciclos de longitud 3, luego la restricción $f|_{A_6}$ no es la restricción de un automorfismo interno de Σ_6.

Por otro lado, si $f, g \in \mathrm{Aut}(A_6)$ no están en Σ_6, entonces fg^{-1} transforma ciclos de longitud 3 en ciclos de longitud 3, luego $fg^{-1} \in \Sigma_6$, luego se cumple que $|\mathrm{Aut}(A_6) : \Sigma_6| = 2$, luego $|\mathrm{Aut}(A_6)| = 2 \cdot 6!$.

El homomorfismo $\mathrm{Aut}(\Sigma_6) \longrightarrow \mathrm{Aut}(A_6)$ determinado por la restricción es suprayectivo, pues su imagen contiene por una parte a Σ_6, pero acabamos de ver que también contiene automorfismos que no están en Σ_6 y, teniendo en cuenta que $|\mathrm{Aut}(A_6) : \Sigma_6| = 2$, la imagen tiene que ser todo $\mathrm{Aut}(A_6)$. Como ambos grupos tienen el mismo orden, en realidad tenemos un isomorfismo:

Teorema 2.37 *La restricción induce un isomorfismo* $\mathrm{Aut}(\Sigma_6) \cong \mathrm{Aut}(A_6)$.

En particular, $\mathrm{Int}(A_6) \cong A_6 < \Sigma_6 < \mathrm{Aut}(A_6)$, por lo que

$$|\mathrm{Aut}(A_6) : \mathrm{Int}(A_6)| = 4.$$

Así pues, salvo los casos triviales de A_2 y A_3, sucede que A_6 es el único grupo alternado A_n que tiene automorfismos no inducidos por la conjugación desde Σ_n. Véase el teorema 7.41 para más detalles sobre la estructura de este grupo de automorfismos.

2.6 Grupos de simetrías de polígonos y poliedros regulares

Polígonos Sea E un plano euclídeo (sobre $\mathbb{R}$), y consideremos el grupo $\mathrm{Is}(E)$ de todas las isometrías de E (que claramente es un grupo con la composición de aplicaciones). De acuerdo con el teorema [G 3.27], los elementos de E son las biyecciones afines que conservan las distancias entre puntos.

El grupo $\mathrm{Is}(E)$ actúa sobre los puntos de E y, para cada subconjunto $V \subset E$, podemos considerar el subgrupo $\mathrm{Is}_V(E)$ formado por las isometrías $f \in \mathrm{Is}(E)$ que cumplen $f[V] = V$, es decir, que transforman los puntos de V en los puntos de V.

Concretamente, vamos a estudiar el grupo de las isometrías que fijan al conjunto V de los vértices de un polígono regular de n lados, que es lo que se conoce como el grupo de las simetrías del polígono (puede probarse —y es intuitivamente evidente— que las isometrías que fijan los vértices de un polígono regular P coinciden con las isometrías que fijan a P, es decir, las que cumplen $f[P] = P$, pero en este contexto nos basta tomar como definición de $\mathrm{Is}_V(E)$ que sus elementos fijan a los vértices).

Los vértices de un polígono regular están contenidos en una circunferencia de centro O, de modo que O es el único punto que equidista de todos los puntos de V. Por lo tanto, si $f \in \mathrm{Is}_V(E)$, el punto $f(O)$ también equidista de todos los puntos de V, luego tiene que ser $f(O) = O$.

Así pues, $\mathrm{Is}_V(E) \leq \mathrm{Is}_O(E)$, es decir, el grupo de simetrías de un polígono regular está contenido en el grupo de las isometrías que fijan a su centro.

En la discusión tras [G 3.40] hemos probado que todo elemento de $\mathrm{Is}_O(E)$ es una simetría axial o un giro, así como que los giros forman un subgrupo $\mathrm{Is}_O^+(E) \leq \mathrm{Is}_O(E)$.

Observamos ahora que un giro (de centro O) distinto de la identidad no fija a ningún punto más que a O, mientras que una simetría axial fija a los puntos de una recta que pasa por O, luego fija únicamente dos puntos diametralmente opuestos de la circunferencia circunscrita al polígono, luego a lo sumo fijará a dos vértices del polígono. Como tiene que haber al menos tres vértices, concluimos que si una simetría fija a todos los vértices, es que es la identidad. Esto significa que la restricción determina un monomorfismo de grupos

$$\mathrm{Is}_V(E) \longrightarrow \Sigma_V \cong \Sigma_n,$$

es decir, que podemos ver a los elementos de $\mathrm{Is}_V(E)$ como permutaciones de V en lugar de como isometrías del plano. Más aún, ahora es fácil concluir:

> *Si (v_1, v_2) y (w_1, w_2) son los extremos de dos lados de un polígono regular cuyo conjunto de vértices es V, existe una única simetría $f \in \mathrm{Is}_V(E)$ que cumple $f(v_i) = w_i$.*

En efecto, es claro que podemos tomar un giro que cumpla $f(v_1) = w_1$, y entonces $f(v_1)$ es uno de los dos vértices contiguos a w_1, es decir, uno de los dos vértices cuya distancia a w_1 es la longitud del lado del polígono. Si $f(v_1) \neq w_1$, basta componer f con la simetría respecto de la recta que pasa por w_1 y O (que fija a w_1) para obtener una nueva simetría g que cumple $g(v_1) = w_1$ y también $g(v_2) = w_2$.

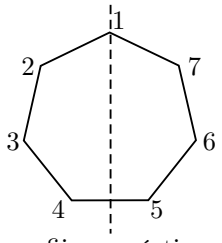
Esto prueba la existencia, y la unicidad se debe a que si f y g cumplen lo mismo, entonces $(f \circ g^{-1})(v_i) = v_i$, pero v_1 y v_2 son puntos de la circunferencia circunscrita no diametralmente opuestos, y ninguna isometría de $\mathrm{Is}_O(E)$ distinta de la identidad puede fijar a dos puntos en esas condiciones, luego $f \circ g^{-1} = 1$, luego $f = g$.

Como conclusión, si el polígono tiene n vértices, se cumple que $|\mathrm{Is}_V(E)| = 2n$.

En efecto, fijado un lado del polígono, digamos de extremos (v_1, v_2), para cada uno de los n lados del polígono, digamos de extremos (w_1, w_2), existen exactamente dos simetrías que transforman un lado en el otro, una que cumple $f(v_1) = w_1$ y otra que cumple $f(v_1) = w_2$. Por lo tanto, un polígono regular de n lados tiene exactamente $2n$ simetrías, y ahora es fácil encontrarlas todas.

Por una parte, si numeramos los n vértices del polígono consecutivamente (por ejemplo en sentido antihorario), el giro σ de amplitud $2\pi/n$ en sentido

antihorario permuta los vértices cíclicamente, luego $\sigma \in \mathrm{Is}_V(E)$ y, visto como permutación, es $\sigma = (1, 2, \ldots, n)$. Por lo tanto, $\langle\sigma\rangle$ es un subgrupo cíclico de $\mathrm{Is}_V(E)$ de orden n. Si n es impar, $\mathrm{Is}_V(E)$ contiene también las simetrías respecto de las n rectas que pasan por O y por cada uno de los vértices.

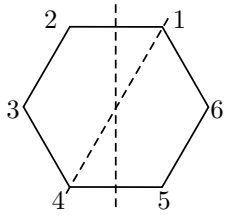


En el caso de un heptágono, si llamamos τ a la simetría respecto del eje que pasa por el vértice 1, vista como permutación, es

$$\tau = (2, 7)(3, 6)(4, 5).$$

En general, para un polígono de un número impar n de lados, cada simetría se corresponde con una permutación que fija un vértice e intercambia los otros por pares, concretamente una de ellas es

$$\tau = (2, n)(3, n-1)\cdots((n+1)/2, (n+3)/2).$$



Si n es par tenemos dos clases de simetrías: aquellas cuyo eje pasa por dos vértices y las que pasan por los puntos medios de dos lados opuestos. La figura muestra el caso de un hexágono. La simetría que fija los vértices 1 y 4 se corresponde con la permutación

$$\tau = (2, 6)(3, 5),$$

mientras que la que pasa por los puntos medios de los lados 12 y 45 se corresponde con

$$\tau' = (1, 2)(3, 6)(4, 5).$$

En general, una simetría en $\mathrm{Is}_V(E)$ cuando n es par (concretamente, la que fija a los vértices 1 y $n/2 + 1$) es

$$\tau = (2, n)(3, n-1)\cdots(n/2, n/2+2).$$

En ambos casos se cumple que $\sigma^\tau = \sigma^{-1}$. En efecto, como $\langle\sigma\rangle$ es un subgrupo normal (porque tiene índice 2) tiene que ser $\sigma^\tau = \sigma^i$, para cierto exponente i, pero $\sigma^\tau(1) = \tau(\sigma(1)) = \tau(2) = n$ y un elemento de $\langle\sigma\rangle$ está completamente determinado por la imagen de 1, luego tiene que ser $\sigma^\tau = \sigma^{-1}$.

Trivialmente $\mathrm{Is}_V(E) = \langle\sigma, \tau\rangle$, pues $\langle\sigma\rangle \cap \langle\tau\rangle = 1$, luego $|\langle\sigma, \tau\rangle| = 2n$, luego se da la igualdad. En virtud del teorema 1.38 concluimos que $\mathrm{Is}_V(E) \cong D_{2n}$. En resumen, hemos obtenido una representación geométrica de los grupos diédricos:

Teorema 2.38 *El grupo de las simetrías de un polígono regular de n lados (es decir, el grupo de las isometrías del plano que dejan invariante al conjunto de sus vértices) es isomorfo a D_{2n}. El subgrupo cíclico de orden n de D_{2n} se corresponde con el grupo de los giros y los otros n elementos se corresponden con las simetrías axiales.*

Si pensamos en un polígono regular de n lados hecho "de cartulina" y situado sobre una mesa, los movimientos que podemos hacer para intercambiar sus vértices sin levantarlo de la mesa forman un grupo cíclico de orden n, mientras que

si admitimos la posibilidad de voltear el polígono sobre la mesa intercambiando sus dos caras tenemos otras n simetrías axiales que extienden el grupo cíclico hasta un grupo diédrico. De ahí el nombre de "diédrico" (gr. = dos caras).

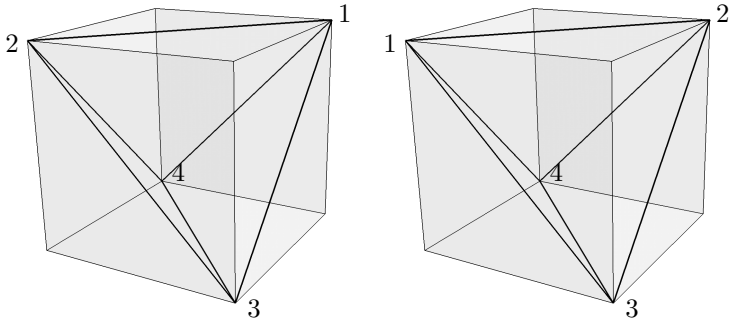
Isometrías del espacio A partir de aquí consideramos un espacio euclídeo tridimensional E y su grupo de isometrías $\mathrm{Is}(E)$. En la sección 5.5 de [G] veremos que las hay de dos tipos, "directas" e "inversas", de modo que las isometrías directas forman un subgrupo $\mathrm{Is}^+(E)$.

Una característica que las distingue es que una isometría directa puede efectuarse gradualmente. Por ejemplo, en el plano un giro es una isometría directa, y, en efecto, para girar 90 grados un cuadrado, podemos hacerlo poco a poco, hasta que cada vértice llega a ocupar la posición que ocupaba al principio uno de sus vértices adyacentes. En cambio, no es posible aplicar gradualmente una simetría axial a un cuadrado sin "sacarlo del plano". Las simetrías axiales son inversas y "dejan una huella" en las figuras a las que se aplican, y es que invierten su orientación.

$$\begin{array}{ccc} 2 & - & 1 \\ | & & | \\ 3 & - & 4 \end{array} \qquad \begin{array}{ccc} 2 & - & 3 \\ | & & | \\ 1 & - & 4 \end{array}$$

Por ejemplo, si tenemos un cuadrado de cartón con sus vértices numerados como muestra la figura de la izquierda y luego pasa a estar como indica la figura de la derecha, podemos estar seguros de que se le ha aplicado una isometría inversa, porque al principio los vértices estaban numerados en sentido antihorario, mientras que al final lo están en sentido horario. Los giros conservan la orientación, mientras que las simetrías la invierten.

Ahora bien, una simetría axial de un plano puede realizarse de forma continua "saliendo del plano", es decir, girando 180° respecto del eje de simetría, lo cual puede hacerse paulatinamente. Las isometrías inversas planas pueden realizarse mediante isometrías directas espaciales. Lo mismo sucede si aumentamos una dimensión. Por ejemplo, consideremos un tetraedro regular, que podemos construir sin más que tomar cuatro vértices de un cubo opuestos por diagonales de sus caras:



Es imposible mover el tetraedro (o el cubo) de la izquierda para disponerlo como muestra la figura de la derecha. La figura de la derecha resulta de aplicar la simetría especular respecto del plano vertical que pasa por los vértices 3 y 4, de modo que la segunda figura es el reflejo en un espejo de la primera, y todos sabemos que las imágenes de los espejos no son iguales a las figuras originales. Una forma de distinguirlas es observar que, si miramos la cara 234 desde el vértice 1, vemos los vértices ordenados en sentido antihorario en la figura de la izquierda, pero en sentido horario en la figura de la derecha, y este cambio no puede realizarse moviendo la figura. Para realizar este cambio de forma continua, paulatina, sería necesario girar la figura 180° en una cuarta dimensión.

No necesitamos los detalles de la discusión precedente, sino que la hemos presentado para explicar que vamos a considerar únicamente el subgrupo $\mathrm{Is}^+(E)$ de las isometrías directas del espacio, las que se conocen como "movimientos", porque son las que pueden realizarse moviendo las figuras (sin reflejarlas en un espejo).

Sí que vamos a necesitar un hecho no trivial descubierto por Euler, y es que el grupo $\mathrm{Is}^+_O(E)$ formado por todas las isometrías directas del espacio que dejan fijo a un punto O está formado únicamente por los giros respecto de rectas que pasan por O. De hecho, ni siquiera es evidente que al componer dos giros respecto de dos rectas distintas que pasan por O la isometría resultante es un giro respecto de una tercera recta que pasa por O. Esto lo demostraremos en [G 4.14], si bien será inmediato tras los resultados de la sección [G 5.5], donde clasificaremos las isometrías de un espacio euclídeo.

De momento, podemos considerar que $\mathrm{Is}^+_O(E)$ es, por definición, el conjunto de todos los giros respecto de un eje que pasa por O, lo que supone admitir [G 4.14] (es decir, que tales giros forman un grupo), y conviene tener presente que, según veremos, se trata en realidad del grupo de todos los movimientos (isometrías directas) que fijan el punto O.

Las simetrías del tetraedro Sea ahora V el conjunto de los vértices de un tetraedro regular. Es fácil ver que un cubo está inscrito en una esfera, cuyo centro O es el único punto que equidista de sus vértices, y lo mismo vale para el tetraedro, de modo que O es el único punto que equidista de todos los puntos de V. Por lo tanto, si $f \in \mathrm{Is}(E)$ cumple $f[V] = V$, entonces $f(O)$ equidista de todos los puntos de V, luego tiene que ser $f(O) = O$. Esto significa que el grupo $\mathrm{Is}^+_V(E)$ de las simetrías (directas) de un tetraedro regular, formado por las isometrías directas que fijan sus vértices es un subgrupo de $\mathrm{Is}^+_O(E)$, luego está formado por giros respecto de ejes que pasan por O.

Esto se traduce en que cada elemento de $\mathrm{Is}^+_V(E)$ fija a lo sumo un vértice del tetraedro (ya que no hay vértices diagonalmente opuestos respecto de O). En particular, si un elemento de $\mathrm{Is}^+_V(E)$ fija a dos vértices del tetraedro, es la identidad. A su vez, esto implica que la restricción a V induce un monomorfismo de grupos

$$\mathrm{Is}^+_V(E) \longrightarrow \Sigma_V \cong \Sigma_4$$

que nos permite considerar las simetrías del tetraedro como permutaciones de sus vértices, en lugar de como isometrías del espacio.

Como en el caso de los polígonos, ahora podemos probar que existe una única simetría que transforma cualquier arista dada del tetraedro en cualquier otra (eligiendo cómo se corresponden sus vértices), por lo que de hecho hay exactamente dos simetrías que transforman una arista en otra.

En efecto, es claro que un giro de 120° respecto de la recta que pasa por un vértice permuta cíclicamente los otros tres, luego siempre hay uno que lleva un vértice dado a otro cualquiera. Así podemos hacer que un extremo de una arista se corresponda con otro extremo de otra cualquiera, y aplicando a continuación un giro respecto del eje que pasa por dicho extremo, podemos hacer que la primera arista se transforme en la segunda.

Esto se traduce en que, como cada arista puede llevarse de dos formas distintas a cualquiera de las 6 que tiene el tetraedro, $|\mathrm{Is}_V^+(E)| = 12$, pero, por 2.20, el único subgrupo de Σ_4 de orden 12 es A_4, por lo tanto:

> *El grupo de las simetrías (directas) de un tetraedro regular es isomorfo a A_4.*

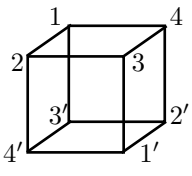
Ahora es fácil describirlas: los 8 ciclos de longitud 3 de A_4 se corresponden con los giros de 120° respecto de los ejes que pasan por O y un vértice (que lo fijan mientras permutan cíclicamente los otros tres), y las tres permutaciones como $(1,2)(3,4)$ intercambian los vértices dos a dos, por lo que son giros de 180° respecto de rectas que pasan por los puntos medios de las dos aristas cuyos extremos se intercambian. ∎

Las simetrías del cubo Si ahora V es el conjunto de los vértices de un cubo, como en el caso anterior podemos justificar que $\mathrm{Is}_V^+(E) \leq \mathrm{Is}_O^+(E)$, así como que un cubo puede girarse de forma única de modo que cualquier par de vértices adyacentes se correspondan con cualquier otro par. Por lo tanto, el número de simetrías es el doble del número de aristas, es decir, que $|\mathrm{Is}_V^+(E)| = 24$.

Razonando como antes, podríamos identificar el grupo $\mathrm{Is}_V^+(E)$ con un subgrupo de Σ_8, pero podemos hacer algo mejor. Para ello llamamos Ω al conjunto de los 4 pares de vértices opuestos del cubo. Como cada isometría tiene que transformar vértices opuestos en vértices opuestos, tenemos un homomorfismo

$$\mathrm{Is}_V^+(E) \longrightarrow \Sigma_\Omega \cong \Sigma_4.$$

Si probamos que es inyectivo, de hecho será un isomorfismo.

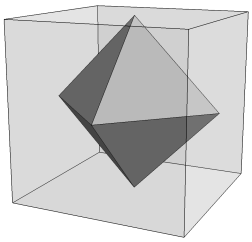


Ahora bien, supongamos que una isometría $f \in \mathrm{Is}_V^+(E)$ fija los cuatro pares de vértices opuestos y no es la identidad. Supongamos que, por ejemplo, $f(1) = 1'$. Entonces $f(2)$ tiene que ser un vértice adyacente a $1'$, luego tiene que ser $f(2) = 2'$, pero sabemos que sólo hay un giro que cumple $f(1) = 1'$ y $f(2) = 2'$, y es el giro de 180° respecto al eje que pasa por los puntos medios de las aristas 34 y $3'4'$, el cual cumple $f(3) = 4$, luego no fija los pares $\{3, 3'\}$ y $\{4, 4'\}$ de Ω, en contra de lo supuesto. Así pues:

El grupo de las simetrías (directas) de un cubo es isomorfo a Σ_4.

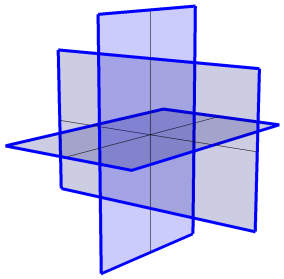
Las simetrías (aparte de la identidad) son de tres tipos:

1. Los 8 ciclos de longitud 3 se corresponden con los giros de 120° alrededor de los cuatro ejes que unen cada par de vértices opuestos.
2. Los 6 ciclos de longitud 4 se corresponden con los giros de 90° alrededor de los tres ejes que pasan por los centros de cada par de caras opuestas.
3. Las 3 permutaciones de tipo $(a, b)(c, d)$ (los cuadrados de las anteriores) se corresponden con los giros de 180° alrededor de los mismos ejes.
4. Las 6 trasposiciones se corresponden con los giros de 180° alrededor de los ejes que pasan por los centros de cada par de aristas opuestas.



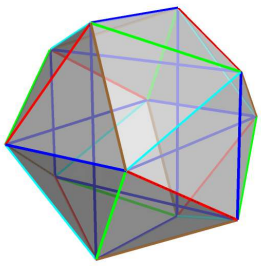
Nota Los centros de las caras de un cubo son los vértices de un octaedro regular y, recíprocamente, los centros de las caras de un octaedro regular son los vértices de un cubo. Esto se expresa diciendo que el octaedro es el poliedro dual del cubo y viceversa. De aquí se desprende fácilmente que el grupo de simetrías (directas) de un octaedro es el mismo que el del cubo. ∎

Las simetrías del icosaedro Un icosaedro regular es un poliedro regular con 12 vértices y 20 caras triangulares. Una forma de probar su existencia es tomar como vértices los de los tres rectángulos que muestra la figura:



Los lados menores miden 1 unidad y los mayores miden $\phi = (1 + \sqrt{5})/2$ (el número áureo). Observemos que los doce vértices están a la misma distancia del punto O en el que se cortan los tres rectángulos, luego están inscritos en una esfera de centro O.

Conviene recordar de la sección [IGE 3.4] que las diagonales de un pentágono regular están en proporción áurea con sus lados. Así, no es difícil concluir que los cinco vértices más cercanos a cada uno de ellos forman un pentágono regular de arista unitaria.



La figura siguiente muestra el poliedro que resulta de unir cada vértice con los cinco vértices más cercanos. Hemos mantenido el color azul en las seis aristas que forman parte de los tres rectángulos de partida. Si tomamos cualquier arista no pintada de azul, por ejemplo una de las pintadas de rojo, podemos pintar del mismo color las otras cinco aristas que están en el plano que pasa por ella y por O y en los dos planos perpendiculares por O.

De este modo, las 30 aristas del icosaedro quedan divididas en 5 grupos de 6 aristas del mismo color, de modo que a cada vértice concurren cinco aristas de colores distintos.

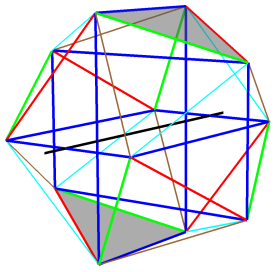
Si llamamos V al conjunto de los vértices del icosaedro, el argumento habitual muestra que $\mathrm{Is}_V^+(E) \leq \mathrm{Is}_O^+(E)$, así como que entre las simetrías del icosaedro se encuentran los giros de 72° alrededor de cada eje que pasa por dos vértices opuestos, y usando estos giros es claro que existe una única simetría que transforma cualquier par de vértices adyacentes (v_1, v_2) en cualquier otro (w_1, w_2): en primer lugar movemos el icosaedro usando los giros mencionados para hacer corresponder v_1 con w_1, y luego, mediante un giro alrededor de un eje que pase por w_1, podemos hacer que v_2 se corresponda con w_2. La unicidad se debe, como es habitual, a que ningún giro que fije a O y que no sea la identidad puede fijar a dos vértices adyacentes de un poliedro (pues no son diametralmente opuestos). Esto basta para concluir que $|\mathrm{Is}_V^+(E)| = 60$.

Llamemos ahora Ω a los cinco conjuntos de aristas que hemos pintado del mismo color. Es claro que si una simetría del icosaedro transforma una arista de un color en otra de otro, de hecho transforma todas las aristas del primer color en las aristas del segundo color, pues transformará el plano que pasa por O y por la primera en el que pasa por O y por la segunda, y a su vez transformará los planos perpendiculares al primero en los perpendiculares al segundo. Esto nos permite definir un homomorfismo de grupos

$$\mathrm{Is}_V^+(E) \longrightarrow \Sigma_\Omega \cong \Sigma_5.$$

Si probamos que es un monomorfismo, podremos concluir que $\mathrm{Is}_V^+(E) \cong A_5$, pues A_5 es el único subgrupo de índice 2 en Σ_5. En resumen, habremos probado lo siguiente:

> *El grupo de las simetrías (directas) de un icosaedro regular es isomorfo a A_5.*



Para ello basta comprobar que la cara superior tiene aristas de colores azul, verde y rojo, y que sólo hay otra cara con las aristas del mismo color, que es la cara opuesta, señalada en la figura, por lo que una simetría que conserve los colores tiene que fijar dichas caras (en cuyo caso fija seis vértices, luego es la identidad) o bien transforma una en la otra, pero hay una única simetría que transforma una cara en la otra llevando la arista azul en la azul, que es el giro de 180° respecto del eje señalado en la figura, pero dicho giro transforma la arista verde en la roja y viceversa.

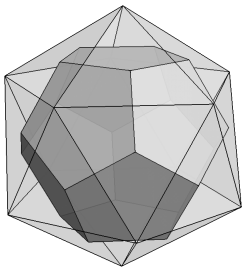
Esto termina la prueba de que $\mathrm{Is}_V^+(E)$ tiene la estructura indicada, y ahora podemos describir sus elementos (aparte de la identidad):

1. Los 24 ciclos de longitud 5 se corresponden con los giros respecto de ejes que pasan por cada uno de los 6 pares de vértices opuestos (hay cuatro giros respecto de cada eje).

2. Los 20 ciclos de longitud 3 se corresponden con los giros de 120° respecto de ejes que pasan por los centros de cada uno de los 10 pares de caras opuestas (hay dos giros por eje).

3. Las 15 permutaciones de tipo $(a,b)(c,d)$ se corresponden con los giros de 180° respecto de los ejes que pasan por los puntos medios de cada uno de los 15 pares de aristas opuestas.

Así tenemos una representación geométrica del grupo alternado de orden 5.



Nota Los centros de las caras de un icosaedro forman los vértices de un dodecaedro regular y, recíprocamente, los centros de las caras de un dodecaedro forman los vértices de un icosaedro, de modo que ambos forman otro par de poliedros duales, como el cubo y el octaedro, y por ello sus grupos de simetrías también son isomorfos. ∎

2.7 El teorema de Burnside

Vamos a demostrar un sencillo teorema[2] sobre acciones de grupos que tiene muchas aplicaciones a la combinatoria.

Teorema 2.39 (Burnside) *Si un grupo finito G actúa sobre un conjunto finito Ω, el número de órbitas de la acción es*

$$|\Omega/G| = \frac{1}{|G|}\sum_{g\in G}|\Omega^g|,$$

donde $\Omega^g = \{x \in \Omega \mid xg = x\}$.

Demostración: Observemos que

$$\sum_{g\in G}|\Omega^g| = \sum_{g\in G}|\{x\in\Omega \mid xg=x\}| = |\{(x,g)\in\Omega\times G \mid xg=x\}|$$

$$= \sum_{x\in\Omega}|\{g\in G \mid xg=x\}| = \sum_{x\in\Omega}|G_x|.$$

Ahora, por el teorema 2.2 tenemos que $|\Omega_x| = |G|/|G_x|$, por lo que

$$\frac{1}{|G|}\sum_{g\in G}|\Omega^g| = \sum_{x\in\Omega}\frac{1}{|\Omega_x|} = \sum_{O\in\Omega/G}\sum_{x\in O}\frac{1}{|\Omega_x|} = \sum_{O\in\Omega/G}1 = |\Omega/G|.$$

∎

Vamos a ver cómo este teorema nos permite responder sistemáticamente a preguntas como éstas:

[2]Pese a su nombre, no se debe a Burnside, sino que éste lo incluyó en un libro sin ninguna referencia porque lo consideraba suficientemente conocido, pero esto hizo que le fuera atribuido por error.

1. Queremos diseñar un tiovivo con 10 caballos dispuestos en círculo, y tenemos tres tipos de figuras de caballo. ¿Cuántos tiovivos diferentes podemos formar?

2. ¿De cuántas formas se pueden pintar las caras de una pirámide cuadrangular usando 3 colores?

3. ¿Cuántas pulseras distintas podemos formar ensartando en un hilo 6 cuentas de 3 colores?

4. ¿De cuántas formas distintas podemos pintar las caras de un cubo usando 4 colores?

Collares Consideremos el caso en que Ω es el conjunto de todas las formas de colorear los vértices de un polígono regular de n lados con k colores, de modo que $|\Omega| = n^k$.

Por ejemplo, si $n = k = 4$, la figura siguiente representa dos elementos de Ω:

$$\begin{array}{ccc} 3 & - & 3 \\ | & & | \\ 1 & - & 4 \end{array} \qquad \begin{array}{ccc} 3 & - & 4 \\ | & & | \\ 3 & - & 1 \end{array}$$

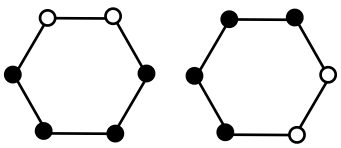
Pero podemos pensar que estos esquemas describen dos tiovivos con 4 caballos de distintos modelos, en cuyo caso debemos considerar que ambos describen el mismo tiovivo, pues el segundo se obtiene del primero mediante un giro de $90°$.

Así pues, contar tiovivos no es lo mismo que contar coloraciones, pues en el primer caso debemos considerar que dos coloraciones son el mismo tiovivo si una puede obtenerse de la otra mediante un giro.

En general, consideramos el grupo cíclico $G \cong C_n$ de todos los giros que dejan invariante a un polígono regular de n lados, que actúa de forma obvia sobre Ω: dada una coloración $c \in \Omega$ y un giro $g \in G$, la coloración cg es la que resulta de aplicarle al polígono coloreado c el giro g. En estos términos, la coloración de la derecha anterior es cg, donde c es la coloración de la izquierda y g el giro de $90°$ en sentido antihorario.

Se llaman *collares* con n cuentas de k colores a las órbitas de Ω respecto de la acción de G, es decir, al número de formas de colorear con k colores los vértices de un polígono regular de n lados considerando que dos coloraciones son la misma si una se puede obtener de la otra mediante un giro.

Por ejemplo, la figura siguiente muestra dos coloraciones de un hexágono que determinan un mismo collar:

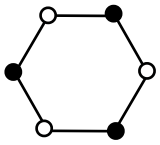


En estos términos, la pregunta que hemos formulado tras el teorema 2.39 sobre el diseño de tiovivos equivale a contar los collares con 10 cuentas y 3 colores, y la pregunta sobre las formas de pintar las caras de una pirámide equivale a contar los collares con 4 cuentas y 3 colores (y multiplicar el resultado por 3 si queremos pintar también la base).

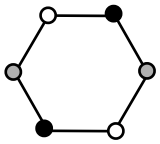
Veamos que el teorema de Burnside nos permite calcular el número de collares con cualquier número de cuentas y de colores.

Para ello sólo tenemos que calcular el número de coloraciones fijadas por cada permutación $\sigma \in G$. Éste depende únicamente del orden de σ. Por simplicidad vamos a considerar primero el caso particular $n = 6$. Tomemos $f \in \Omega^\sigma$ y distingamos casos:

- Si $o(\sigma) = 1$, es decir, si σ es la identidad, obviamente fija a todas las coloraciones, luego $|\Omega^\sigma| = |\Omega| = k^6$.
- Si $o(\sigma) = 6$, es decir, si σ es un giro de $360/6 = 60°$, entonces para que una coloración resulte fijada, cada vértice tiene que ser del mismo color que el siguiente, luego todos los vértices tienen que ser del mismo color, y sólo hay k coloraciones que cumplen eso, es decir, $|\Omega^\sigma| = k$.
- Si $o(\sigma) = 3$, entonces σ es un giro de $360/3 = 120°$, luego para que una coloración resulte fijada tiene que ser de la forma



  donde los colores pueden ser iguales o distintos (pero los vértices que hemos pintado del mismo color tienen que estar pintados del mismo color). Claramente entonces $|\Omega^\sigma| = k^2$.
- Si $o(\sigma) = 2$, entonces σ es un giro de $180°$, luego una coloración fijada tiene que ser de la forma



  donde los tres colores no son necesariamente distintos, luego $|\Omega^\sigma| = k^3$.

Por último recordamos que un grupo cíclico tiene $\phi(d)$ elementos de orden d (para todo divisor del orden del grupo), luego la fórmula de Burnside nos da ahora que el número de collares es

$$C_k^6 = \frac{\phi(1)k^6 + \phi(2)k^3 + \phi(3)k^2 + \phi(6)k}{6} = \frac{k^6 + k^3 + 2k^2 + 2k}{6}.$$

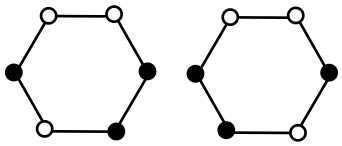
Pero todo el razonamiento vale en realidad para un n arbitrario:

Si $d \mid n$ y $o(\sigma) = d$, podemos ver a σ como una permutación $\sigma \in \Sigma_n$ del conjunto de los vértices del polígono y, según el teorema 2.10, σ es un producto de n/d ciclos disjuntos de longitud d (notemos que d es aquí lo que en el teorema es k/d), lo que se traduce en que una coloración resulta fijada por σ si y sólo si asigna el mismo color a todos los vértices de la órbita de cada ciclo, por lo que $|\Omega^\sigma| = k^{n/d}$, luego la fórmula general es para el número de collares es

$$C_k^n = \frac{1}{n}\sum_{d|n} \phi(d) k^{n/d}.$$

Por ejemplo, $C_3^{10} = 5\,934$, y esto responde a la pregunta sobre el número de tiovivos con 10 caballos de tres tipos distintos, mientras que $C_3^4 = 24$ es el número de formas de pintar las caras laterales de una pirámide cuadrangular con tres colores (o 72 si pintamos también la base). ∎

Pulseras La figura muestra dos collares distintos con 6 cuentas y 2 colores:



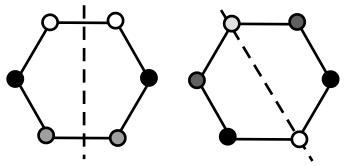
No es posible obtener uno a partir del otro mediante un giro. Ahora bien, sí que es posible convertir uno en el otro mediante una simetría respecto a una recta vertical. Si pensamos que las figuras representan cuentas ensartadas en un hilo, en realidad son indistinguibles, pues una sarta se convierte en la otra "volteándola". Esto no es aplicable a los tiovivos o a las pirámides cuadrangulares, pero sí a las pulseras hechas de cuentas. Cuando admitimos simetrías a la hora de identificar dos coloraciones de Ω, se habla de "pulseras" en lugar de "collares".

Concretamente, ahora podemos considerar la acción sobre el conjunto Ω de todas las coloraciones con k colores de un polígono regular de n lados del grupo $G \cong D_{2n}$ de todos los giros y simetrías que lo dejan invariante. Las órbitas de esta acción se llaman *pulseras* con n cuentas y k colores.

Claramente el número de pulseras con n cuentas de k colores es en efecto el número de pulseras diferentes que pueden fabricarse ensartando n cuentas de k colores en un hilo circular, entendiendo que dos pulseras son iguales si una se puede transformar en la otra mediante un giro o una simetría.

Veamos cómo el teorema de Burnside nos permite contar el número P_k^n de pulseras con n cuentas de k colores. Observemos que todo el cálculo que hemos hecho en el caso de los collares sigue siendo válido: si g es un giro y $o(g) = d$, entonces $|\Omega^g| = k^{n/d}$. Nos falta considerar el caso en que g es una simetría. De nuevo vamos a considerar primero el caso $n = 6$.

Si g es una simetría que pasa por los puntos medios de dos lados, una coloración $c \in \Omega^g$ si pinta del mismo color cada par de vértices que se corresponden por la simetría, lo que deja un total de 3 colores posibles, $|\Omega^g| = k^3$. Sin embargo, si el eje de simetría de g pasa por dos vértices, entonces podemos usar hasta 4 colores distintos, luego $|\Omega^g| = k^4$:



Como hay 3 simetrías de cada uno de los dos tipos, la fórmula del teorema de Burnside nos da:

$$P_k^6 = \frac{\phi(1)k^6 + \phi(2)k^3 + \phi(3)k^2 + \phi(6)k}{12} + \frac{3k^3 + 3k^4}{12} = \frac{k^6 + 3k^4 + 4k^3 + 2k^2 + 2k}{12}.$$

En general, si n es impar, todas las simetrías pasan por un vértice y fijan las coloraciones que coinciden sobre cada uno de los $(n-1)/2$ pares de puntos homólogos, luego podemos emplear $(n-1)/2+1$ colores, luego $|\Omega^g| = k^{(n+1)/2}$ y la fórmula es

$$P_k^n = \frac{1}{2n}\sum_{d|n} \phi(d)k^{n/d} + \frac{1}{2}k^{(n+1)/2}.$$

En cambio, si n es par, las simetrías que pasan por los puntos medios de dos lados opuestos fijan las coloraciones que coinciden en cada uno de los $n/2$ pares de puntos homólogos, luego podemos usar $n/2$ colores y $|\Omega^g| = k^{n/2}$, mientras que las simetrías que pasan por dos vértices fijan las coloraciones que coinciden en los $(n-2)/2$ pares de puntos homólogos, luego $|\Omega^g| = k^{(n-2)/2+2}$ y la fórmula es:

$$P_k^n = \frac{1}{2n}\sum_{d|n} \phi(d)k^{n/d} + \frac{1}{4}k^{n/2} + \frac{1}{4}k^{n/2+1}.$$

En resumen:

$$P_k^n = \frac{1}{2n}\sum_{d|n} \phi(d)k^{n/d} + \frac{k+1}{4}k^{n/2} \quad \text{(si } n \text{ es par)}$$

$$P_k^n = \frac{1}{2n}\sum_{d|n} \phi(d)k^{n/d} + \frac{1}{2}k^{(n+1)/2} \quad \text{(si } n \text{ es impar).}$$

La tabla siguiente calcula algunos casos para $n = 6$:

k	1	2	3	4	5
C_k^6	1	14	130	700	2 635
P_k^6	1	13	92	430	1 505

En particular en ella vemos la respuesta a la tercera pregunta que habíamos planteado tras el teorema 2.39. Hay 92 pulseras en las condiciones requeridas. Por otro lado, la diferencia entre C_2^6 y P_2^6 consiste únicamente en el par de collares distintos mostrados al principio de este apartado sobre "pulseras" que determinan la misma pulsera. ∎

Permutaciones circulares con repetición Si $r_1 + \cdots + r_k = n$, el número de *permutaciones circulares con repetición* $\mathrm{PCR}^n_{r_1,\ldots,r_k}$ es el número de collares que se pueden formar con n cuentas de colores, de modo que haya exactamente r_1 de un color, r_2 de otro, etc.

Vamos a probar que, si $h = \mathrm{mcd}(r_1, \ldots, r_k)$, entonces

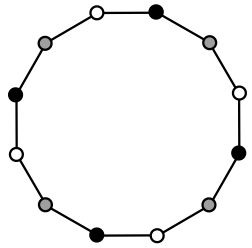
$$\mathrm{PCR}^n_{r_1,\ldots,r_k} = \sum_{d|h} \frac{\phi(d)}{n} \frac{(n/d)!}{(r_1/d)! \cdots (r_k/d)!}.$$

La fórmula se simplifica drásticamente si los r_i son primos entre sí, es decir, si $h = 1$, en cuyo caso

$$\mathrm{PCR}^n_{r_1,\ldots,r_k} = \frac{(n-1)!}{r_1! \cdots r_k!}.$$

Consideramos el conjunto $\Omega \subset \Omega_k^n$ formado por las aplicaciones que toman r_i veces el valor i, sobre el que actúa el grupo cíclico $G = \langle(1, \ldots, n)\rangle$. Notemos que si $f \in \Omega$ y $\sigma \in G$, entonces $f^\sigma \in \Omega$, por lo que la acción está bien definida.

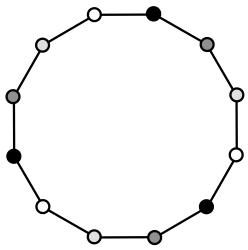
Vamos a ilustrar el razonamiento general calculando $\mathrm{PCR}^{12}_{3,3,6}$. Por ejemplo, si $g \in G$ tiene orden 4, una coloración está en Ω^g si y sólo si tiene del mismo color las cuentas que en la figura siguiente tienen el mismo color:



pero eso es imposible, porque el número de cuentas de cada color tendría que ser múltiplo de 4, luego concluimos que $\Omega^g = \varnothing$.

En general, si $d \mid n$ y $g \in G$ tiene orden d, una coloración estará en Ω^g si y sólo si los colores de sus cuentas se repiten cíclicamente d veces con un periodo de longitud n/d, luego el número de cuentas de cada color es múltiplo de d, para lo cual es necesario que $d \mid h$ (en caso contrario $\Omega^g = \varnothing$).

Volviendo a nuestro ejemplo, supongamos que g tiene orden 3, con lo que las coloraciones fijadas tienen que tener la forma



donde los cuatro colores que hemos representado no tienen por qué ser distintos. De hecho, para que se repitan 3, 3 y 6 veces, es necesario que los dos primeros aparezcan una vez en cada periodo y el tercero 2 veces.

En general, si $d \mid h$, en cada periodo (de longitud n/d), el color i-ésimo tiene que aparecer r_i/d veces, y esto nos lleva a que

$$|\Omega^g| = \frac{(n/d)!}{(r_1/d)!\cdots(r_k/d)!}.$$

En efecto, se trata de probar que el número de formas de colorear n objetos de modo que haya r_i de cada color i es

$$\frac{n!}{r_1!\cdots r_k!}.$$

Esto es evidente para $k = 1$ y, si vale para un k y tenemos $k+1$ colores, para construir una coloración tenemos que elegir r_{k+1} objetos de color $k+1$, para lo cual tenemos

$$\binom{n}{r_{k+1}} = \frac{n!}{r_{k+1}!(n-r_{k+1})!}$$

posibilidades y, de entre los $n - r_{k+1}$ objetos restantes, tenemos que elegir r_i objetos de cada color i, para lo cual, por hipótesis de inducción, tenemos

$$\frac{(n-r_{k+1})!}{r_1!\cdots r_k!}$$

posibilidades, luego en total tenemos

$$\frac{n!}{r_{k+1}!(n-r_{k+1})!}\frac{(n-r_{k+1})!}{r_1!\cdots r_k!} = \frac{n!}{r_1!\cdots r_{k+1}!}$$

posibilidades.

Como en g hay $\phi(d)$ elementos de orden d, el teorema de Burnside nos da la fórmula anunciada. ∎

Es posible dar una fórmula general para el número de pulseras con exactamente r_i cuentas de color i, pero hay que distinguir varios casos. Por ejemplo, si $n = r_1 + \cdots + r_k$ es impar, la fórmula es

$$\sum_{d\mid h}\frac{\phi(d)}{2n}\frac{(n/d)!}{(r_1/d)!\cdots(r_k/d)!}$$

salvo si todos los r_i son pares excepto uno de ellos (que podemos suponer que es r_k). Sólo en ese caso hay coloraciones fijadas por las n simetrías del grupo D_{2n}, y el resultado es

$$\sum_{d|h} \frac{\phi(d)}{2n} \frac{(n/d)!}{(r_1/d)! \cdots (r_k/d)!} + \frac{((n-1)/2)!}{2(r_1/2)! \cdots (r_{k-1}/2)!((r_k-1)/2)!}.$$

Si n es par hay que distinguir tres casos, según si todos los r_i son pares, hay exactamente dos impares o hay más de dos impares. El número de coloraciones fijadas por una simetría que pase por los puntos medios de dos aristas es 0 salvo que todos los r_i sean pares, en cuyo caso estas $n/2$ simetrías aportan el sumando

$$\frac{(n/2)!}{2(r_1/2)! \cdots (r_k/2)!}.$$

En cuanto a las simetrías respecto a un eje que pasa por dos vértices, no fijan ninguna coloración si hay más de dos r_i impares. Si hay exactamente 2 colores impares (digamos r_{k-1} y r_k), los dos vértices fijados por la simetría tienen que pintarse de dichos colores, lo que nos da dos posibilidades, y el sumando correspondiente es

$$\frac{(n/2)!}{2(r_1/2)! \cdots (r_{k-2}/2)!((r_{k-1}-1)/2)!((r_k-1)/2)!}.$$

El caso más complicado se da cuando todos los r_i son pares, porque entonces podemos pintar los dos vértices fijados de cualquiera de los colores (pero ambos del mismo color), y el sumando es

$$\sum_{i=1}^{k} \frac{((n-2)/2)!}{4(r_1/2)! \cdots ((r_i-2)/2)! \cdots (r_k/2)!}.$$

En resumen, si $n = r_1 + \cdots + r_k$ y $h = (r_1, \ldots, r_k)$, el número de collares de n cuentas en las que hay exactamente r_i de color i (lo que podríamos llamar permutaciones diédricas con repetición) es igual a

$$\mathrm{PDR}^n_{r_1,\ldots,r_k} = \sum_{d|h} \frac{\phi(d)}{2n} \frac{(n/d)!}{(r_1/d)! \cdots (r_k/d)!} + S,$$

donde S depende de los cinco casos siguientes:

I n es impar y hay más de una multiplicidad r_i impar.

II n es impar y sólo una multiplicidad r_i es impar.

III n es par y hay más de dos r_i impares.

IV n es par y hay exactamente dos r_i impares.

V n es par y todos los r_i son pares.

Concretamente,

$$\begin{aligned}
S_{\mathrm{I}} &= S_{\mathrm{III}} = 0,\\
S_{\mathrm{II}} &= \frac{((n-1)/2)!}{2(r_1/2)!\cdots(r_{k-1}/2)!((r_k-1)/2)!},\\
S_{\mathrm{IV}} &= \frac{(n/2)!}{2(r_1/2)!\cdots(r_{k-2}/2)!((r_{k-1}-1)/2)!((r_k-1)/2)!},\\
S_{\mathrm{V}} &= \frac{(n/2)!}{2(r_1/2)!\cdots(r_k/2)!} + \sum_{i=1}^{k} \frac{((n-2)/2)!}{4(r_1/2)!\cdots((r_i-2)/2)!\cdots(r_k/2)!}.
\end{aligned}$$

■

Coloraciones de un cubo Vamos a determinar de cuántas formas distintas podemos pintar las caras de un cubo con k colores. Para ello consideramos el conjunto Ω de todas las coloraciones de las caras de un cubo, de modo que $|\Omega| = k^6$, y la acción sobre este conjunto del grupo $G \cong \Sigma_4$ formado por las simetrías del cubo. Vamos a calcular los cardinales de los conjuntos Ω^g para cada $g \in G$.

- Si $g = 1$, claramente $|\Omega^g| = |\Omega| = k^6$.
- Si g es un giro de 90° respecto de un eje que pase por el centro de dos caras opuestas (y hay 6 giros así, correspondientes a los ciclos de longitud 4 en Σ_4), entonces una coloración queda fija si y sólo si asigna el mismo color a las cuatro caras que giran, y colores arbitrarios a las dos que no se mueven, luego $|\Omega^g| = k^3$.
- Si g es un giro de 180° respecto al mismo eje (y hay 3 giros así, correspondientes a los productos de dos trasposiciones en Σ_4), entonces una coloración queda fija si y sólo si asigna el mismo color a cada par de caras opuestas que giran y colores arbitrarios a las dos que no se mueven, luego $|\Omega^g| = k^4$.
- Si g es un giro de 120° respecto a una recta que pase por dos vértices opuestos del cubo (y hay 8 giros así, correspondientes a los ciclos de longitud 3 en Σ_4), entonces una coloración queda fija si y sólo si asigna el mismo color a cada grupo de tres caras que rodean a uno de los dos vértices fijados, luego $|\Omega^g| = k^2$.
- Si g es un giro de 180° respecto de un eje que pasa por los puntos medios de dos aristas opuestas (y hay 6 giros así, correspondientes a las transposiciones de Σ_4), las caras se intercambian por pares, luego $|\Omega^g| = k^3$.

En total, el número de formas de pintar las caras de un cubo con k colores es

$$\frac{k^6 + 6k^3 + 3k^4 + 8k^2 + 6k^3}{24} = \frac{k^6 + 3k^4 + 12k^3 + 8k^2}{24}.$$

Ejercicio: Determinar el número de formas de pintar los vértices de un cubo con k colores.

El lector puede plantear y resolver problemas similares al anterior para cualquier otro poliedro regular, teniendo en cuenta la estructura de los grupos de simetrías determinada en la sección anterior. ∎

Capítulo III

Teoremas de estructura

En la prueba del teorema [Al 5.50] hemos dejado pendientes de demostración dos resultados no triviales sobre grupos finitos. En realidad ambos son casos particulares de un mismo hecho:

> *Si G es un grupo finito y $p^n \mid |G|$, donde p es primo, entonces G tiene un subgrupo de orden p^n.*

En este capítulo vamos a demostrar resultados de este tipo, es decir, resultados que nos den información sobre qué podemos esperar de la estructura de un grupo. No es lo mismo saber que un grupo es no abeliano y tiene seis elementos que saber que tiene concretamente un único subgrupo normal de orden 3 y tres subgrupos de orden 2 que no son normales, pero eso es justo lo que podemos decir si sabemos que un grupo es no abeliano y tiene seis elementos. Similarmente, si sabemos que un grupo tiene 9 elementos, no es trivial en absoluto que es necesariamente abeliano, pero hemos visto que es así, etc.

3.1 Producto de grupos

Una forma de describir con claridad la estructura de un grupo es probar que es isomorfo al producto cartesiano de otros grupos de menor orden (luego más sencillos). En esta sección vamos a desarrollar para el producto grupos una teoría análoga a la que desarrollamos en la sección [Al 4.2] para la suma de módulos. Concretamente, vamos a definir lo que es una descomposición de un grupo en producto directo interno de una familia de subgrupos y demostraremos que esto equivale a que sea isomorfo al producto directo externo de esos mismos subgrupos (el producto cartesiano que ya tenemos definido).

Conviene probar primero un resultado elemental:

Teorema 3.1 *Si dos subgrupos normales de un grupo G tienen intersección trivial, entonces conmutan elemento a elemento.*

DEMOSTRACIÓN: Sean N y $M \trianglelefteq G$ tales que $N \cap M = 1$. Sean $n \in N$ y $m \in M$. Entonces $n^{-1}m^{-1}nm = \left(m^{-1}\right)^n m = n^{-1}n^m \in N \cap M = 1$, luego $nm = mn$. ∎

Definición 3.2 Diremos que un grupo G es *producto directo (interno)* de los subgrupos $N_1, \ldots, N_r$ si todos son normales en G, se cumple que $G = N_1 \cdots N_r$ y la intersección de cada N_i con el producto de los factores restantes es trivial. En tal caso se escribe $G = N_1 \times \cdots \times N_r$.

Observemos que la notación es la misma que hemos empleado en 1.2 para el producto que podemos llamar "externo" para distinguirlo del anterior, en el que los factores no son subgrupos de un grupo dado de antemano. Enseguida veremos que, cuando G es producto directo internos de unos subgrupos, de hecho es isomorfo a su producto directo externo, exactamente igual que sucede con la suma directa y el producto de módulos. Esto se debe al teorema siguiente:

Teorema 3.3 *Sea G un grupo y $N_1, \ldots, N_r$ una familia de subgrupos. Las afirmaciones siguientes son equivalentes:*

1. $G = N_1 \times \cdots \times N_r$.
2. *Cada $N_i \trianglelefteq G$ y cada elemento $g \in G$ se expresa de forma única como producto $g = n_1 \cdots n_r$ con cada $n_i \in N_i$.*

DEMOSTRACIÓN: Si se cumple 1), por definición tenemos que $N_i \trianglelefteq G$, así como que todo elemento de G se expresa de la forma indicada. Falta probar que la expresión es única. Supongamos que $n_1 \cdots n_r = n'_1 \cdots n'_r$. Entonces

$$n_1'^{-1} n_1 = (n'_2 \cdots n'_r)(n_2 \cdots n_r)^{-1} \in N_1 \cap (N_2 \cdots N_r) = 1,$$

luego $n_1 = n'_1$, luego $n_2 \cdots n_r = n'_2 \cdots n'_r$ y, procediendo del mismo modo, llegamos a que $n_i = n'_i$ para todo índice i.

Si se cumple 2), tenemos trivialmente que $G = N_1 \cdots N_r$, y si se cumple que $n \in N_1 \cap (N_2 \cdots N_r)$, entonces $n = n_2 \cdots n_r$, con $n_i \in N_i$, luego $n^{-1}n_2 \cdots n_r = 1$ y, como tambiñen $1 \cdots 1 = 1$, por la unicidad de la expresión tiene que ser $n_i = 1$ para todo i, luego $n = 1$, luego $N_1 \cap (N_2 \cdots N_r) = 1$.

Ahora, por el teorema 3.1, tenemos que N_1 y $N_2 \cdots N_r$ conmutan elemento a elemento, luego si se cumple que $n \in N_2 \cap (N_1 N_3 \cdots N_r)$, entonces tenemos que $n = n_1 n_3 \cdots n_r$, con $n_i \in N_i$, pero N_2 conmuta con N_1 elemento a elemento, luego podemos escribir $n_1 n^{-1} n_3 \cdots n_r = 1$, de donde concluimos como antes que $n = 1$, luego $N_2 \cap (N_1 N_3 \cdots N_r) = 1$, y prosiguiendo de este modo concluimos que cada N_i tiene intersección trivial con el producto de los demás subgrupos. ∎

Notemos que, tal y como hemos usado en la demostración, si tenemos un producto $G \times H$ de grupos no abelianos, se trata de un grupo no abeliano, pero los elementos de G conmutan con los de H.

Ahora es inmediato que la aplicación $(N_1 \times \cdots \times N_r)_{\text{ext}} \longrightarrow (N_1 \times \cdots \times N_r)_{\text{int}}$ dada por $(n_1, \ldots, n_r) \mapsto n_1 \cdots n_r$ es un isomorfismo de grupos. Notemos que

$$(n_1, \ldots, n_r)(n'_1, \ldots, n'_2) \mapsto n_1 \cdots n_r n'_1 \cdots n'_r = (n_1 n'_1) \cdots (n_r n'_r)$$

porque n'_1 conmuta con $n_2 \cdots n_n$, luego podemos escribir

$$(n_1 n'_1) n_2 \cdots n_r n'_2 \cdots n'_r,$$

y a su vez, n'_2 conmuta con $n_3 \cdots n_r$, por lo que podemos escribir

$$(n_1 n'_1)(n_2 n'_2) n_3 \cdots n_r n'_3 \cdots n'_r,$$

y así llegamos a la expresión final $(n_1 n'_1) \cdots (n_r n'_r)$.

Recíprocamente, si tenemos un producto externo $G = G_1 \times \cdots \times G_r$, donde los factores no son, en principio, subgrupos de ningún otro grupo, tenemos monomorfismos de grupos $\iota_i : G_i \longrightarrow G$ dados por $\iota_i(g_i) = (1, \ldots, g_i, \ldots, 1)$ y las imágenes $N_i = \operatorname{Im} \iota_i$ son subgrupos normales de G, pues

$$(h_1, \ldots, h_n)^{-1}(1, \ldots, g_i, \ldots, 1)(h_1, \ldots, h_n) = (1, \ldots, h_i^{-1} g_i h_i, \ldots, 1) \in N_i,$$

y el producto de los N_j para $j \neq i$ está formado por los elementos de G con componente i-ésima trivial, luego es un subgrupo que tiene intersección trivial con N_i, luego $G = N_1 \times \cdots \times N_r$ (como producto interno).

Así pues, los conceptos de "producto interno" y "producto externo" son equivalentes.

Dejamos al lector la extensión de estos conceptos y resultados al caso de infinitos factores, que es completamente análogo al caso de los módulos, aunque no vamos a necesitarlo en ningún momento.

Hay que distinguir igualmente entre el *producto (externo) de grupos:* $\prod_{i \in I} G_i$, con la operación $(fg)(i) = f(i)g(i)$, y el *producto directo (externo):*

$$\prod_{i \in I}{}^{*} G_i = \{f \in \prod_{i \in I} G_i \mid \{i \in I \mid f(i) \neq 1\} \text{ es finito}\} \leq \prod_{i \in I} G_i.$$

Internamente sólo podemos definir un producto directo interno (análogo a la suma directa de módulos) que resulta ser equivalente al producto directo externo.

Grupos abelianos Citamos ahora el teorema [Al 4.51] (véanse también las observaciones posteriores), que hemos demostrado en [Al] porque la prueba es válida para módulos sobre un DIP arbitrario:

Teorema 3.4 *Todo grupo abeliano finitamente generado G (en particular todo grupo abeliano finito) es producto directo de un número finito de grupos cíclicos: $G = C_{d_1} \times \cdots \times C_{d_r}$, y la descomposición es única si exigimos que cada d_i finito sea potencia de primo, o que los d_i finitos cumplan $d_i \mid d_{i+1}$.*

Cuando los d_i finitos se escogen de modo que sean potencias de primo se llaman *factores invariantes* del grupo, y cuando se escogen de modo que $d_i \mid d_{i+1}$ se llaman *divisores elementales.*

A la hora de manipular descomposiciones en producto de grupos cíclicos finitos, el único resultado de fondo es el teorema chino del resto [Al 3.53], que en términos de grupos finitos dice así:

Teorema 3.5 *Si m, n son números naturales primos entre sí, $C_{mn} \cong C_m \times C_n$.*

Ejemplo Si queremos determinar todos los grupos abelianos de orden 24, las posibilidades son, en términos de factores invariantes:

$$C_8 \times C_3, \quad C_2 \times C_4 \times C_3, \quad C_2 \times C_2 \times C_2 \times C_3.$$

No hay más posibilidades de productos de grupos cíclicos de órdenes potencia de primo que tengan orden 24. En términos de factores invariantes son

$$C_{24}, \quad C_2 \times C_{12}, \quad C_2 \times C_2 \times C_6.$$

Estos grupos son isomorfos a los anteriores en virtud del teorema 3.5, y son los únicos productos de grupos cíclicos con orden 24 en total en los que el orden de cada factor divida al del siguiente. Así pues, hay exactamente 3 clases de grupos abelianos de orden 24. ∎

Ejercicio: Probar que si n es impar $D_{4n} \cong D_{2n} \times C_2$.

Recordemos por último el teorema [Al 4.53], según el cual un grupo finito abeliano contiene subgrupos de todos los órdenes que dividen al orden del grupo. Esto también es cierto para p-grupos no abelianos:

Teorema 3.6 *Si p es un primo, todo p-grupo posee subgrupos de todos los grupos que dividen a su orden.*

Demostración: Sea $|G| = p^n$. Vamos a probar que G cumple el resultado por inducción sobre n. Si $n = 1$ entonces G es cíclico y no hay nada que probar. Si vale para grupos de orden p^m con $m < n$ distinguimos dos casos: si G es abeliano ya sabemos que cumple el teorema. En caso contrario, $|Z(G)| = p^r$, con $r > 0$, por 2.5, luego $|G/Z(G)| = p^{n-r}$. Por hipótesis de inducción $G/Z(G)$ tiene un subgrupo $H/Z(G)$ de orden p^i, para todo $i \leq n - r$, luego $|H| = p^{i+r}$. Esto prueba que G tiene subgrupos de todos los órdenes p^i con $r \leq i \leq n$, pero como $Z(G)$ es abeliano, tiene subgrupos de orden p^i para $0 \leq i \leq r$, luego G también. ∎

En particular todo p-grupo tiene un subgrupo de índice p, que es necesariamente normal, por el teorema 2.27.

Ejemplo La descomposición de un grupo abeliano en producto de grupos cíclicos determina completamente su estructura. Por ejemplo, consideremos el grupo $A = C_2 \times C_4$. Teniendo en cuenta que el orden de un par (g_1, g_2) es el mínimo común múltiplo de los órdenes de sus componentes, consideramos la tabla siguiente:

	1	4	2	4
1	1	4	2	4
2	2	4	2	4

En C_4 hay un elemento de orden 2 y dos de orden 4, mientras que en C_2 hay un elemento de orden 2. La tabla contiene el mínimo común múltiplo de cada par, y en ella vemos que A tiene un elemento de orden 1, tres de orden 2 y cuatro de orden 4.

Hilando más fino, los tres elementos de orden 2 no son todos "iguales". Si $C_2 = \langle x\rangle$ y $C_4 = \langle y\rangle$, los elementos de orden 4 son $(1, y), (1, y^3), (x, y), (x, y^3)$, y vemos que sus cuadrados son todos iguales a $(1, y^2)$, luego hay un elemento de orden 4 que se distingue por que es el cuadrado de todos los elementos de orden 4, mientras que los otros dos no son el cuadrado de ningún elemento de A.

De aquí podemos deducir que el grupo $\operatorname{Aut} A$ tiene 8 elementos. En efecto, si $x, x' \in A$ son dos elementos de orden 2 que no sean cuadrados e $y, y' \in A$ son dos elementos de orden 4, entonces $A = \langle x\rangle \times \langle y\rangle = \langle x'\rangle \times \langle y'\rangle$ y claramente tenemos isomorfismos $\langle x\rangle \longrightarrow \langle x'\rangle$, $\langle y\rangle \longrightarrow \langle y'\rangle$ dados por $x^j \mapsto x'^j$, $y^j \mapsto y'^j$, respectivamente, que inducen un automorfismo $f : A \longrightarrow A$ dado por

$$f(x^j y^k) = x'^j y'^k.$$

En otras palabras, fijados $x, y \in A$ de órdenes 2 y 4, respectivamente (y de modo que x no sea un cuadrado), para cada par de elementos gx, y' en las mismas condiciones existe un único automorfismo $f \in \operatorname{Aut} A$ determinado por que $f(x) = x'$ y $f(y) = y'$, y esto nos da un total de 8 automorfismos distintos (y ninguno más).

Más precisamente, se cumple que $\operatorname{Aut} A \cong D_8$. En efecto, fijado un par (x, y) en las condiciones indicadas, la tabla siguiente describe cada automorfismo por su imagen sobre dicho par:

1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
(x, y)	(xy^2, xy)	(x, y^3)	(xy^2, xy^3)	(xy^2, y)	(x, xy^3)	(xy^2, y^3)	(x, xy)

El lector puede comprobar que cada automorfismo se obtiene de σ y τ como se indica. Por ejemplo, $\sigma^2(y) = \sigma(xy) = \sigma(x)\sigma(y) = xy^2xy = y^3$, así como que se cumplen las relaciones $\sigma^4 = \tau^2 = 1$ y $\sigma^\tau = 1$, por lo que el teorema 1.38 nos asegura que el grupo es diédrico.

La estructura de los grupos de unidades Los grupos U_n de las unidades del anillo $\mathbb{Z}/n\mathbb{Z}$ son ejemplos de grupos abelianos finitos cuya descomposición en producto de grupos cíclicos no es obvia. El primer paso para determinar su estructura es observar que si m y n son números naturales primos entre sí, entonces, por el teorema chino del resto [Al 3.53]

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

donde el isomorfismo es $[a] \mapsto ([a], [a])$, y es claro que este isomorfismo de anillos se restringe a un isomorfismo de grupos $U_{mn} \cong U_m \times U_n$.

Recordemos que la función de Euler es $\phi(m) = |U_m|$. Ahora es fácil probar:

Teorema 3.7 *La función de Euler está caracterizada por las propiedades siguientes:*

$$\phi(p^n) = (p-1)p^{n-1}, \qquad si\ (m,n) = 1, \quad \phi(mn) = \phi(m)\phi(n).$$

DEMOSTRACIÓN: La segunda propiedad es consecuencia inmediata del isomorfismo $U_{mn} \cong U_m \times U_n$. En cuanto a la primera, los números naturales menores que p^n que no son primos con p^n son los de la forma pm, con $0 \leq m < p^{n-1}$, luego son p^{n-1}, luego $\phi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$. ∎

Si p es un número primo, el grupo U_p es cíclico, por el teorema [Al 4.51]. No merece la pena repetir aquí las demostraciones de los teoremas [ITAl 3.31] e [ITAl 3.32], que aseguran que U_{p^n} es un grupo cíclico siempre que p es un primo impar, mientras que [ITAl 3.33] afirma que si $n \geq 3$, entonces $U_{2^n} \cong C_2 \times C_{2^{n-2}}$. Reuniendo estos hechos tenemos:

Teorema 3.8 *Si $n = p_1^{e_1} \cdots p_r^{e_3}$, donde los p_i son primos distintos, entonces*

$$U_n \cong U_{p_1^{e_1}} \times \cdots \times U_{p_r^{e_r}},$$

donde cada factor es cíclico salvo si $p_i = 2$, en cuyo caso, $U_2 = 1$, $U_4 \cong C_2$ y, para $n \geq 3$, $U_{2^n} \cong C_2 \times C_{2^{n-2}}$.

Remitimos a la sección 3.6 de [ITAl] para los detalles sobre cómo encontrar generadores explícitos de los grupos U_n.

Por ejemplo, $U_{3000} \cong U_8 \times U_3 \times U_{125} \cong C_2 \times C_2 \times C_2 \times C_{100}$.

3.2 Grupos libres

Introducimos ahora una familia de grupos que figura entre las construcciones más abstractas que vamos a considerar, pero que en la sección siguiente nos permitirá introducir la forma más eficiente de definir grupos en términos de su pura estructura algebraica. Se trata de la versión análoga para grupos del concepto de módulo libre, sólo que en el caso de los grupos es mucho más delicada. Los definimos a partir del análogo al teorema [Al 4.21]:

Definición 3.9 Un subconjunto X de un grupo G es una *base* de G si para todo grupo H y toda aplicación $f : X \longrightarrow H$ existe un único homomorfismo de grupos $f^* : G \longrightarrow H$ que extiende a f. Un grupo es *libre* si tiene una base.

Por ejemplo, es claro que un grupo trivial cumple la definición de grupo libre tomando como base el conjunto vacío. También es fácil ver que el grupo aditivo $\mathbb{Z}$ es libre con base 1. En cambio, veremos que el $\mathbb{Z}$-módulo libre $\mathbb{Z}^2$ no es un grupo libre.

Ejercicio: Probar que $\mathbb{Z}^2$ no es un grupo libre a partir de la definición.

Las bases de un módulo se definen como sistemas generadores libres. Es posible dar una caracterización análoga de las bases de un grupo, pero la definición de sistema libre es un poco más delicada:

Un subconjunto X de un grupo G es *libre* si siempre que $x_1, \ldots, x_n \in X$ de modo que no haya dos elementos consecutivos iguales y $m_1, \ldots m_n$ son enteros no nulos, entonces $x_1^{m_1} \cdots x_n^{m_n} \neq 1$.

Notemos que una adaptación más superficial de la definición de subconjunto libre de un módulo exigiría que los x_i fueran distintos dos a dos, pero no podemos exigir eso si queremos que un generador libre cumpla la propiedad de extensión de aplicaciones que hemos usado para definir las bases. Sólo podemos exigir que un mismo elemento no aparezca dos veces seguidas en lo que es el análogo de una combinación lineal.

Veamos algunas consecuencias elementales esta definición:

- El conjunto vacío es libre, pues cumple trivialmente la definición. Más en general, todo subconjunto de un conjunto libre es libre.
- Si $1 \in X$, entonces X no es libre, pues $1^1 = 1$ contradice la definición.
- Si X es libre y $x \in X$, entonces $x^{-1} \notin X$. En efecto, si $x \neq x^{-1}$ tenemos que $x^1 y^1 = 1$, con $y = x^{-1}$, y esto contradice la definición. Si $x = x^{-1}$ entonces $x^2 = 1$ contradice la definición.
- Si X es libre y $x, y \in X$, con $x \neq y$, entonces $xy \neq yx$, pues por definición $x^{-1}y^{-1}xy \neq 1$. En particular un grupo que contenga un subconjunto libre con al menos dos elementos no es abeliano.

Teorema 3.10 *Un subconjunto X de un grupo G es una base si y sólo si es un sistema generador libre. En tal caso, todo $g \in G$ no trivial se expresa de forma única como $g = x_1^{m_1} \cdots x_n^{m_n}$, con $x_i \in X$, $m_i \in \mathbb{Z}$ no nulo y donde no hay dos potencias consecutivas con la misma base.*

Demostración: Supongamos que X es un generador libre y veamos primero la última parte del enunciado. El hecho de que X sea un generador implica que todo $g \in G$ puede expresarse como $g = x_1^{m_1} \cdots x_n^{m_n}$, con $x_i \in X$, $m_i \in \mathbb{Z}$. Podemos suponer que los exponentes son todos no nulos, pues los exponentes nulos se pueden eliminar (y si $g \neq 1$, no los eliminaremos todos). Si hay dos bases consecutivas iguales, podemos agrupar las potencias sumando los exponentes y, tras un número finito de pasos, llegaremos a una expresión en la que ya no se dé el caso. Supongamos ahora que

$$x_1^{m_1} \cdots x_n^{m_n} = y_1^{k_1} \cdots y_l^{k_l},$$

con $x_i, y_j \in X$, $m_i, k_j \in \mathbb{Z}$ no nulos, $n \leq l$ y de modo que en ningún miembro hay dos bases consecutivas iguales. Entonces

$$x_n^{-m_n} \cdots x_1^{-m_1} y_1^{k_1} \cdots y_l^{k_l} = 1.$$

Por la definición de subconjunto libre, esto sólo puede ocurrir si $x_1 = y_1$, luego tenemos que

$$x_n^{-m_n} \cdots x_2^{-m_2} y_1^{k_1 - m_1} y_2 \cdots y_l^{k_l} = 1,$$

pero esto sólo es posible si $m_1 = k_1$, con lo que tenemos

$$x_n^{-m_n} \cdots x_2^{-m_2} y_2 \cdots y_l^{k_l} = 1.$$

Repitiendo el argumento llegamos a que $x_i = y_i$, $m_i = k_i$ y, si fuera $n < l$, quedaría

$$y_{n+1}^{k_{n+1}} \cdots y_l^{k_l} = 1,$$

lo que contradice la definición de subconjunto libre, luego tiene que ser $n = l$ y así la expresión de cada $g \in G$ no trivial en las condiciones del enunciado es única.

Veamos ahora que X es una base de G. Para ello consideramos un grupo H y una aplicación $f : X \longrightarrow H$. Entonces definimos $f^* : G \longrightarrow H$ mediante

$$f^*(x_1^{m_1} \cdots x_n^{m_n}) = f(x_1)^{m_1} \cdots f(x_n)^{m_n}, \qquad f^*(1) = 1.$$

El hecho de que todo elemento de G admita una única expresión de la forma considerada justifica que f^* está bien definida y claramente extiende a f. Veamos que es un homomorfismo de grupos, es decir, que $f^*(g_1 g_2) = f^*(g_1) f^*(g_2)$. Claramente podemos suponer que $g_1 \neq 1 \neq g_2$. Entonces, expresando g_1 y g_2 en las condiciones del enunciado, tenemos que probar que

$$f^*(x_1^{m_1} \cdots x_n^{m_n} y_1^{k_1} \cdots y_l^{k_l}) = f^*(x_1^{m_1} \cdots x_n^{m_n}) f^*(y_1^{k_1} \cdots y_l^{k_l}).$$

Lo probamos primero en el caso en que $l = 1$, es decir, que

$$f^*(x_1^{m_1} \cdots x_n^{m_n} y_1^{k_1}) = f^*(x_1^{m_1} \cdots x_n^{m_n}) f(y_1)^{k_1}.$$

Para ello distinguimos si $y_1 = x_n$ o si $y_1 \neq x_n$. En el primer caso, si además $m_n + k_1 \neq 0$,

$$f^*(x_1^{m_1} \cdots x_n^{m_n} y_1^{k_1}) = f^*(x_1^{m_1} \cdots x_n^{m_n + k_1}) = f(x_1)^{m_1} \cdots f(x_n)^{m_n + k_1}$$

$$f(x_1)^{m_1} \cdots f(x_n)^{m_n} f(y_1)^{k_1} = f^*(x_1^{m_1} \cdots x_n^{m_n}) f(y_1)^{k_1}.$$

Si $m_n + k_1 = 0$ el cálculo es similar, eliminando la potencia correspondiente antes de aplicar f^*. En el segundo caso basta aplicar directamente la definición de f^*.

Ahora, razonando inductivamente obtenemos que

$$f^*(x_1^{m_1} \cdots x_n^{m_n} y_1^{k_1} \cdots y_l^{k_l}) = f^*(x_1^{m_1} \cdots x_n^{m_n}) f(y_1^{k_1}) \cdots f(y_l^{k_l})$$

$$= f^*(x_1^{m_1} \cdots x_n^{m_n}) f^*(y_1^{k_1} \cdots y_l^{k_l}).$$

Es claro que f^* es la única extensión posible de f, luego concluimos que X es una base. Supongamos ahora que X es una base de G y veamos que es un sistema generador. Para ello llamamos G_0 el subgrupo generado por X. Tenemos que probar que $G_0 = G$.

La inclusión $X \longrightarrow G_0$ se extiende a un homomorfismo $i : G \longrightarrow G_0$. Consideramos también la inclusión $j : G_0 \longrightarrow G$. Entonces $i \circ j : G \longrightarrow G$ es un homomorfismo que se restringe a la identidad en X. Por la unicidad de las extensiones tiene que ser la identidad, lo que implica que j es suprayectiva, luego $G = G_0$.

Dejamos pendiente para más adelante la prueba de que toda base es un subconjunto libre (la veremos tras el teorema 3.13). ∎

Veamos ahora que un grupo libre está completamente determinado por el cardinal de cualquiera de sus bases:

Teorema 3.11 *Si G y H son grupos libres con bases X e Y, respectivamente, entonces G y H son isomorfos si y sólo si X e Y tienen el mismo cardinal.*

DEMOSTRACIÓN: Si $f : X \longrightarrow Y$ es una aplicación biyectiva, a partir de ella obtenemos homomorfismos de grupos $f^* : G \longrightarrow H$ y $(f^{-1})^* : H \longrightarrow G$ que extienden a f y f^{-1}, respectivamente, luego $f^* \circ (f^{-1})^*$ es un homomorfismo de G en sí mismo que extiende a la identidad en X, luego por la unicidad es la identidad, e igualmente sucede con $(f^{-1})^* \circ f^*$, luego ambas extensiones son isomorfismos mutuamente inversos.

Supongamos ahora que existe un isomorfismo $f^* : G \longrightarrow H$. Sea $\mathrm{Hom}(G, C_2)$ el conjunto de todos los homomorfismos de G en un grupo cíclico de orden 2, e igualmente con H. Tenemos una biyección $\mathrm{Hom}(G, C_2) \longrightarrow \mathrm{Hom}(H, C_2)$ dada por $g \mapsto (f^*)^{-1} \circ g$, luego ambos conjuntos tienen el mismo cardinal. Pero por definición de grupo libre hay tantos homomorfismos de G en C_2 como aplicaciones de X en C_2, e igualmente con H e Y, luego:

$$2^{|X|} = |\mathrm{Hom}(G, C_2)| = |\mathrm{Hom}(H, C_2)| = 2^{|Y|}.$$

Si X es finito, esto implica que Y también es finito y que $|X| = |Y|$. Obviamente, llegamos a la misma conclusión si Y es finito, luego sólo queda el caso en que ambas bases son infinitas. Este caso requiere más resultados sobre cardinales de los que hemos presentado aquí, pero consiste en probar[1] (y esto requiere AE) que en tal caso $|G| = |X|$, con lo que, de hecho, $|X| = |G| = |H| = |Y|$. ∎

Definición 3.12 Llamamos *rango* de un grupo libre al cardinal de cualquiera de sus bases.

En estos términos, el teorema anterior afirma que dos grupos libres son isomorfos si y sólo si tienen el mismo rango.

El teorema siguiente prueba la existencia de grupos libres, pero, sobre todo, nos da una idea más concreta de cómo son sus elementos:

[1] En realidad la prueba es sencilla: si llamamos $\bar{X} = X \cup X^{-1}$ (donde X^{-1} es el conjunto de los inversos de los elementos de X), el hecho de que X sea un sistema generador implica que la aplicación que a cada sucesión finita $(x_1, \ldots, x_n)$ de elementos de $\bar{X}$ le asigna $x_1 \cdots x_n \in G$ es suprayectiva, luego el cardinal de G es menor o igual que el cardinal del conjunto de sucesiones finitas en $\bar{X}$, y la teoría de cardinales da que dicho cardinal es $|\bar{X}| = |X|$. Por lo tanto $|G| \leq |X|$, y la otra desigualdad es trivial.

Teorema 3.13 *Existen un grupo libre de cualquier rango posible, y es único salvo isomorfismo.*

DEMOSTRACIÓN: La unicidad ya la tenemos probada. Fijemos un conjunto arbitrario X_0 y vamos a construir un grupo libre de rango $|X_0|$. Podemos suponer que X_0 no es vacío, pues ya sabemos que el grupo trivial es libre de rango 0.

Llamamos $X = X_0 \times \{0\}$, $X^{-1} = X_0 \times \{1\}$ y $\bar{X} = X \cup X^{-1}$. Obviamente, $|X| = |X_0|$, por lo que $|X|$ es un cardinal arbitrario (no nulo). Consideramos la biyección $\bar{X} \longrightarrow \bar{X}$ dada por $(x,0)^{-1} = (x,1)$, $(x,1)^{-1} = (x,0)$. Notemos que si $x \in \bar{X}$, entonces $(x^{-1})^{-1} = x$.

Sea L el conjunto de todas las sucesiones finitas en $\bar{X}$ tales que no hay ningún término x precedido o seguido de x^{-1}. Entendemos que L contiene también la sucesión vacía de longitud 0, que representaremos por 1.

Los elementos de L se llaman *palabras reducidas* (donde el adjetivo reducidas hace referencia a la condición que excluye las parejas xx^{-1} o $x^{-1}x$). Podemos considerar que $\bar{X} \subset L$ identificando cada elemento de $\bar{X}$ con una sucesión de longitud 1.

Por ejemplo, si $X = \{a, b\}$, entonces los elementos de L de longitud ≤ 2 son

$$1, \quad a, \quad b, \quad a^{-1}, \quad b^{-1}, \quad aa, \quad ab, \quad ab^{-1}, \quad ba, \quad ba^{-1}, \quad bb,$$
$$a^{-1}a^{-1}, \quad a^{-1}b, \quad a^{-1}b^{-1}, \quad b^{-1}a, \quad b^{-1}a^{-1}, \quad b^{-1}b^{-1}.$$

Para cada $x \in \bar{X}$, definimos $\pi_x : L \longrightarrow L$ como la aplicación que a cada sucesión $p \in L$ le añade x como último término si no termina en x^{-1}, o le quita su último término si éste es x^{-1}.

Por ejemplo, $\pi_{a^{-1}}(ab) = aba^{-1}$, $\pi_{a^{-1}}(ba) = b$.

Se comprueba inmediatamente que $\pi_x \circ \pi_{x^{-1}} = \pi_{x^{-1}} \circ \pi_x$ son ambas la identidad en L, luego las aplicaciones π_x son biyectivas y $(\pi_x)^{-1} = \pi_{x^{-1}}$.

Así tenemos definida $\pi : \bar{X} \longrightarrow \Sigma_L$ dada por $x \mapsto \pi_x$, que a su vez podemos extender a una aplicación $\pi : L \longrightarrow \Sigma_L$ mediante $\pi_{x_1 \cdots x_n} = \pi_{x_1} \circ \cdots \circ \pi_{x_n}$ (con el convenio de que π_1 es la identidad en L). Teniendo en cuenta que $\pi_x(1) = x$, para todo $x \in \bar{X}$, vemos que $\pi_p(1) = p$ para todo $p \in L$, luego π es inyectiva.

Ahora observamos que $\pi[L]$ es el subgrupo de Σ_L generado por $\pi[X]$.

En efecto, obviamente $1 = \pi_1 \in \pi[L]$. Veamos ahora que si $g, h \in \pi[L]$, también $gh \in \pi[L]$. Podemos suponer que ambos factores son no triviales. Entonces $g = \pi_{x_1} \circ \cdots \circ \pi_{x_n}$ y $h = \pi_{y_1} \circ \cdots \circ \pi_{y_m}$, para ciertos $x_i, y_j \in \bar{X}$, y un razonamiento inductivo nos reduce la comprobación al caso en que $h = \pi_y$, con $y \in \bar{X}$. Basta distinguir dos casos, según si $y = x_n^{-1}$ o bien $y \neq x_n^{-1}$. En el primer caso $gh = \pi_{x_1 \cdots x_{n-1}} \in \pi[L]$ y en el segundo $gh = \pi_{x_1 \cdots x_n y} \in \pi[L]$.

Por otra parte, $x_n^{-1} \cdots x_1^{-1} \in L$, y $\pi^{-1}_{x_1 \cdots x_n} = \pi_{x_n^{-1} \cdots x_1^{-1}} \in \pi[L]$, luego $\pi[L]$ es un subgrupo, obviamente generado por $\pi[\bar{X}]$, pero como los elementos de $\pi[X^{-1}]$ son los inversos de los elementos de $\pi[X]$, de hecho $\pi[L]$ está generado por $\pi[X]$.

Consideramos en L la estructura de grupo que convierte a π en un isomorfismo. Así, L es un grupo generado por X, de modo que si $x \in \bar{X}$, se cumple que x^{-1} es su inverso respecto a dicha estructura, pues

$$x \cdot x^{-1} = \pi^{-1}(\pi_x \circ \pi_{x^{-1}}) = \pi^{-1}(1) = 1,$$

e igualmente $x^{-1} \cdot x = 1$.

Similarmente, si $x_1 \cdots x_n \in L$, con cada $x_i \in \bar{X}$, tenemos que

$$x_1 \cdots x_n = \pi^{-1}(\pi_{x_1} \circ \cdots \circ \pi_{x_n}) = x_1 \cdot \ \cdots \ \cdot x_n,$$

es decir, que la sucesión $x_1 \cdots x_n$ es el producto de los elementos $x_1, \ldots, x_n$ respecto de la estructura de grupo.

En definitiva, tenemos que L es un grupo en el que todo elemento no trivial se expresa de forma única como producto $x_1 \cdots x_n$ de elementos de X o de sus inversos de modo que en la expresión no aparece ningún x precedido o seguido de x^{-1}.

Esto implica que X es un generador libre de L, pues, ciertamente, todo $g \in L$ no trivial se expresa en la forma $g = x_1^{m_1} \cdots x_n^{m_n}$, donde no hay dos bases consecutivas iguales y los exponentes son no nulos, y la expresión es única, pues si hubiera dos, desarrollando cada potencia $x_i^{m_i} = x_i^{\epsilon_i} \cdots x_i^{\epsilon_i}$, con $\epsilon_i = \pm 1$, tendríamos dos expresiones distintas de g en las condiciones anteriores. Por la parte ya probada del teorema 3.10 tenemos que X es una base de L. ∎

Así pues, un grupo libre de base X (salvo isomorfismo) no es más que el conjunto de todas las palabras reducidas que pueden formarse con los elementos de X. Por ejemplo, si $X = \{a, b, c\}$, entonces una palabra reducida "típica" es de la forma

$$g = a^3 b^5 c^{-3} b^{-1} c^2,$$

donde "reducida" significa que no puede simplificarse de forma obvia, como sería el caso de $ab^3b^{-2}cc^2$, que podría reducirse a abc^3.

Notemos que hemos construido un grupo libre de un cardinal arbitrario cuya base es un generador libre. Esto nos permite probar la parte que nos faltaba del teorema 3.10:

Sea X una base de un grupo G. Ya sabemos que X es un sistema generador, y ahora podemos probar que es libre. En efecto, si tenemos una expresión $x_1^{m_1} \cdots x_n^{m_n} = 1$, con $x_i \in X$, $m_i \in \mathbb{Z}$ y no hay dos bases consecutivas iguales, consideramos un grupo L que tenga un generador libre X' del mismo cardinal que X (acabamos de probar su existencia) y tomamos $f : X \longrightarrow X'$ biyectiva, que se extiende a un homomorfismo $f^* : G \longrightarrow L$. Entonces $f^*(x_1)^{m_1} \cdots f^*(x_n)^{m_n} = 1$ y no hay dos bases consecutivas iguales, luego tiene que ser $m_1 = \cdots m_n = 0$. ∎

Ahora ya es inmediato que todo grupo libre de rango mayor o igual que 2 es no abeliano, pues tiene un generador libre con al menos dos elementos.

Ejercicio: Probar que si X es una base de un grupo G y $X_0 \subset X$, entonces X es una base de $G_0 = \langle X_0 \rangle$.

Puede probarse que todo subgrupo de un grupo libre es libre, pero en general no es cierto que su rango sea menor o igual que el rango del grupo. Veamos un ejemplo:

Teorema 3.14 *Si G es un grupo libre de rango 2, su subgrupo derivado G' es libre de rango numerable.*

DEMOSTRACIÓN: Sea $X = \{a, b\}$ una base de G. Sea $f : X \longrightarrow \mathbb{Z}^2$ la aplicación dada por $f(a) = (1, 0)$ y $f(b) = (0, 1)$. Entonces f se extiende a un homomorfismo de grupos $f^* : G \longrightarrow \mathbb{Z}^2$ y sea N su núcleo. Como $G/N \cong \mathbb{Z}^2$ es abeliano, tiene que ser $G' \leq N$, luego podemos definir $\bar{f}^* : G/G' \longrightarrow \mathbb{Z}^2$, de modo que $\bar{f}^*([a]) = (1, 0)$ y $\bar{f}^*([b]) = (0, 1)$.

Por otro lado, como G/G' es un $\mathbb{Z}$-módulo y $\mathbb{Z}^2$ es un $\mathbb{Z}$-módulo libre, podemos definir un homomorfismo de módulos (luego de grupos) $g : \mathbb{Z}^2 \longrightarrow G/G'$ determinado por que $g(1, 0) = [a]$, $g(0, 1) = [b]$. Como $\bar{f}^* \circ g$ y $g \circ \bar{f}^*$ coinciden con la identidad sobre un sistema generador, ambos son la identidad, luego ambos son isomorfismos.

Así pues un elemento $g \in G$ cumple $g \in G'$ si y sólo si $\bar{f}^*([g]) = (0, 0)$. Pero, explícitamente, si

$$g = a^{m_1} b^{n_1} \cdots a^{m_k} b^{n_k},$$

tenemos que $\bar{f}^*([g]) = \left(\sum_{i=1}^{k} m_i, \sum_{j=1}^{k} n_j \right)$. Esto implica que el subgrupo derivado G' está generado por los conmutadores de la forma $[a^m, b^n] = a^{-m} b^{-n} a^m b^n$.

En efecto, usando que $a^m b^n = b^n a^m [a^m, b^n]$, podemos operar la expresión de un $g \in G'$ en términos de la base hasta agrupar todas las potencias de a y b:

$$\begin{aligned} a^{m_1} b^{n_1} \cdots a^{m_k} b^{n_k} &= a^{m_1} b^{n_1} \cdots a^{m_{k-1}} b^{n_{k-1}+n_k} a^{m_k} [a^{m_k}, b^{n_k}] \\ &= a^{m_1} b^{n_1} \cdots a^{m_{k-1}+m_k} b^{n_{k-1}+n_k} [b^{n_{k-1}+n_k}, a^{m_k}][a^{m_k}, b^{n_k}]. \end{aligned}$$

Teniendo en cuenta que tanto los m_i como los n_i suman 0, tras un número finito de pasos llegamos a un producto de conmutadores de la forma $[a^m, b^n]$ o bien de la forma $[b^n, a^m] = [a^m, b^n]^{-1}$.

Veamos ahora que $X' = \{[a^m, b^n] \mid m, n \in \mathbb{Z} \setminus \{0\}\}$ es una base de G'. Acabamos de probar que es un generador, luego sólo tenemos que probar que es libre. Para ello suponemos que

$$[a^{m_1}, b^{n_1}]^{k_1} \cdots [a^{m_l}, b^{n_l}]^{k_l} = 1,$$

donde no hay dos bases consecutivas iguales. Tenemos que probar que todos los k_i son nulos. En caso contrario, eliminando los términos que sí tengan exponente nulo, podemos suponer que ninguno es nulo. Sustituyendo cada conmutador por su definición y cada potencia de exponente k_i por $|k_i|$ factores con exponente ± 1, obtenemos una expresión

$$[a^{m_1}, b^{n_1}]^{\epsilon_1} \cdots [a^{m_r}, b^{n_r}]^{\epsilon_r} = 1,$$

donde $\epsilon_i = \pm 1$ y ningún conmutador está precedido o seguido por su inverso. Pongamos, por concretar, que $\epsilon_1 = 1$. Entonces, la expresión empieza por $a^{-m_1}b^{-n_1}a^{m_1}b^{n_1}\cdots$. Si $\epsilon_2 = 1$, la expresión continúa con

$$a^{-m_1}b^{-n_1}a^{m_1}b^{n_1}a^{-m_2}b^{-n_2}a^{m_2}b^{n_2}\cdots,$$

donde no hay dos bases consecutivas iguales. Si, por el contrario, $\epsilon_2 = -1$, tenemos

$$a^{-m_1}b^{-n_1}a^{m_1}b^{n_1-n_2}a^{-m_2}b^{n_2}a^{m_2}\cdots,$$

donde, o bien $n_1 - n_2 \neq 0$, o bien $n_1 - n_2 = 0$ y entonces $m_1 - m_2 \neq 0$ (porque los dos conmutadores consecutivos no pueden ser mutuamente inversos) y tenemos

$$a^{-m_1}b^{-n_1}a^{m_1-m_2}b^{n_2}a^{m_2}\cdots$$

En cualquier caso, seguimos teniendo una secuencia no vacía sin bases consecutivas iguales. En general, cada vez que consideramos un nuevo conmutador, o bien se añaden cuatro nuevos términos a la sucesión, o bien dos se contraen y sólo añadimos tres, o bien hay dos contracciones y sólo añadimos uno, pero, como mínimo, se añade uno. Por lo tanto, al llegar hasta el último conmutador, acabamos con una expresión que contradice que X sea libre. ∎

Teniendo en cuenta que todo subconjunto de un conjunto libre es libre, vemos que un grupo libre de rango 2 contiene subgrupos libres de todos los rangos finitos (además de subgrupos de rango numerable).

Ejemplo Aunque puede parecer que los grupos libres son unos objetos muy "artificiosos", lo cierto es que aparecen de forma natural en algunos contextos. Uno de los más importantes es la topología algebraica, pero también existen ejemplos geométricos sencillos. Por ejemplo, consideremos el grupo $G = \mathrm{LG}(3,\mathbb{R})$ formado por las matrices regulares 3×3 con coeficientes reales, que es ciertamente un grupo con el producto de matrices, y en él los elementos

$$\sigma = \frac{1}{7}\begin{pmatrix} 6 & 2 & -3 \\ 2 & 3 & 6 \\ 3 & -6 & 2 \end{pmatrix}, \qquad \tau = \frac{1}{7}\begin{pmatrix} 2 & 6 & -3 \\ -6 & 3 & 2 \\ 3 & 2 & 6 \end{pmatrix}.$$

Vamos a probar que el conjunto $X = \{\sigma, \tau\}$ es libre, con lo que $L = \langle \sigma, \tau\rangle$ es un subgrupo[2] libre en G de rango 2.

Supongamos, por reducción al absurdo, que se cumple

$$x_1^{m_1}\cdots x_n^{m_n} = 1,$$

donde los exponentes son enteros no nulos, cada x_i es σ o τ y no hay dos potencias consecutivas con la misma base.

[2]En la sección 4.3 de [G] hemos visto que las matrices σ y τ son, más concretamente las matrices (respecto de la base canónica) de dos giros en $\mathbb{R}^3$ respecto que ejes que pasan por el origen de coordenadas, así como que el conjunto de todos estos giros forman un grupo (isomorfo al grupo formado por sus matrices asociadas). Por lo tanto, en realidad vamos a demostrar que el grupo de todos los giros contiene un subgrupo libre de rango 2.

En primer lugar veamos que podemos suponer sin pérdida de generalidad que $x_1 = \sigma$ y que $m_1 > 0$. En efecto, si $x_1 = \tau$ y $x_n = \tau$, entonces

$$\sigma x_1^{m_1} \cdots x_n^{m_n} \sigma^{-1} = 1$$

es otra expresión como la dada, pero que empieza por σ. Si $x_1 = \tau$ y $x_n = \sigma$ tenemos igualmente

$$\sigma x_1^{m_1} \cdots x_n^{m_n - 1} = 1,$$

donde puede suceder que $m_n = 1$, en cuyo caso suprimimos la última potencia. Si $x_1 = \sigma$, pero $m_1 < 0$, y $x_n = \tau$, hacemos

$$\sigma x_2^{m_2} \cdots x_n^{m_n} \sigma^{m_1 - 1} = 1.$$

Por último, si $x_1 = \sigma$ con $m_1 < 0$ y $x_n = \sigma$, entonces hacemos

$$\sigma x_2^{m_2} \cdots x_n^{m_n + m_1 - 1} = 1,$$

eliminando la última potencia si su exponente es nulo.

Ahora conviene considerar las matrices

$$M_\sigma = \begin{pmatrix} 6 & 2 & -3 \\ 2 & 3 & 6 \\ 3 & -6 & 2 \end{pmatrix}, \qquad M_\tau = \begin{pmatrix} 2 & 6 & -3 \\ -6 & 3 & 2 \\ 3 & 2 & 6 \end{pmatrix},$$

$$M_\sigma^- = \begin{pmatrix} 6 & 2 & 3 \\ 2 & 3 & -6 \\ -3 & 6 & 2 \end{pmatrix}, \quad M_\tau^- = \begin{pmatrix} 2 & -6 & 3 \\ 6 & 3 & 2 \\ -3 & 2 & 6 \end{pmatrix}.$$

Una simple comprobación muestra que

$$M_\sigma = 7\sigma, \quad M_\tau = 7\tau, \quad M_\sigma^- = 7\sigma^{-1}, \quad M_\tau^- = 7\tau^{-1}.$$

Podemos expresar la relación que estamos suponiendo como

$$\frac{1}{7^n} x_1^{m_1} \cdots x_n^{m_n} = 1,$$

donde ahora cada x_i es una de las matrices M_σ, M_τ, M_σ^-, M_τ^- (y, concretamente, $x_1 = M_\sigma$) y todos los exponentes son $m_i > 0$. En particular,

$$(1,0,0)\frac{1}{7^n} x_1^{m_1} \cdots x_n^{m_n} = (1,0,0),$$

o, equivalentemente,

$$(1,0,0) x_1^{m_1} \cdots x_n^{m_n} = (7^n, 0, 0).$$

Todas las matrices tienen coeficientes enteros, por lo que, si se cumple esta igualdad, también se cumple la igualdad correspondiente cuando sustituimos los coeficientes por sus imágenes en $k = \mathbb{Z}/7\mathbb{Z}$, en cuyo caso equivale a

$$(1,0,0) x_1^{m_1} \cdots x_n^{m_n} = (0,0,0).$$

Vamos a ver que esto es imposible. Definimos cuatro subconjuntos de k^3:

$$\begin{aligned} V_\sigma &= \{(3,1,2),(5,4,1),(6,2,4)\},\\ V_\sigma^- &= \{(3,2,6),(5,1,3)),(6,4,5)\}\\ V_\tau &= \{(1,5,4),(2,3,1),(4,6,2)\},\\ V_\tau^- &= \{(3,5,1),(5,6,4),(6,3,2)\}. \end{aligned}$$

Ahora observamos que, siempre módulo 7,:

$$(1,0,0)M_\sigma = (6,2,-3) = (6,2,4) \in V_\sigma.$$

A continuación, una comprobación rutinaria muestra los cuatro hechos siguientes:

1. Si $v \in V_\sigma \cup V_\tau \cup V_\tau^-$, entonces $vM_\sigma \in V_\sigma$,
2. Si $v \in V_\sigma^- \cup V_\tau \cup V_\tau^-$, entonces $vM_\sigma^- \in V_\sigma^-$,
3. Si $v \in V_\tau \cup V_\sigma \cup V_\sigma^-$, entonces $vM_\tau \in V_\tau$,
4. Si $v \in V_\tau^- \cup V_\sigma \cup V_\sigma^-$, entonces $vM_\tau^- \in V_\tau^-$.

De aquí se sigue que al ir multiplicando el vector $(1,0,0)$ por las matrices x_i, se va transformando sucesivamente en los vectores de los cuatro conjuntos que hemos definido, luego nunca se convierte en el vector $(0,0,0)$.

Más detalladamente: partimos de $(6,2,4) \in V_\sigma$, y la matriz siguiente no puede ser M_σ^- (porque σ no puede ir seguido de σ^{-1}), con lo que, al aplicarle M_σ, M_τ o M_τ^-, obtenemos un vector del conjunto correspondiente. Si, por ejemplo, hemos llegado a V_τ, habrá sido multiplicando por M_τ, luego la matriz siguiente no puede ser M_τ^-, luego al aplicar cualquiera de las otras tres matrices, obtenemos un vector del conjunto correspondiente, etc.

Así pues, el grupo de las matrices regulares 3×3 con coeficientes en $\mathbb{R}$ (o incluso en $\mathbb{Q}$) contiene un subgrupo libre de rango 2, luego por el teorema anterior contiene de hecho subgrupos libres de cualquier rango finito o numerable. ∎

3.3 Presentaciones de grupos

Tal y como anticipábamos en la sección anterior, el concepto de grupo libre nos proporciona una de las formas más útiles de expresar la estructura de un grupo de forma abstracta, es decir, sin adoptar ninguna construcción concreta del mismo. (En realidad sí que vamos a adoptar una construcción concreta, pero ésta será irrelevante, como lo es la construcción concreta de los números enteros, racionales, reales, complejos, los polinomios, etc.)

Se trata de lo que se conoce como *presentación de un grupo mediante generadores y relaciones.* La idea es que vamos a dar definiciones precisas que nos permitirán, por ejemplo, definir el grupo cíclico de orden n como

$$C_n = \langle a \mid a^n = 1 \rangle,$$

o expresar el teorema 1.38 simplemente como

$$D_{2n} = \langle a, b \mid a^n = b^2 = 1,\ a^b = a^{-1} \rangle,$$

donde esto puede tomarse como definición "abstracta" del grupo diédrico.

El punto de partida es la siguiente consecuencia inmediata de la definición de grupo libre:

Teorema 3.15 *Todo grupo es isomorfo a un cociente de un grupo libre.*

DEMOSTRACIÓN: Sea G un grupo y sea Y un sistema generador de G, sea L un grupo libre de rango $|Y|$ y sea X una base de L. Sea $f : X \longrightarrow Y$ una biyección, que se extiende a un epimorfismo de grupos $f^* : L \longrightarrow G$. Si N es el núcleo de f^*, entonces $L/N \cong G$. ∎

Aunque los grupos libres sean grupos bastante complicados, vamos a ver que describir grupos como cocientes de grupos libres resulta muy conveniente.

Antes de explicar el procedimiento general, consideremos el teorema 1.38, que ya hemos mencionado más arriba, según el cual, todo grupo $G = \langle \sigma, \tau \rangle$ de orden $2n$ generado por dos elementos que satisfagan las relaciones

$$\sigma^n = \tau^2 = 1, \quad \tau^{-1}\sigma\tau = \sigma^{-1}$$

es isomorfo al grupo diédrico D_{2n}.

Las "relaciones" no son en principio objetos matemáticos, sino afirmaciones que pedimos que cumplan ciertos objetos matemáticos (los generadores de un grupo). Los grupos libres nos permiten convertir las relaciones en objetos:

Definición 3.16 Si L es un grupo libre de base X y $R \subset L$, diremos que R es un conjunto de *relaciones* sobre el generador X. Diremos que un generador Y de un grupo G *satisface* el conjunto de relaciones R si existe una aplicación $f : X \longrightarrow Y$ suprayectiva cuya extensión $f^* : L \longrightarrow G$ cumple que $f^*[R] = 1$.

Por ejemplo, en estos términos, cuando en el teorema 1.38 hablamos de un grupo que satisface las relaciones indicadas, podemos entenderlo en el sentido que acabamos de introducir, es decir, consideramos un grupo libre L de rango 2 con base $\{a, b\}$ y el conjunto de relaciones $R = \{a^n, b^2, b^{-1}aba\}$. Cuando decimos que un grupo $G = \langle \sigma, \tau \rangle$ satisface el conjunto de relaciones R, queremos decir que la aplicación $f : \{a, b\} \longrightarrow \{\sigma, \tau\}$ se extiende a un epimorfismo $f^* : L \longrightarrow G$ de modo que

$$f^*(a^n) = \sigma^n = 1, \quad f^*(b^2) = \tau^2 = 1, \quad f^*(b^{-1}aba) = \tau^{-1}\sigma\tau\sigma = 1.$$

Esto es justo la hipótesis que requiere el teorema 1.38.

Puede parecer retorcido expresarlo en estos términos, pero así podemos dar la definición general siguiente:

Definición 3.17 Sea L un grupo libre de base X, sea $R \subset L$ un conjunto de relaciones y sea N la *envoltura normal* de R, es decir, la intersección de todos los subgrupos normales de L que contienen a R (que obviamente es un subgrupo normal de L). Cuando hablemos del *grupo definido por los generadores X y las relaciones R* nos referiremos al grupo cociente

$$\langle X \mid R\rangle = L/N.$$

Por ejemplo, el grupo

$$\left\langle a, b \mid a^n, b^2,\ b^{-1}aba\right\rangle$$

es, por definición, el grupo L/N, donde L es el grupo libre de base $\{a, b\}$ y N es la envoltura normal de $R = \{a^n, b^2, b^{-1}aba\}$.

En general, el grupo $\langle X \mid R\rangle$ está generado por $\bar{X} = \{xN \mid x \in X\}$, y este generador satisface las relaciones R, ya que la aplicación $f : X \longrightarrow \bar{X}$ dada por $f(x) = xN$ se extiende a un epimorfismo $f^* : L \longrightarrow L/N$ que no es sino la proyección natural en el cociente, luego $f^*[R] = 1$, ya que $R \subset N$.

En el ejemplo concreto $G = \left\langle a, b \mid a^n, b^2,\ b^{-1}aba\right\rangle$, tenemos que $G = \langle \bar{a}, \bar{b}\rangle$, donde $\bar{a} = aN$, $\bar{b} = bN$, y se cumple que $\bar{a}^n = \bar{b}^2 = 1$, $\bar{b}^{-1}\bar{a}\bar{b}\bar{a} = 1$. En la práctica expresaremos los grupos definidos por generadores y relaciones en la forma

$$G = \left\langle a, b \mid a^n = b^2 = 1,\ b^{-1}aba = 1\right\rangle,$$

donde hay que entender que aquí a, b representan en realidad a las clases $\bar{a}, \bar{b}$ (y, en particular, no podemos asegurar *a priori* que sean elementos distintos de G). Esta notación expresa el hecho de que, realmente, G admite un generador por dos elementos a, b (que en realidad son $\bar{a}, \bar{b}$) que cumplen las relaciones indicadas. Así, después de un rodeo teórico que nos ha llevado a tratar las relaciones como objetos (elementos de un grupo libre), volvemos a expresarlas en la práctica como auténticas relaciones. Más aún, no hay inconveniente en expresar las relaciones como ecuaciones equivalentes en las que el miembro derecho no es necesariamente trivial. Por ejemplo:

$$G = \left\langle a, b \mid a^n = b^2 = 1,\ b^{-1}ab = a^{-1}\right\rangle.$$

Lo importante es que esta expresión define un grupo concreto, a saber, un cierto cociente de un grupo libre de rango 2, que admite un sistema generador $\{a, b\}$ que cumple las relaciones indicadas. No podemos aplicar directamente el teorema 1.38 para concluir que $G \cong D_{2n}$, pues para ello necesitamos justificar que $|G| = 2n$.

En principio, un elemento de G es un producto finito de potencias de a alternadas con potencias de b, pero la relación $ab = ba^{-1}$ permite conmutar las potencias (alterando los exponentes) hasta reducirlo a la forma $a^k b^l$, y las relaciones $a^n = b^2 = 1$ permiten reducir los exponentes al rango $0 \le k < n$, $0 \le l \le 1$, lo que nos da que $|G| \le 2n$.

Para probar la desigualdad opuesta conviene probar un resultado general, que viene a decir que $\langle X \mid R\rangle$ es el mayor grupo que cumple las relaciones que lo definen:

Teorema 3.18 (von Dyck) *Sea $G = \langle X \mid R\rangle$ un grupo definido por generadores y relaciones y sea H un grupo con un generador que satisfaga las relaciones R. Entonces existe un epimorfismo de grupos $G \longrightarrow H$ (luego H es un cociente de G).*

DEMOSTRACIÓN: Sea Y un generador de H que satisfaga las relaciones R. Por definición, esto significa que si L es el grupo libre de base X, existe una aplicación $f : X \longrightarrow Y$ suprayectiva tal que la extensión $f^* : L \longrightarrow H$ cumple que $f^*[R] = 1$, luego R está contenido en el núcleo de f^*, que es un subgrupo normal, luego, si N es la clausura normal de R, también se cumple que N está contenido en el núcleo de f^*, luego f^* induce un epimorfismo $G = L/N \longrightarrow H$. ∎

Puesto que sabemos que el grupo diédrico D_{2n} tiene un generador que cumple las relaciones $a^n = b^2 = 1$, $b^{-1}ab = a^{-1}$, ahora podemos concluir que existe un epimorfismo

$$G = \left\langle a, b \mid a^n = b^2 = 1,\ b^{-1}ab = a^{-1}\right\rangle \longrightarrow D_{2n},$$

lo que implica que $2n = |D_{2n}| \leq |G|$ y, como habíamos probado la desigualdad opuesta, de hecho $|G| = 2n$ y el epimorfismo tiene que ser un isomorfismo.

En teoría es más conveniente adoptar como definición de grupo diédrico su presentación por generadores y relaciones:

$$D_{2n} = \left\langle a, b \mid a^n = b^2 = 1,\ b^{-1}ab = a^{-1}\right\rangle,$$

y considerar el grupo construido antes del teorema 1.38 como un ejemplo —entre otros muchos posibles— de grupo isomorfo a D_{2n}. Así, D_{2n} está definido exclusivamente por sus propiedades algebraicas, sin entrar en ninguna consideración sobre la naturaleza de sus elementos.

Similarmente, la definición abstracta del grupo cíclico de orden n es

$$C_n = \langle a \mid a^n = 1\rangle.$$

De esta definición podemos concluir inmediatamente que C_n es un grupo cíclico con un generador a que cumple $a^n = 1$, lo cual significa que su orden es divisor de n, luego $|C_n| \leq n$. Ahora bien, si tomamos cualquier grupo cíclico G de orden n, es obvio que su generador cumple la relación que define a C_n, luego tenemos un epimorfismo $C_n \longrightarrow G$, que prueba que $n = |G| \leq |C_n|$, luego concluimos que C_n tiene orden n. ∎

Es importante destacar que para determinar el tamaño real de un grupo presentado por generadores y relaciones es necesario encontrarle una realización concreta, es decir, encontrar un grupo concreto que cumpla las relaciones, pues

a priori no podemos asegurar que unas relaciones dadas no impliquen otras aparentemente más fuertes. Por ejemplo, se cumple que

$$\langle a, b \mid aba^{-1}b^{-2} = 1,\ a^{-2}b^{-1}ab = 1\rangle = 1.$$

En efecto, este grupo tiene un generador $\{a, b\}$ que cumple las relaciones $ab = b^2a$, $ab = ba^2$, luego $b^2a = ba^2$, luego $b = a$, luego $a^2 = a^3$, luego $b = a = 1$.

En este caso no ha sido difícil comprobar que el grupo era trivial, pero en otros casos puede ser mucho más complicado. Puede probarse que no existe ningún algoritmo para determinar si un elemento de un grupo finitamente presentado por generadores y relaciones es trivial o no.

Ejercicio: Probar que $\langle a, b \mid ab = ba\rangle \cong \mathbb{Z} \times \mathbb{Z}$.

El estudio que hemos hecho de la presentación del grupo D_{2n} puede considerarse "típico". Como ha quedado disperso al haberlo usado como hilo conductor de esta sección, lo resumimos aquí:

- Por una parte se prueba, analizando las relaciones, que los elementos del grupo D_{2n} definido por generadores y relaciones son de la forma a^kb^l, con $0 \leq k < n$, $0 \leq l \leq 1$, lo que en particular implica que $|D_{2n}| \leq 2n$.

- En segundo lugar encontramos una realización concreta del grupo, es decir, un grupo concreto que cumpla las relaciones indicadas y probamos que tiene orden $2n$. Concretamente, hemos encontrado un cociente del grupo diédrico infinito D_∞, que a su vez hemos definido como un grupo de permutaciones.

- Esto implica que existe un epimorfismo de D_{2n} en la realización concreta que hemos encontrado, y por lo tanto $|D_{2n}| = 2n$ y el epimorfismo es un isomorfismo.

A su vez, el grupo D_∞ también puede ser definido mediante generadores y relaciones y analizado según este esquema (con las variantes necesarias debidas a que es un grupo infinito, por lo que no podemos apoyarnos en su orden). Concretamente, podemos definir

$$D_\infty = \langle a, b \mid b^2 = 1,\ b^{-1}ab = a^{-1}\rangle.$$

El mismo análisis de las relaciones realizado en el caso finito nos permite concluir que los elementos de D_∞ son de la forma a^kb^l, con $0 \leq l \leq 1$. Si llamamos $G = \langle \sigma, \tau\rangle$ al grupo de permutaciones que hemos tomado como definición en la página 27, sabemos que cumple las relaciones que definen a D_∞, pero además sabemos que los elementos $\sigma^k b^l$, con $0 \leq l \leq 1$ son distintas dos a dos. Por lo tanto, tenemos un epimorfismo $f : D_\infty \longrightarrow G$ dado por $f(a^kb^l) = \sigma^k\tau^l$, luego $f(a^kb^l) = 1$ sucede sólo si $k = l = 0$, luego se trata de un isomorfismo.

El grupo de Klein Similarmente, una definición alternativa del grupo de Klein es:

$$V_4 = \langle a, b \mid a^2 = b^2 = 1,\, ab = ba \rangle .$$

En efecto, si tomamos esto como definición, es inmediato que todo elemento de V_4 se expresa en la forma $a^i b^j$, con $0 \leq i, j \leq 1$, por lo que $|V_4| \leq 4$, y tomando cualquier grupo G de orden 4 con elementos de orden 2 (por ejemplo $G = \{\pm 1\} \times \{\pm 1\}$), es claro que G cumple las relaciones de V_4, luego existe un epimorfismo $f : V_4 \longrightarrow G$, lo que prueba que $|V_4| = 4$ y, por consiguiente, todo grupo de orden 4 generado por dos elementos que satisfagan las relaciones de V_4 es isomorfo a V_4. ∎

Un razonamiento similar permite probar, por ejemplo, que

$$C_2 \times C_4 = \langle a, b \mid a^2 = b^4 = 1,\, ab = ba \rangle ,$$

de modo que todo grupo de orden 8 generado por dos elementos que cumplan las relaciones indicadas es de tipo $C_2 \times C_4$.

Otro ejemplo:

$$Q_8 = \{a, b \mid a^4 = 1,\, a^2 = b^2,\, a^b = a^{-1}\}.$$

En efecto, si llamamos G al grupo definido por las relaciones, como $a = i$, $b = j$ en Q_8 las cumplen obviamente, podemos afirmar que $|G| \geq 8$, y por otro lado, la relación $ab = ba^{-1}$ permite expresar todos los elementos de G en la forma $a^i b^j$, con $0 \leq i \leq 4$ y $0 \leq j \leq 1$, pues b^2 puede sustituirse por a^2, lo que prueba que $|G| = 8$ y, por consiguiente, G es isomorfo a cualquier grupo de orden 8 que cumpla las relaciones dadas. ∎

En todos los ejemplos de presentaciones que hemos analizado hemos contado con una relación de la forma $b^{-1}ab = a^{-1}$ que ha facilitado considerablemente la acotación del orden del grupo. Veamos ahora algunos ejemplos en los que necesitamos aplicar técnicas adicionales en ausencia de una relación similar:

Una presentación de A_4 Vamos a comprobar que

$$A_4 = \langle a, b \mid a^3 = b^3 = (ab)^2 = 1 \rangle .$$

Demostración: Llamemos G al grupo dado por la presentación. Por una parte es fácil ver que las permutaciones $a = (1, 2, 3)$, $b = (2, 3, 4)$ satisfacen las relaciones dadas así como que generan A_4, por lo que existe un epimorfismo $G \longrightarrow A_4$. Basta probar que $|G| \leq 12$.

Para ello llamamos $u = ab$ y $v = ba$. Como $u^a = a^{-1}aba = ba = v$, vemos que $v^2 = u^2 = 1$. Además

$$(uv)^2 = ab^2a^2b^2a = ab^{-1}a^{-1}b^{-1}a = a(ab)^{-1}(ab)^{-1}a^2 = au^{-2}a^2 = a^3 = 1,$$

lo que es equivalente a que $uvu^{-1}v^{-1} = 1$, es decir, a que $uv = vu$.

Por consiguiente, $V = \langle u, v\rangle$ es un subgrupo de G de orden 4. Además $u^a = v \in V$ y

$$v^a = a^{-1}ba^2 = a^{-1}b^{-1}b^2a^2 = (ba)^{-1}(ab)^{-1} = v^{-1}u^{-1} \in V.$$

Esto prueba que $H = \langle a\rangle \leq N_G(V)$ y $V \trianglelefteq N_G(V)$, luego por 1.34 tenemos que VH es un subgrupo de G de orden a lo sumo 12 y, como contiene a a y a $b = va^2$, de hecho $G = VH$ y $|G| \leq 12$. ∎

Una presentación de A_5 Hemos probado que A_5 es simple, por lo que a la hora de comprobar que

$$A_5 = \langle a, b \mid a^5 = b^3 = (ab)^2 = 1\rangle$$

no podemos apoyarnos en subgrupos normales intermedios como hemos hecho en el ejemplo anterior, pero podemos emplear un argumento similar.

Llamemos G al grupo definido por la presentación. Por una parte se comprueba que las permutaciones $\sigma = (1,2,3,4,5)$ y $\tau = (1,5,3)$ cumplen las relaciones que definen a G. También es fácil ver que generan A_5, pues $G_0 = \langle\sigma, \tau\rangle$ tiene elementos de orden 2, 3 y 5, luego su orden es al menos 30, pero no puede tener orden 30 porque entonces tendría índice 2 en A_5, luego sería normal. Por lo tanto existe un epimorfismo $G \longrightarrow A_5$ y basta probar que $|G| \leq 60$.

Llamemos $a_1 = b$ y $b_1 = a_1^{a^{-2}} = a^2ba^3$. Así $a_1^3 = b_1^3 = 1$. Ahora observamos que la relación $(ab)^2 = 1$ implica que $aba = b^2$. Usando esto repetidas veces obtenemos que

$$(a_1b_1)^2 = ba^2ba^3ba^2ba^3 = ba(aba)a(aba)(aba)a^2$$

$$= bab^2aba^2 = bab^2b^2a = baba = b^3 = 1.$$

Por lo tanto $H = \langle a_1, b_1\rangle$ satisface las relaciones que definen a A_4, luego $|H| \leq 12$ y basta probar que $|G/H| \leq 5$. Notemos que H no es necesariamente un subgrupo normal de G, por lo que G/H representa únicamente al conjunto de las clases de congruencia módulo H por la derecha.

Las cinco clases H, Ha, Ha^2, Ha^3, Ha^4 se transforman unas en otras cuando se multiplican por la derecha por a. Si probamos que sucede lo mismo cuando se multiplican por b, teniendo en cuenta que todo elemento de G se expresa como un producto con factores iguales a a o b, concluiremos que son todas las clases de G/H y habremos terminado. Ahora bien:

$$\begin{aligned}
Hb &= Ha_1 = H,\\
Hab &= Habaa^4 = Hb^2a^4 = Ha^4,\\
Ha^2b &= Ha^2ba^{-2}a^2 = Hb_1a^2 = Ha^2,\\
Ha^3b &= Ha^2abaa^4 = Ha^2b^2a^4 = Ha^2a^4 = Ha\\
Ha^4b &= Ha^3abaa^4 = Ha^3b^2a^4 = Haba^4 = Ha^4a^4 = Ha^3,
\end{aligned}$$

donde en los dos últimos cálculos hemos usado los anteriores. ∎

Una presentación de LE(2,5) En los ejemplos de presentaciones de grupos finitos que hemos estudiado hasta el momento siempre hemos contado con restricciones que acotaban el orden de los generadores. El ejemplo siguiente resulta mucho más difícil de tratar porque ya no está en ese caso.

Consideramos el grupo $\mathrm{LG}(2,5)$ formado por las matrices regulares 2×2 sobre el cuerpo $k=\mathbb{Z}/5\mathbb{Z}$ de 5 elementos y el subgrupo $\mathrm{LE}(2,5)$ formado por las matrices que tienen determinante 1.

Si llamamos $V=k^2$, el teorema [Al 4.38] nos da que las matrices regulares 2×2 con coeficientes en k se corresponden biunívocamente con los automorfismos de V. A su vez, fijada una base (e_1,e_2) de V, el teorema [Al 4.21] nos da que cada automorfismo f de V se corresponde biunívocamente con la base $(f(e_1),f(e_2))$ de V, luego el orden de $\mathrm{LG}(2,5)$ es igual al número de bases de V. Éste es fácil de calcular: como primer elemento de una base podemos tomar cualquier elemento no nulo de V, lo que nos deja 24 posibilidades. Una vez fijado este primer elemento, podemos completar una base con cualquier otro que no sea linealmente dependiente con el anterior, lo que nos deja 20 posibilidades. En total $|\mathrm{LG}(2,5)|=24\cdot 20=480$. Por último, el epimorfismo $\det:\mathrm{LG}(2,5)\longrightarrow k^*$ nos da que $|\mathrm{LE}(2,5)|=120$.

Vamos a probar que

$$\mathrm{LE}(2,5)=\langle a,b\mid a^5=b^3=(ab)^2\rangle.$$

Llamamos G al grupo definido por la presentación. A primera vista, uno podría conjeturar que se trata de un grupo infinito, pues nada parece indicar que los órdenes de sus generadores tengan que estar acotados.

Llamamos $\alpha=ab$ y $\beta=ba$. Así $\alpha^2=a^5=b^3$, de donde se sigue que α^2 conmuta con a y con b, luego $\alpha^2\in Z(G)$. Por otra parte,

$$\beta^2=baba=a^{-1}ababa=a^{-1}\alpha^2a=\alpha^2a^{-1}a=\alpha^2.$$

En particular tenemos que $\langle\alpha^2\rangle\trianglelefteq G$, y las clases de a y b en el cociente $G/\langle\alpha^2\rangle$ satisfacen las relaciones de la presentación de A_5 que hemos visto en el ejemplo anterior, luego $|G/\langle\alpha^2\rangle|\leq 60$ y basta probar que $\alpha^4=1$ para concluir que $|G|\leq 120$. Vamos a ver una prueba elemental, pero que requiere buena dosis de ingenio:

De la relación $b^3=abab$ deducimos que $b^2=aba$, luego $b=b^{-1}aba$, luego $ba^{-1}=b^{-1}ab$. Ahora consideramos el elemento

$$\gamma=\alpha\beta^{-1}=\alpha\beta\beta^{-2}=ab^2a\beta^{-2}=a^{-3}a^5a^{-1}b^{-1}b^3a^{-2}a^3\beta^{-2}$$

$$=a^{-3}\beta^2\beta^{-1}\beta^2a^{-2}a^3\beta^{-2}=a^{-3}(ba^{-1})a^3=a^{-3}b^{-1}aba^3=a^{ba^3},$$

donde en el penúltimo paso hemos utilizado la relación probada previamente. Así pues, γ es conjugado de a, luego $\gamma^5=(a^5)^{ba^3}=\alpha^2$.

Ahora partimos de $\alpha = \gamma\beta$, con lo que $\beta^2 = \alpha^2 = \gamma\beta\gamma\beta$, luego $\beta = \gamma\beta\gamma$ y $\beta^{-1}\gamma\beta = \gamma^{-1}$. Elevando a 5 resulta que $\beta^{-1}\gamma^5\beta = \gamma^{-5}$, lo que equivale a $\beta^2 = \beta^{-2}$, o también a que $\alpha^2 = \alpha^{-2}$, es decir, a que $\alpha^4 = 1$.

Con esto tenemos probado que $|G| \leq 120$. Por otra parte, es fácil ver que las matrices

$$\sigma = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

cumplen las relaciones de G, luego $G_0 = \langle \sigma, \tau \rangle \leq \mathrm{LE}(2,5)$ es una imagen de G. El razonamiento precedente se aplica en particular a G_0, con lo que podemos afirmar que $\alpha = \sigma\tau$ cumple que $\langle \alpha^2 \rangle$ es un subgrupo normal de G_0 (no trivial, pues ahora podemos comprobar que $\alpha^2 = -I$) y el cociente $G_0/\langle \alpha^2 \rangle$ cumple las relaciones de A_5, luego existe un epimorfismo $A_5 \longrightarrow G_0/\langle \alpha^2 \rangle$. Como A_5 no tiene subgrupos normales propios, su núcleo tiene que ser trivial, luego $|G_0/\langle \alpha^2 \rangle| = 60$ y $|G_0| = 120$, luego $G_0 = \mathrm{LE}(2,5)$ y existe un epimorfismo $G \longrightarrow \mathrm{LE}(2,5)$, que necesariamente es un isomorfismo. ∎

Grupos de automorfismos Ahora enfatizamos un hecho al que le podemos sacar mucho partido: si tenemos un grupo finito $G = \langle X, R \rangle$ presentado por generadores y relaciones y $H = \langle X' \rangle$ es otro grupo del mismo orden con un generador X' que cumple las relaciones, el teorema 3.18 no sólo nos da un isomorfismo $f : G \longrightarrow H$, sino un isomorfismo que hace corresponder los generadores X y X'.

Por ejemplo, si tenemos un grupo $G = \langle x, y \rangle$ de orden 8 de modo que $x^4 = 1$, $y^2 = x^2$, $x^y = x^{-1}$, es decir, de modo que cumple las relaciones de Q_8, podemos afirmar que existe un isomorfismo $f : Q_8 \longrightarrow G$ tal que $f(i) = x$, $f(j) = y$.

Por ejemplo, en la página 84 hemos probado que

$$\mathrm{Aut}\,(C_2 \times C_4) \cong D_8,$$

y para ello hemos usado que si $x, y \in A = C_2 \times C_4$ son elementos de orden 2 y 4 respectivamente y x no es un cuadrado, entonces, para cualquier otro par de generadores x', y' en las mismas condiciones, existe $f \in \mathrm{Aut}\, A$ tal que $f(x) = x'$ y $f(y) = y'$. Allí lo hemos razonado en términos de las posibles factorizaciones de A en producto directo, y un razonamiento alternativo se basa en que

$$A = \langle a, b \mid a^2 = b^4 = 1,\ ab = ba \rangle.$$

Claramente, cualquier par $x, y \in A$ en las condiciones indicadas es un generador que cumple las relaciones, pues, como x no es un cuadrado, $x \notin \langle y \rangle$, luego $\langle x \rangle \cap \langle y \rangle = 1$, luego $A = \langle x \rangle \langle y \rangle = \langle x, y \rangle$, luego la observación precedente implica la existencia del automorfismo requerido.

Similarmente, podemos probar que

$$\mathrm{Aut}\, V_4 \cong \Sigma_3.$$

En efecto, por una parte, llamando $\Omega = V_4 \setminus \{1\}$, como todo $f \in \operatorname{Aut} V_4$ cumple $f(1) = 1$, es claro que se restringe a una permutación de Ω, luego tenemos un monomorfismo de grupos

$$\operatorname{Aut} V_4 \longrightarrow \Sigma_\Omega \cong \Sigma_3$$

que a cada automorfismo le hace corresponder su restricción a Ω. Basta probar que $|\operatorname{Aut} V_4| = 6$, pues esto implica que el monomorfismo es un isomorfismo.

Ahora bien, tenemos que $V_4 = \langle a, b \mid a^2 = b^2 = 1,\ ab = ba\rangle$, y es claro que dos elementos cualesquiera $x, y \in V_4$ no triviales son un generador que cumple las relaciones. Por lo tanto, fijado un generador x, y, tenemos que, para cualquier par $x', y' \in V_4$ de elementos no triviales, existe un $f \in \operatorname{Aut} V_4$ que cumple $f(x) = x'$, $f(y) = y'$, lo cual implica que hay exactamente 6 automorfismos, ya que hay 6 pares ordenados (x', y') de elementos distintos de un conjunto de 3 elementos.

Como último ejemplo, veamos que

$$\operatorname{Aut}(D_8) \cong D_8.$$

Nos basamos en que $D_8 = \langle a, b \mid a^4 = b^2 = 1,\ a^b = a^{-1}\rangle$, observando que cada par $(a^i, a^j b)$, con $i = \pm 1$, $j = 0, 1, 2, 3$ es un generador de D_4 que cumple las mismas relaciones que (a, b), luego el teorema 3.18 nos da un $\phi \in \operatorname{Aut}(D_4)$ tal que $\phi(a) = a^i$, $\phi(b) = a^j b$. Recíprocamente, las imágenes de a yb por un automorfismo deben ser claramente de esta forma (pues $a^{\pm 1}$ son los únicos elementos de D_8 de orden 4 y $a^j b$ son los únicos elementos de orden 2 que no están en $Z(D_8)$). Concluimos que $|\operatorname{Aut}(D_8)| = 8$, pues tenemos dos posibilidades para i y cuatro para j.

En particular hemos visto que el grupo $\operatorname{Aut}(D_8$ actúa sobre el conjunto $\Omega = \{b, ab, a^2 b, a^3 b\}$, es decir, que la restricción determina un homomorfismo $\alpha : \operatorname{Aut}(D) \longrightarrow \Sigma_\Omega$. Se trata de un monomorfismo, pues si $\alpha(\phi) = 1$, entonces $\phi(a) = a$ y $\phi(ab) = ab = a\phi(b)$, luego $\phi(b) = b$, luego $\phi = 1$. Así pues, $\operatorname{Aut}(D)$ es isomorfo a un subgrupo de orden 8 de Σ_4, pero todos los subgrupos de orden 8 de Σ_4 son isomorfos a D_8. ∎

3.4 Productos semidirectos

Introducimos ahora una generalización del producto directo de grupos que nos permitirá construir grupos "de diseño" con características prefijadas. Para ello necesitamos el concepto de acción de un grupo sobre otro grupo.

El grupo $G = \Sigma_3$ tiene un subgrupo normal $N = \langle\sigma\rangle$ de orden 3 y tres subgrupos no normales de orden 2. Si $H = \langle\tau\rangle$ es uno de ellos, se cumple que $G = HN$ y $H \cap N = 1$. Si fuera $H \lhd G$, entonces tendríamos que $G = H \times N$ y G sería abeliano, que no es el caso. Sin embargo, vamos a ver que la estructura de Σ_3 está completamente determinada por los subgrupos H y N y la acción de H sobre N por conjugación. Esta acción respeta la estructura de grupo de N en el sentido siguiente:

Definición 3.19 Una *acción* de un grupo H sobre otro grupo N es un homomorfismo de grupos $\alpha : H \longrightarrow \operatorname{Aut} N$.

Notemos que $\operatorname{Aut} N \leq \Sigma_N$, por lo que una acción de H sobre N como grupo es una acción de H sobre N como conjunto a la que pedimos además que las permutaciones de N asociadas a los elementos de H no sean meras permutaciones, sino automorfismos. En términos de la acción $N \times H \longrightarrow N$ esto equivale a que se cumpla la propiedad adicional

$$(n_1 n_2)h = (n_1 h)(n_2 h).$$

Esta igualdad tiene un aspecto más natural si expresamos la acción exponencialmente, con lo que, en total, las propiedades que cumple una acción de un grupo sobre otro son:

1. $n^1 = n$,
2. $n^{h_1 h_2} = (n_1^h)^{h_2}$,
3. $(n_1 n_2)^h = n_1^h n_2^h$.

Por ejemplo, si $N \trianglelefteq G$, entonces cualquier subgrupo $H \leq G$, actúa sobre N por conjugación. La acción es el homomorfismo $\alpha : H \longrightarrow \operatorname{Aut}(N)$ dado por $\alpha_h(n) = n^h$.

Supongamos ahora que un grupo G se encuentra en la situación que hemos mostrado antes en el caso de Σ_3, es decir, que $G = HN$, donde $H \leq G$, $N \trianglelefteq G$ y $H \cap N = 1$. Entonces, todo elemento de G se expresa de forma única como $g = hn$, con $h \in H$ y $n \in N$. En efecto, la expresión es única porque si $h_1 n_1 = h_2 n_2$, entonces $h_2^{-1} h_1 = n_2 n_1^{-1} \in H \cap N = 1$, luego $h_1 = h_2$ y $n_1 = n_2$. Y el producto en G se puede expresar en términos del producto en H y en N y de la acción de H sobre N por conjugación:

$$(h_1 n_1)(h_2 n_2) = h_1 h_2 h_2^{-1} n_1 h_2 n_2 = (h_1 h_2)(n_1^{h_2} n_2).$$

Esto nos lleva a la definición siguiente:

Si H es un grupo que actúa sobre otro grupo N, el *producto semidirecto* $H[N]$ (respecto de la acción dada) es el conjunto $H[N] = H \times N$ con el producto dado por

$$(h_1, n_1)(h_2, n_2) = (h_1 h_2, n_1^{h_2} n_2).$$

Esta operación es asociativa:

$$((h_1, n_1)(h_2, n_2))(h_3, n_3) = (h_1 h_2, n_1^{h_2} n_2)(h_3, n_3) = (h_1 h_2 h_3, n_1^{h_2 h_3} n_2^{h_3} n_3),$$

$$(h_1, n_1)((h_2, n_2)(h_3, n_3)) = (h_1, n_1)(h_2 h_3, n_2^{h_3} n_3) = (h_1 h_2 h_3, n_1^{h_2 h_3} n_2^{h_3} n_3),$$

tiene por elemento neutro a $(1, 1)$ y $(h, n)^{-1} = (h^{-1}, (n_1^{h_1^{-1}})^{-1})$. Por lo tanto, $H[N]$ es un grupo.

Además tenemos monomorfismos $H \longrightarrow H[N]$, $N \longrightarrow H[N]$ dados por $h \mapsto (h,1)$ y $n \mapsto (1,n)$, respectivamente, que nos permiten identificar a H y N con subgrupos de $H[N]$. Más aún, la conjugación de un elemento de $N \leq H[N]$ por un elemento de $H \leq H[N]$ es

$$(1,n)^{(h,1)} = (h^{-1},1)(1,n)(h,1) = (h^{-1},n)(h,1) = (1,n^h),$$

de donde se desprende, por una parte, que $N \trianglelefteq H[N]$ y, más aún, que al identificar H y N con subgrupos de $H[N]$, la conjugación de un elemento $n \in N$ por un elemento $h \in H$ es el elemento $n^h \in N$ determinado por la acción dada de H sobre N.

La discusión previa a la definición del producto semidirecto prueba el teorema siguiente:

Teorema 3.20 *Si G es un grupo, $H \leq G$ y $N \trianglelefteq G$ son subgrupos tales que $G = HN$ y $H \cap N = 1$, entonces la aplicación $H[N] \longrightarrow G$ dada por $(h,n) \mapsto hn$ es un isomorfismo de grupos, donde el producto semidirecto es el definido por la acción de H sobre N por conjugación.*

Observemos que todo grupo H actúa sobre cualquier grupo N mediante la acción trivial $n^h = n$ (que se corresponde con el homomorfismo $H \longrightarrow \operatorname{Aut} N$ con imagen trivial) y, respecto de esta acción, $H[N] = H \times N$, luego el producto directo de dos grupos es siempre un caso particular de producto semidirecto.

Grupos diédricos Como primera aplicación del producto semidirecto, vamos a dar una construcción alternativa de los grupos diédricos. Tomamos como definición la presentación

$$D_{2n} = \{a, b \mid a^n = b^2 = 1,\ a^b = a^{-1}\}.$$

La tercera relación equivale a $ba = a^{-1}b$, y esto nos permite expresar cada elemento de D_{2n} en la forma $a^i b^j$, y las primeras relaciones permiten reducir los exponentes a los rangos $0 \leq i < n$, $0 \leq j < 2$, por lo que $|D_{2n}| \leq 2n$.

Para probar que $|D_{2n}| = 2n$ necesitamos encontrar un grupo de orden $2n$ que cumpla las relaciones, y para ello podemos emplear el producto semidirecto. Para ello tomamos un grupo cíclico $N = \langle\sigma\rangle$ de orden n y el automorfismo $\tau \in \operatorname{Aut} N$ dado por $\tau(g) = g^{-1}$, con lo que $H = \langle 1, \tau\rangle \leq \operatorname{Aut} N$ es un grupo que actúa sobre N, y el producto semidirecto $G = H[N]$ es un grupo de orden $2n$, que tiene un subgrupo cíclico normal $N = \langle\sigma\rangle$ de orden n y un subgrupo $H = \langle 1, \tau\rangle$, de modo que se cumple $G = HN = \langle\sigma, \tau\rangle$ y

$$\sigma^4 = \tau^2 = 1, \quad \sigma^\tau = \sigma^{-1}.$$

Por lo tanto, existe un epimorfismo $D_{2n} \longrightarrow G$, lo que implica que $|D_{2n}| = n$ y que el epimorfismo es en realidad un isomorfismo, luego el grupo que hemos construido es isomorfo a D_{2n}.

En otras palabras, D_{2n} puede verse como el producto semidirecto de un grupo C_n por un grupo C_2 respecto de la acción que al generador τ de C_2 le hace corresponder el automorfismo de C_n determinado por $g^\tau = g^{-1}$. (Notemos que D_∞ se puede construir del mismo modo.) ∎

Veamos algunos ejemplos de construcciones sencillas de productos semidirectos con propiedades específicas. Por ejemplo, el teorema 2.6 asegura que todo grupo de orden p^2 es abeliano. En cambio, ahora podemos probar que siempre hay grupos no abelianos de orden p^3:

Grupos no abelianos de orden p^3 Si p es cualquier primo, podemos construir un grupo no abeliano de orden p^3 observando que $\operatorname{Aut} C_{p^2} \cong U_{p^2}$, que es un grupo abeliano de orden $\phi(p^2) = (p-1)p$, luego existe un automorfismo $\tau \in \operatorname{Aut} C_{p^2}$ de orden p.

En realidad es fácil describirlo explícitamente. Un elemento de orden p en U_{p^2} es $[p+1]$, pues no es trivial y

$$[p+1]^p - [1] = \left[\sum_{i=1}^{p} \binom{p}{i} p^i\right] = 0,$$

pues todos los sumandos son obviamente múltiplos de p^2, luego $[p+1]^p = 1$ en U_{p^2}. Por lo tanto, si $C_{p^2} = \langle\sigma\rangle$, podemos tomar el automorfismo dado por $\sigma^\tau = \sigma^{p+1}$. Así, el producto semidirecto $C_p[C_{p^2}]$ es un ejemplo de grupo no abeliano de orden p^3. Para $p = 2$ es $\sigma^\tau = \sigma^3 = \sigma^{-1}$ y el grupo es D_8. ∎

He aquí un ejemplo similar:

Grupos no abelianos de orden pq Si p y q son dos primos tales que $q \mid p-1$, podemos construir un grupo no abeliano de orden pq. Basta observar que, según el teorema 1.17, se cumple que $\operatorname{Aut} C_q \cong U_q \cong C_{q-1}$, luego podemos tomar un automorfismo $\tau \in \operatorname{Aut} C_q$ de orden p, con lo que $C_p = \langle\tau\rangle$ es un grupo de orden p que actúa sobre C_q no trivialmente, y el producto semidirecto $C_p[C_q]$ es un grupo no abeliano de orden pq (es no abeliano porque la conjugación no es trivial). Más adelante veremos (véase 3.28) que la condición $q \mid p-1$ es necesaria. ∎

Ejemplo Consideremos los grupos

$$K_{4n} = \left\langle a, b \mid a^n = b^4 = 1,\ a^b = a^{-1} \right\rangle.$$

La última relación implica, más en general, que para todo entero r se cumple $(a^{-r})^b = a^r$, lo que se traduce en que $ba^r = a^{-r}b$, es decir, que una a se puede pasar a la izquierda de una b invirtiendo su exponente. Esto permite expresar cada elemento de K_{4n} en la forma $a^i b^j$, y las primeras relaciones permiten reducir los exponentes a $0 \le i < n$, $0 \le j < 4$, por lo que $|K_{4n}| \le 4n$.

Para obtener un grupo de orden $4n$ que satisfaga estas relaciones la construcción es obvia: como en el caso de los grupos diédricos, partimos de un grupo cíclico $N = \langle\sigma\rangle$ de orden n y de otro $H = \langle\tau\rangle$ de orden 4. Consideramos además el automorfismo $\bar\tau \in \operatorname{Aut} N$ dado por $\bar\tau(g) = g^{-1}$, de modo que $\langle\bar\tau\rangle$ es un subgrupo de $\operatorname{Aut} N$ de orden 2. Claramente podemos definir un epimorfismo de grupos $H \longrightarrow \langle\bar\tau\rangle \le \operatorname{Aut} N$ determinado por que $\tau \mapsto \bar\tau$. Este homomorfismo es una acción de H sobre N que nos permite construir el producto semidirecto

$G = H[N]$, que es un grupo de orden $4n$ que, identificando a H y a N con subgrupos de G, se cumple que $G = \langle \sigma, \tau \rangle$ y

$$\sigma^n = \tau^4 = 1, \qquad \sigma^\tau = \sigma^{-1}.$$

Por lo tanto existe un epimorfismo $K_{4n} \longrightarrow G$, que será de hecho un isomorfismo, pues ahora sabemos que $|K_{4n}| = 4n$.

En conclusión, cada elemento de K_{4n} se expresa de forma única como $a^i b^j$, con $0 \le i < n$, $0 \le j < 4$. Vamos a calcular el centro de K_{4n}. Para ello observamos que $a^{b^2} = a$, luego b^2 conmuta con a y, trivialmente, con b, luego $b^2 \in Z(K_{4n})$. Por otro lado, suponiendo $n > 2$, $a^b \neq a$, luego $b \notin Z(K_{4n})$.

Si $a^i b^j \in Z(K_{4n})$, entonces $a^i b^j = (a^i b^j)^b = a^{-i} b^j$, luego $a^{2i} = 0$, luego $n \mid 2i$. Si n es impar, esto equivale a que $n \mid i$, luego $i = 0$, luego $j = 0, 2$.

Por el contrario, si n es par tenemos que $n/2 \mid i$, luego $i = 0, n/2$, luego $a^{n/2} \in Z(K_{4n})$, luego $b^j \in Z(K_{4n})$, luego $j = 0, 2$. En total, si $n \ge 3$,

$$Z(K_{4n}) = \begin{cases} \{1, a^{n/2}, b^2, a^{n/2}b^2\} & \text{si } n \text{ es par,} \\ \{1, b^2\} & \text{si } n \text{ es impar.} \end{cases}$$

mientras que es claro que $K_8 = C_2 \times C_4$ es abeliano. ∎

Grupos dicíclicos Introducimos ahora una familia de grupos que incluye al grupo cuaternio Q_8:

Definición 3.21 Para cada número natural $n \ge 2$, el grupo *dicíclico* de orden $4n$ es el grupo

$$Q_{4n} = \left\langle a, b \mid a^{2n} = 1,\ b^2 = a^n,\ b^{-1}ab = a^{-1} \right\rangle.$$

Vamos a probar que, en efecto, Q_{4n} tiene orden $4n$.

De la última relación se sigue que $(a^{-r})^b = (a^b)^{-r} = a^r$, luego $ba^r = a^{-r}b$. Esto implica que todo elemento de Q_{4n} es de la forma $a^i b^j$, y las dos primeras relaciones nos permiten reducir los exponentes a $0 \le i < 2n$, $0 \le j < 2$. Por lo tanto $|Q_{4n}| \le 4n$.

Por otra parte, consideramos el grupo K_{8n}, que tiene orden $8n$ y hemos visto que $a^n b^2 \in Z(K_{8n})$, luego $N = \langle a^n b^2 \rangle \trianglelefteq K_{8n}$ y podemos formar el cociente $G = K_{8n}/N$, que es un grupo de orden $4n$ generado por $x = aN$, $y = bN$ y claramente

$$x^n = y^4 = 1, \quad x^n = y^2, \quad x^y = x^{-1},$$

luego G cumple las relaciones de Q_{4n}, lo que prueba que $|Q_{4n}| = 4n$, por lo que sus elementos se expresan de forma única como $a^i b^j$, con $0 \le i < 2n$, $0 \le j < 2$. Además $ba^r = a^{-r}b$, y esto determina completamente el producto, pues

$$a^i a^j = a^{i+j}, \quad a^i(a^j b) = a^{i+j}b, \quad (a^i b)a^j = a^{i-j}b, \quad (a^i b)(a^j b) = a^{n+i-j}.$$

Notemos que todos los elementos de la forma $a^i b$ tienen orden 4, ya que

$$(a^i b)^2 = a^i b a^i b = b^2 = a^n,$$

que tiene orden 2.

Ejercicio: Probar que $Z(Q_{4n}) = \{1, a^n\}$, $Q'_{4n} = \langle a^2 \rangle$.

Observemos que si $n \geq 3$ es impar, entonces $K_{4n} \cong Q_{4n}$, pues en $Q_{4n} = \langle a, b\rangle$ podemos llamar $x = a^2$, $y = b$ y entonces $o(x) = n$, $o(y) = 4$, $\langle x\rangle \cap \langle y\rangle = 1$, luego $|\langle x\rangle \langle y\rangle| = 4n$, luego $Q_{4n} = \langle x, y\rangle$ y estos generadores cumplen

$$x^n = y^4 = 1, \qquad x^y = x^{-1},$$

que son las relaciones de K_{4n}, luego ambos grupos son isomorfos.

Otro hecho obvio es que el grupo dicíclico Q_8 es el grupo cuaternio usual, por lo que a Q_{4n} también se le llama *grupo cuaternio generalizado* (si bien en algunos libros este nombre se restringe a los grupos Q_{2^n}).

En cambio, el grupo $Q_{12} = K_{12}$ es un grupo no abeliano de orden 12 no isomorfo a ninguno de los dos grupos no abelianos de este orden que conocemos, a saber, D_{12} y A_4, ya que éstos no tienen elementos de orden 4. ∎

Grupos de orden p^3 Casi estamos en condiciones de probar el teorema siguiente:

Teorema 3.22 *Si p es un primo impar, todo grupo de orden p^3 es isomorfo a C_{p^3}, $C_p \times C_{p^2}$, $C_p \times C_p \times C_p$, o a uno de los grupos siguientes:*

$$\left\langle a, b \mid a^{p^2} = b^p = 1,\ a^b = a^{p+1}\right\rangle,$$

$$\langle a, b, c \mid a^p = b^p = c^p = 1,\ ab = ba,\ ac = ca,\ b^c = ab\rangle\,.$$

El primero tiene elementos de orden p^2, mientras que en el segundo todos los elementos no triviales tienen orden p.

Demostración: Sea G un grupo no abeliano de orden p^3. Por 1.32 y 2.5, tiene que ser $|Z(G)| = p$. Más aún, por 2.6 y 1.32, se cumple que $G/Z(G) \cong C_p \times C_p$. Por consiguiente, $G' \leq Z(G)$ y, como $G' \neq 1$, tiene que ser $G' = Z(G)$.

Pongamos que $G/Z(G) = \langle xZ(G), yZ(G)\rangle$ y $Z(G) = \langle z\rangle$. Entonces, claramente $G = \langle x, y, z\rangle$, luego x e y no conmutan, o G sería abeliano, luego $[y, x] \neq 1$, luego $Z(G) = G' = \langle [y, x]\rangle$ y podemos tomar, concretamente, $z = [y, x]$, luego $G = \langle x, y\rangle$. Como $yx = xy[y, x] = xyz$, una simple inducción prueba que

$$(xy)^n = x^n y^n z^{n(n-1)/2}.$$

En particular, como $z^p = 1$, tenemos que $(xy)^{rp} = x^{rp} y^{rp}$.

Si $o(x) = o(y) = p^2$, como $x^p, y^p \in Z(G)$ (porque $[x], [y]$ tienen orden p en el cociente), existe un r tal que $y^p = (x^p)^r$, luego $y^p x^{-rp} = 1$ y, por la igualdad anterior, $(yx^{-r})^p = 1$.

Por lo tanto, si llamamos $y' = yx^{-r}$, tenemos igualmente que $G = \langle x, y'\rangle$, pero $o(y') = p$. Así pues, podemos suponer que al menos uno de los dos generadores x, y tiene orden p.

A partir de aquí suponemos que $o(y) = p$ y distinguimos dos casos, según si $o(x) = p^2$ o bien $o(x) = p$.

Si $o(x) = p^2$, entonces $G = \langle x, y\rangle$ y $N = \langle x\rangle \lhd G$, $H = \langle y\rangle$ cumplen que $H \cap N = 1$, luego $G \cong H[N]$, donde el producto semidirecto es el determinado por la acción de H sobre N por conjugación, que a su vez está determinada por el automorfismo $\alpha_y \in \operatorname{Aut} N$ determinado por la conjugación por y. Si es $\alpha_y = 1$ entonces G es abeliano, luego α_y tiene que tener orden p. Esto significa que $\alpha_y(x) = x^u$, donde $[u]$ tiene orden p en U_{p^2}.

Pero U_{p^2} es un grupo cíclico que tiene un único subgrupo de orden p. Si u, v son enteros con orden p módulo p^2, necesariamente $v = u^r$, por lo que, si $x^y = x^u$, entonces $x^{y^r} = x^v$, luego cambiando x por una potencia x^r adecuada, podemos exigir que $x^y = x^u$ para cualquier entero u prefijado de orden p módulo p^2 (notemos que no puede suceder que $x^r = 1$, pues entonces sería $x^{y^r} = x$, en lugar de $x^{y^r} = x^v$). Tal y como hemos visto en la página 107, al estudiar la existencia de grupos no abelianos de orden p^3, podemos tomar $u = p + 1$, y entonces G es claramente isomorfo al primer grupo presentado en el enunciado.

Supongamos ahora que $o(x) = o(y) = p$. Entonces $V = \langle x, z\rangle \lhd G$ es un grupo abeliano de tipo $C_p \times C_p$ y $H = \langle y\rangle$ cumple $V \cap H = 1$, luego de nuevo $G = H[V]$ y $\alpha_y \in \operatorname{Aut}(V)$ es un automorfismo de orden p.

Notemos que, como $z \in Z(G)$, tiene que ser $z^y = z$. Una posibilidad es que $x^y = xz$, pues en tal caso $x^{y^p} = xz^p = x$, luego α_y tiene orden p. En tal caso es claro que G es isomorfo al segundo grupo presentado en el enunciado. Lo único que no estamos en condiciones de probar ahora es que cualquier otra posibilidad se puede reducir a ésta. Véase la observación tras el teorema 3.32. ∎

El subgrupo derivado y el conjunto de los conmutadores Vamos a construir un grupo finito cuyo derivado no sea igual al conjunto de los conmutadores. En la sección 3.3 hemos probado que

$$Q_8 = \{a, b \mid a^4 = 1,\ a^2 = b^2,\ a^b = a^{-1}\},$$

y unos generadores que cumplen estas relaciones son tanto i, j como j, k, luego el teorema de Von Dyck nos da un automorfismo $\alpha_1 \in \operatorname{Aut}(Q_8)$ tal que

$$\alpha_1(i) = j, \quad \alpha_1(j) = k, \quad \alpha_1(k) = i$$

(la tercera igualdad es consecuencia de las dos primeras). Es obvio entonces que α_1 tiene orden 3, luego el producto semidirecto $G_1 = \langle\alpha_1\rangle\,[Q_8]$ tiene orden 24.

Similarmente, la presentación de $V_4 = \{1, a, b, c\}$ nos da un automorfismo $\alpha_2 \in \operatorname{Aut}(V_4)$ tal que

$$\alpha_2(a) = b, \qquad \alpha_2(b) = c, \qquad \alpha_2(c) = a,$$

luego $G_2 = \langle\alpha_2\rangle\,[V_4]$ es un grupo de orden 12.

Sea $N = Q_8 \times V_4 \trianglelefteq G_1 \times G_2$ y sea $\alpha = (\alpha_1, \alpha_1) \in G_1 \times G_2$. Llamamos $G = \langle\alpha\rangle\, N$, que es un grupo de orden 96. Una comprobación rutinaria nos da

los conmutadores siguientes:

$$\begin{array}{llllll} [\alpha,\pm i] & = k & [\alpha,\pm j] & = i & [\alpha,\pm k] & = j, \\ [\alpha^2,\pm i] & = -j & [\alpha^2,\pm j] & = -k & [\alpha^2,\pm k] & = -i \\ [\alpha,a] & = c & [\alpha,b] & = a & [\alpha,c] & = b \end{array}$$

Esto implica en particular que $N \leq G'$, y la inclusión opuesta se debe a que $G/N \cong C_3$ es abeliano, luego $G' = N$. Sin embargo, vamos a probar que $(-1,a) \in G'$ no es un conmutador.

Vamos a usar las fórmulas siguientes, que son válidas en cualquier grupo y se comprueban trivialmente:

$$[xy,z] = [x,z]^y[y,z], \qquad [x,yz] = [x,z][x,y]^z.$$

Todo elemento de G es de la forma $\alpha^e n$, con $n \in N$ y $e = 0,1,2$, luego todo conmutador es de la forma $[\alpha^s n_1, \alpha^t n_2]$. Vamos a probar que podemos exigir $t = 0$. Si $s = 0$ se comprueba inmediatamente que

$$[n_1, \alpha^t n_2] = [\alpha^t n_2 n_1, n_1^{-1}],$$

luego, en efecto, el conmutador admite una expresión alternativa con $t = 0$. Si $0 < t \leq s \leq 2$, entonces $s = ct$, luego, aplicando la primera de las dos fórmulas anteriores,

$$[\alpha^s n_1, \alpha^t n_2] = [(\alpha^t n_2)^{-c}(\alpha^s n_1), \alpha^t n_2] = [(n_2^{-c})^{\alpha^s} n_1, \alpha^t n_2] = [n_3, \alpha^t n_2]$$

y llegamos a una expresión con $s = 0$, que a su vez nos lleva a otra con $t = 0$. La última posibilidad es $0 < s < t \leq 2$, con lo que $s = 1$, $t = 2$. Entonces la segunda identidad con los conmutadores nos da

$$[\alpha n_1, \alpha^2 n_2] = [\alpha n_1, (\alpha n_1)^{-2}(\alpha^2 n_2)] = [\alpha n_1, n_1^{-2} n_2],$$

y de nuevo tenemos una expresión con $t = 0$.

Así pues, si $(-1,a)$ fuera un conmutador, sería de la forma

$$(-1,a) = [\alpha^e n_1, n_2].$$

Llamando $n_i = (q_i, d_i) \in Q_8 \times V_4$, es

$$(-1,a) = ([\alpha_1^e q_1, q_2], [\alpha_2^e d_1, d_2]),$$

luego

$$[\alpha_1^e q_1, q_2] = -1, \qquad [\alpha_2^e d_1, d_2] = a.$$

La primera igualdad equivale a

$$[\alpha_1^e, q_2]^{q_1}[q_1, q_2] = -1,$$

donde $[q_1, q_2] \in Q_8' = \{\pm 1\}$, luego tiene orden 2. Si suponemos que $e = 1,2$, hemos visto que $[\alpha_1^e, q_2]$ tiene orden 4 siempre que $q_2 = \pm i, \pm j, \pm k$, y esto es imposible, porque entonces -1 tendría orden 4, luego podemos concluir que $q_2 = \pm 1 \in Z(G_1)$, pero entonces los conmutadores con q_2 son triviales y llegamos a que $1 = -1$. Por consiguiente, tiene que ser $e = 0$, pero esto nos da que $1 = [d_1, d_2] = a$, y tenemos igualmente una contradicción. ∎

Acciones conjugadas Un mismo par de grupos puede definir productos semidirectos no isomorfos si consideramos acciones distintas de uno sobre otro. Sin embargo, a veces acciones distintas pueden dar lugar a productos semidirectos isomorfos. Veamos un caso:

Definición 3.23 Diremos que dos acciones $\alpha_1, \alpha_2 : H \longrightarrow \operatorname{Aut} N$ son *conjugadas* si existe $\phi \in \operatorname{Aut} N$ tal que, para todo $h \in H$, se cumpla que

$$\alpha_2(h) = (\alpha_1(h))^\phi.$$

En tal caso, la aplicación $\Phi : H[N]_{\alpha_1} \longrightarrow H[N]_{\alpha_2}$ dada por

$$\Phi(h, n) = (h, \phi(n))$$

es un isomorfismo de grupos, pues

$$\Phi((h,n)(h',n')) = \Phi(hh', n^{\alpha_1(h')}n') = (hh', \phi(n^{\alpha_1(h')})\phi(n')),$$

$$\Phi(h,n)\Phi(h',n') = (h,\phi(n))(h',\phi(n')) = (hh', \phi(n)^{\alpha_2(h')}\phi(n'))$$

$$= (hh', \phi(n)^{\phi^{-1}\alpha_1(h')\phi}\phi(n')) = (hh', \phi(n^{\alpha_1(h')})\phi(n')).$$

Por ejemplo, imaginemos que queremos construir un producto semidirecto $G = C_4[V_4]$. Para ello tenemos que especificar una acción $\alpha : C_4 \longrightarrow \operatorname{Aut} V_4$. Al final de la sección anterior hemos visto que $\operatorname{Aut} V_4 \cong \Sigma_3$, que no tiene elementos de orden 4. Las únicas acciones no triviales tienen imagen de orden 2, y hay tres posibilidades, pues en Σ_3 hay tres elementos de orden 2, pero todos ellos son conjugados, así que el teorema anterior nos asegura que los tres productos semidirectos no triviales $C_4[V_4]$ son isomorfos, por lo que podemos hablar de "el producto semidirecto no trivial $C_4[V_4]$" sin más especificaciones. Concretamente, es fácil ver que

$$C_4[V_4] = \langle a, b, c \mid a^2 = b^2 = c^4 = 1,\ ab = ba,\ a^c = b,\ b^c = a \rangle.$$

La clave está en que si $V_4 = \{1, x, y, z\}$, cualquiera que sea el automorfismo asociado a c, va a intercambiar dos elementos y dejar fijo al tercero, luego podemos llamar a y b a los elementos intercambiados, y así $C_4[V_4] = \langle a, b, c\rangle$ cumple las relaciones indicadas.

Similarmente, podemos definir $C_2[Q_8]_{\text{int}}$ como el producto semidirecto determinado por la acción $\alpha : C_2 \longrightarrow \operatorname{Aut} Q_8$ tal que si $C_2 = \langle g\rangle$, entonces $\alpha(g)$ es cualquiera de los automorfismos internos no triviales de Q_8, pues en la sección 4.3 de [G] hemos visto que $\operatorname{Aut} Q_8 \cong \Sigma_4$ y los automorfismos internos (un subgrupo normal isomorfo a $C_2 \times C_2$) se corresponde con el subgrupo de los pares de trasposiciones, cuyos elementos no triviales son conjugados. Si elegimos, concretamente, $\alpha(g) = \alpha_k$ (la conjugación por k), obtenemos fácilmente que $C_2[Q_8]_{\text{int}}$ es isomorfo a

$$G = \langle i, j, g \mid i^4 = 1 = g^2,\ i^2 = j^2, \quad i^j = i^{-1}, i^g = i^{-1},\ j^g = j^{-1}\rangle.$$

Tenemos que $gi = -ig$, $gj = -jg$, $gk = kg$, por lo que todo elemento de G se expresa de forma única como $i^u j^v g^w$, con $0 \leq u < 4$, $0 \leq v, w < 2$. Es fácil calcular los órdenes de sus elementos:

1	-1	i	$-i$	j	$-j$	k	$-k$
1	2	4	4	4	4	4	4
g	$-g$	ig	$-ig$	jg	$-jg$	kg	$-kg$
2	2	2	2	2	2	4	4

Por ejemplo, $(ig)^2 = igig = i(-i)g^2 = 1$, luego $o(ig) = 2$, pero en cambio $(kg)^2 = k^2 = -1$, luego $o(kg) = 4$. Notemos además que $Z(G) = \langle kg \rangle$ tiene orden 4, pues

$$(kg)^g = kg, \quad (kg)^i = -ikgi = j(-i)g = kg, \quad (kg)^j = -jkgj = -i(-j)g = kg.$$

Por lo tanto, $\langle kg \rangle \leq Z(G)$, pero el centro de un grupo no abeliano de orden 16 no puede tener más de 4 elementos por el teorema 1.32.

Por otro lado, $\operatorname{Aut} C_8 \cong U_8 = \{[1], [3], [5], [7]\} \cong C_2 \times C_2$ contiene tres elementos de orden 2 no conjugados entre sí, de modo que podemos formar tres productos semidirectos no triviales

$$C_2[C_8]_i = \langle a, b \mid a^8 = b^2 = 1,\, a^b = a^i \rangle,$$

para $i = 3, 5, 7$, y los tres son muy distintos entre sí. En efecto, los elementos de cualquiera de ellos se expresan de forma única como $a^u b^v$, con $0 \leq u < 8$, $0 \leq v < 2$, pero sus órdenes son muy distintos. En efecto, para $i = 7$ el grupo es D_{16}, y sabemos que sus elementos de la forma $a^u b$ tienen todos orden 2. En cambio, para $i = 3$ tenemos que

$$(a^u b)^2 = a^u b a^u b = a^u a^{3u} = a^{4u},$$

que tiene orden 2 si u es impar y tiene orden 1 si u es par, luego los órdenes de los elementos de esta forma son los que indica la tabla siguiente:

i	b	ab	a^2b	a^3b	a^4b	a^5b	a^6b	a^7b
3	2	4	2	4	2	4	2	4
5	2	8	4	8	2	8	4	8
7	2	2	2	2	2	2	2	2

Para $i = 5$ es $(a^u b)^2 = a^u b a^u b = a^{6u}$, que tiene orden $1, 4, 2, 4, 1, 4, 2, 4$ en función de i, luego el orden de $a^u b$ es el doble (el que indica la tabla anterior).

Por lo tanto, contando también los elementos de $\langle a \rangle$, concluimos que el número de elementos de cada orden en cada uno de los tres grupos viene dado por la tabla, en la que indicamos también el centro de cada grupo:

i	2	4	8	$Z(G)$
3	5	6	4	$\langle a^4 \rangle$
5	3	4	8	$\langle a^2 \rangle$
7	9	2	4	$\langle a^4 \rangle$

En efecto, para que un elemento $a^u b^v$ esté en el centro, debe cumplir que

$$a^u b^v = (a^u b^v)^b = a^{iu} b^v,$$

lo cual equivale a que $a^{(i-1)u} = 1$, es decir, a que $8 \mid (i-1)u$.

Si $i = 3$, esto equivale a que $4 \mid u$, luego sólo a^4 y $a^4 b$ pueden estar en el centro. Ciertamente a^4 lo está (pues hemos visto que conmuta con b y trivialmente conmuta con a), pero $a^4 b$ no puede estar en el centro, pues entonces lo estaría b, y no es el caso.

Si $i = 5$ tenemos que la condición necesaria es que $2 \mid u$, y es claro entonces que a^2 está en el centro, pero $a^{2u} b$ no puede estar, ya que entonces lo estaría b.

El caso de $i = 7$ es similar, pero ya conocemos el centro de D_{16}.

Todos estos hechos muestran que los tres grupos no son isomorfos entre sí. ∎

3.5 Clasificación de los grupos de orden 16

Como aplicación de los resultados vistos hasta este punto, vamos a clasificar todos los grupos de orden 16. Concretamente, vamos a demostrar que existen exactamente 14 tipos distintos de grupos de este orden, tal y como detalla el teorema siguiente:

Teorema 3.24 *Todo grupo de orden* 16 *es isomorfo a uno de los* 5 *grupos abelianos*

$$C_{16}, \quad C_2 \times C_8, \quad C_4 \times C_4, \quad C_2 \times C_2 \times C_4, \quad C_2 \times C_2 \times C_2 \times C_2$$

o bien a uno de los 9 *grupos no abelianos siguientes:*

6	Q_{16}	$= \langle a, b \mid a^8 = 1,\ a^4 = b^2,\ a^b = a^{-1} \rangle$
7	D_{16}	$= \langle a, b \mid a^8 = b^2 = 1,\ a^b = a^{-1} \rangle$
8	$C_2[C_8]_3$	$= \langle a, b \mid a^8 = b^2 = 1,\ a^b = a^3 \rangle$
9	$C_2[C_8]_5$	$= \langle a, b \mid a^8 = b^2 = 1,\ a^b = a^5 \rangle$
10	K_{16}	$= \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1} \rangle$
11	$C_4[V_4]$	$= \langle a, b, c \mid a^2 = b^2 = c^4 = 1,\ ab = ba,\ a^c = b,\ a^c = a \rangle$
12	$C_2[Q_8]_{\text{int}}$	$= \langle a, b, c \mid a^4 = 1 = c^2,\ a^2 = b^2,\ a^b = a^{-1},\ a^c = a^{-1},\ b^c = b^{-1} \rangle$
13	$C_2 \times Q_8$	
14	$C_2 \times D_8$	

Además, dos cualesquiera de estos 14 *grupos no son isomorfos entre sí.*

Sabemos que los cinco grupos abelianos no son isomorfos entre sí (tienen factores invariantes distintos) ni tampoco son isomorfos a ninguno de los no abelianos, luego, de la última parte del teorema sólo hay que probar que los nueve grupos no abelianos no son isomorfos entre sí. La tabla siguiente indica

el número de elementos de cada orden en cada subgrupo, así como la estructura de su centro:

		2	4	8	$Z(G)$
6	Q_{16}	1	10	4	C_2
7	D_{16}	9	2	4	C_2
8	$C_2[C_8]_3$	5	6	4	C_2
9	$C_2[C_8]_5$	3	4	8	C_4
10	K_{16}	3	12	0	$C_2 \times C_2$
11	$C_4[V_4]$	7	8	0	$C_2 \times C_2$
12	$C_2[Q_8]_{\text{int}}$	7	8	0	C_4
13	$C_2 \times Q_8$	3	12	0	$C_2 \times C_2$
14	$C_2 \times D_8$	11	4	0	$C_2 \times C_2$

Vemos que los órdenes distinguen todos los grupos entre sí excepto los pares K_{16}, $C_2 \times Q_8$ por un lado y $C_4[V_4]$, $C_2[Q_8]_{\text{int}}$ por otro. El segundo par se distingue por la estructura de su centro, mientras que la diferencia entre los dos primeros es más sutil. A su vez, la tabla siguiente muestra los elementos de K_{16} con sus órdenes correspondientes:

1	a	a^2	a^3
1	4	2	4
b	ab	a^2b	a^3b
4	4	4	4
b^2	ab^2	a^2b^2	a^3b^2
2	4	2	4
b^3	ab^3	a^2b^3	a^3b^3
4	4	4	4

Por ejemplo, $(a^ib)^2 = a^iba^ib = a^{i-i}b^2 = b^2$, luego $o(a^ib) = 4$. Teniendo en cuenta que $b^2 \in Z(K_{16})$, es fácil ver que $o(a^ib^3) = 4$ y que $(a^ib^2)^2 = a^{2i}$, de donde se siguen inmediatamente los órdenes de la tercera fila. Por otro lado, sabemos que $Z(K_{16})$ está formado por el neutro y los tres elementos de orden 2, y ahora sólo necesitamos una última observación, y es que dos de ellos (a^2 y b^2) son cuadrados en K_{16} (el tercero no lo es, pero eso es secundario, lo que importa es que al menos dos elementos no triviales del centro son cuadrados).

Esto no sucede en $C_2 \times Q_8$. Si $C_2 = \langle \pm 1 \rangle$, entonces

$$Z(C_2 \times Q_8) = Z(C_2) \times Z(Q_8) = \{(1,1), (-1,1), (1,-1), (-1,-1)\},$$

y sólo $(1,-1) = (1,i)^2$ es un cuadrado. Los otros no son cuadrados porque -1 no es un cuadrado en C_2.

Así pues, la diferencia que prueba que K_{16} no es isomorfo a $C_2 \times Q_8$ es que en el primer grupo el centro contiene 3 cuadrados (contando el neutro), mientras que en el segundo el centro sólo contiene dos.

El punto de partida de la clasificación es el teorema siguiente:

Teorema 3.25 *Si G es un grupo de orden 16 no isomorfo a $C_2 \times C_2 \times C_2 \times C_2$, entonces tiene un subgrupo normal isomorfo a C_8 o bien a $A = C_2 \times C_4$.*

DEMOSTRACIÓN: No puede ocurrir que todos los elementos de G sean de orden 2, pues entonces G sería abeliano (teorema 1.7) y claramente tendría que ser de tipo $C_2 \times C_2 \times C_2 \times C_2$. Si tiene elementos de orden 8 o 16, entonces tiene un subgrupo isomorfo a C_8 (que será normal por tener índice 2), así que vamos a suponer que G no tiene elementos de orden 8 o 16 y probaremos que tiene un subgrupo (necesariamente normal) isomorfo a A.

Por el teorema 2.5 sabemos que $Z(G) \neq 1$, luego tiene que haber un $z \in Z(G)$ de orden 2. Llamemos $H = \langle z \rangle \lhd G$ (notemos que todo subgrupo del centro de un grupo es obviamente normal).

Como los elementos de G no pueden ser todos de orden 2, tiene que haber al menos un $g \in G$ de orden 4. Si alguno cumple $g^2 \neq z$, entonces $\langle g \rangle \cap H = 1$, luego $A = H\langle g \rangle$ es un grupo abeliano isomorfo a $C_2 \times C_4$.

Suponemos, pues, que todos los elementos de orden 4 en G cumplen $g^2 = z$. Esto implica que todos los elementos de G/H tienen orden 2, luego G/H es un grupo abeliano.

Si $x \in G$ tiene orden 4 y $g \in G$, entonces $x^g H = xH$ (porque el cociente es abeliano), luego $x^g \in xH$, que es un conjunto de 2 elementos, luego $|\mathrm{cl}(x)| \leq 2$, pero el cardinal de la clase de conjugación es $|G : C_G(x)|$, luego $|C_G(x)| \geq 8$, luego existe un $y \in C_G(x) \setminus \langle x \rangle$.

Si $o(y) = 2$, entonces $A = \langle y \rangle \langle x \rangle$ es un subgrupo (porque $\langle x \rangle \lhd C_G(x)$), es abeliano y claramente $A \cong C_2 \times C_4$.

Supongamos ahora que $o(y) = 4$, con lo que $y^2 = z$ (así lo estamos suponiendo), luego $(xy)^2 = x^2y^2 = z^2 = 1$ (donde hemos usado que x e y conmutan). No puede ser $xy = 1$, pues entonces $y = x^{-1} \in \langle x \rangle$. Por lo tanto, $o(xy) = 2$ y $xy \notin \langle x \rangle$, pues en tal caso tendría que ser $xy = x^2$, luego $y = x$. Así pues, $xy \in C_G(x) \setminus \langle x \rangle$ es un elemento de orden 2 y estamos en el caso anterior. ∎

Fijemos ahora un grupo G de orden 16. Vamos a ir distinguiendo casos, de modo que, en cada caso supondremos que no se cumplen los anteriores. Por ejemplo, a partir del caso 2 supondremos que G tiene elementos de orden mayor que 2, a partir del caso 3 supondremos que G no tiene elementos de orden 16, etc.

1. G tiene todos los elementos de orden 2.

   En tal caso G es abeliano y claramente es isomorfo a $C_2 \times C_2 \times C_2 \times C_2$.

2. G tiene un elemento de orden 16.

   En tal caso $G \cong C_{16}$.

3. G tiene un elemento de orden 8.

   Fijemos $N = \langle n \rangle \cong C_8$ y distingamos varios subcasos:

(a) Existe $g \in G \setminus N$ con $o(g) = 2$.

Entonces $H = \langle g \rangle$ cumple que $N \cap H = 1$, luego $G = H[N]$, donde el producto semidirecto se construye respecto de la acción de H sobre N por conjugación, es decir, por el automorfismo $\alpha_g : N \longrightarrow N$, que es independiente de n. De acuerdo con el teorema 1.17, las posibilidades son $\alpha_g = \alpha_1, \alpha_3, \alpha_5, \alpha_7$, donde $\alpha_u(n) = n^u$. En el primer caso G es abeliano, y es, concretamente, isomorfo a $C_2 \times C_8$. En los otros tres casos G es isomorfo a uno de los grupos $C_2[C_8]_i$ (para $i = 3, 5, 7$), de modo que $C_2[C_8]_7 \cong D_{16}$ y ya hemos comprobado que cumplen las características incluidas en la tabla anterior.

(b) Existe $g \in G \setminus N$ con $o(g) = 4$.

Entonces $G = \langle g \rangle N$, luego $|\langle g \rangle \cap N| = 2$, luego tiene que ser $g^2 = n^4$.

Consideramos igualmente el automorfismo $\alpha_g : N \longrightarrow N$. Si fuera α_1, entonces $(n^2g)^2 = n^4g^2 = n^8 = 1$, y $n^2g \neq 1$, pues esto implicaría que $g \in N$, luego habría elementos de orden 2 fuera de N, en contra de lo supuesto.

Si fuera $n^g = n^3$, es decir, $ng = gn^3$, entonces

$$(ng)^2 = ngng = gn^4g = g^4 = 1$$

y $ng \neq 1$ (pues $g \notin N$), luego ng sería un elemento de orden 2 en $G \setminus N$, en contra de lo supuesto. Similarmente, si fuera $n^g = n^5$, entonces

$$(n^2g)^2 = n^2gn^2g = ngn^7g = gn^{12}g = gn^4g = g^4 = 1,$$

y concluimos igualmente. Así pues, tiene que ser $n^g = n^{-1}$. Así:

$$G = \langle n, g \rangle\,, \quad n^8 = 1, \quad n^4 = g^2, \quad n^g = n^{-1},$$

luego G satisface las relaciones de Q_{16}, luego $G \cong Q_{16}$, y sabemos que cumple las características indicadas en la tabla.

(c) Existe $g \in G \setminus N$ con $o(g) = 8$.

Entonces $G = \langle g \rangle N$, luego $|\langle g \rangle \cap N| = 4$, luego tiene que ser $g^2 = n^2$ o bien $g^2 = n^6$, pero en el segundo caso podemos cambiar g por g^{-1} y se cumple $g^2 = n^2$.

Si $n^g = n$, entonces $(n^3g)^2 = n^6g^2 = n^8 = 1$, lo cual es imposible.

Si $n^g = n^5$, entonces $(ng)^2 = ngng = gn^6g = g^8 = 1$, imposible.

Si $n^g = n^3$, entonces $n^2 = g^2 = (g^2)^g = (n^2)^g = n^6$, imposible.

Si $n^g = n^7$, entonces $n^2 = g^2 = (g^2)^g = (n^2)^g = n^6$, imposible.

En suma, este caso no puede darse.

4. G tiene un subgrupo $A = \langle x, y \rangle \cong C_2 \times C_4$.

Notemos que, por el teorema 3.25, este caso tiene que darse si no se da el anterior, luego ya no hay más casos posibles.

Recordemos que $\operatorname{Aut} A = \langle \sigma, \tau \rangle \cong D_8$ y que en la tabla de la página 85 está descrita la acción de cada automorfismo sobre los generadores x, y de A. Vamos a distinguir varios subcasos, como en el caso anterior.

(a) Existe $g \in G \setminus A$ con $o(g) = 2$.

Entonces $H = \langle g \rangle$ cumple que $H \cap A = 1$, luego $G = H[A]$, donde el producto semidirecto se construye respecto de la acción de H sobre A por conjugación, determinada por la conjugación $\alpha_g : A \longrightarrow A$, que será la identidad o uno de los 5 automorfismos de A de orden 2.

Si $\alpha_g = 1$, es decir, si $x^g = x$, $y^g = y$, entonces el producto es directo y $G \cong C_2 \times C_2 \times C_4$.

Si $\alpha_g = \sigma^2$, es decir, $x^g = x$, $y^g = y^{-1}$, entonces $C = \langle x \rangle \lhd G$, $N = \langle y \rangle \lhd G$ y $D = HN = \langle n, g \rangle$ es claramente isomorfo a D_8. Además $C \cap D = 1$, luego $G = C \times D \cong C_2 \times D_8$.

Puesto que conocemos los órdenes de los elementos de D_8, es fácil comprobar que el número de elementos de cada orden en G es el que indica la tabla anterior. En general, es fácil ver que el centro de un producto directo es el producto de los centros, por lo que en este caso $Z(G) \cong C_2 \times C_2$.

Si $\alpha_g = \tau$, es decir, $x^g = xy^2$, $y^g = y$, una comprobación rutinaria muestra que $Q_8 = \langle gy, gx \rangle$ es un subgrupo de G isomorfo al grupo cuaternio. Sus elementos son:

$$\begin{array}{cccccccc} 1 & -1 & i & -i & j & -j & k & -k \\ \hline 1 & y^2 & gy & gy^3 & gx & gxy^2 & xy & xy^3 \end{array}$$

Como tiene índice 2, es normal, y $G = \langle x \rangle\,[Q_8]$, donde la conjugación por x viene determinada por que

$$i^x = xgyx = gy^3 = -i, \qquad j^x = xgxx = gxy^2 = -j,$$

luego $k^x = k$. Así, la conjugación por x coincide con la conjugación por k, y tenemos que $G \cong C_2[Q_8]_{\text{int}}$. Ya hemos comprobado que cumple las características indicadas en la tabla.

Si $\alpha_g = \sigma^2\tau$, la estructura de G es la misma, pues los automorfismos τ y $\sigma^2\tau$ son conjugados en D_4. Igualmente los casos $\alpha_g = \sigma\tau$ y $\alpha_g = \sigma^3\tau$ dan lugar a la misma estructura de grupo, por lo que basta estudiar el segundo. Ahora $x^g = x$, $y^g = xy$, con lo que $\langle x \rangle \lhd G$, luego $V_4 = \langle x, g \rangle \leq G$ es un subgrupo de tipo $C_2 \times C_2$. De hecho es normal, porque

$$g^y = y^3gy = gy^3x^3y = gx \in V_4.$$

Por lo tanto $G = \langle g \rangle\,[V_4] \cong C_4[V_4]$. Dejamos al lector el cálculo del número de elementos de cada orden en este grupo, así como que su centro es $Z(G) = \{1, a, b, c^2, abc^2\}$.

(b) Existe $g \in G \setminus A$ con $o(g) = 4$.
Entonces $|\langle g\rangle \cap A| = 2$, luego $g^2 = y^2, x, xy^2$.

i. $g^2 = y^2$.
Entonces $\alpha_g^2 = 1$, luego α_g tiene que ser la identidad o uno de los 5 automorfismos de orden 2.

Si α_g es la identidad, entonces $(xg)^2 = 1$, contradicción.

Si $\alpha_g = \tau$, entonces $x^g = xy^2$, $y^g = y$, luego

$$(xg)^2 = xgxg = xg^2xy^2 = 1,$$

contradicción. Lo mismo sucede si $\alpha_g = \sigma^2\tau$.

Si $\alpha_g = \sigma^2$, entonces $x^g = x$, $y^g = y^{-1}$, luego $C = \langle x\rangle \lhd G$, $N = \langle y\rangle \lhd G$, y es claro que $Q_8 = \langle g\rangle\, N = \langle y, g\rangle$ es un subgrupo isomorfo a Q_8. Además $C \cap Q_8 = 1$, luego $G = C_2 \times Q_8$.

Si $\alpha_g = \sigma^3\tau$, entonces $x^g = x$, $y^g = xy$. En este caso llamamos

$$N = \langle gy\rangle = \{1, gy, x, gxy\},$$

y observamos que es un subgrupo normal, pues

$$(gy)^g = gxy = (gy)^{-1}, \quad (gy)^x = gy, \quad (gy)^y = gxy,$$

y por otra parte, $\langle g\rangle = \{1, g, y^2, gy^2\}$ cumple $\langle g\rangle \cap N = 1$, por lo que $G = \langle g\rangle\,[N] \cong C_4[C_4]$.

Si $\alpha_g = \sigma\tau$ la situación es la misma. Ahora $x^g = x$, $y^g = xy^3$, pero si llamamos $y' = y^{-1}$, tenemos que $A = \langle x, y'\rangle$ y ahora $x^g = x$, $y'^g = xy = xy'^3$, por lo que estamos en el caso anterior.

ii. $g^2 = x$.
Entonces α_g tiene que tener orden 1 o 2 y $\alpha_g(x) = x$, luego tiene que ser $\alpha_g = 1, \sigma^2, \sigma\tau, \sigma^3\tau$. Descartamos $\alpha_g = \sigma\tau$, pues entonces $y^g = xy^3$ y llegamos a que $o(yg) = 2$.

Si $\alpha_g = \sigma^3\tau$, entonces $y^g = xy$, de donde

$$(yg)^2 = ygyg = yg^2xy = y^2,$$

por lo que llamando $g' = yg$ estamos en el caso i.

Si $\alpha_g = \sigma^2$, entonces $y^g = y^3$, luego $(y^2)^g = y^2$, es decir, que g conmuta con y^2, por lo que $\langle y^2\rangle \lhd G$ y $N = \langle y^2, g\rangle \cong C_2 \times C_4$ es un subgrupo normal de G. Si llamamos $x' = y^2$, $y' = g$ y $g' = yg \notin N$, tenemos que $g'^2 = x = y'^2$ y estamos en el caso i.

Por último, si $\alpha_g = 1$, entonces G es abeliano y, como tiene 12 elementos de orden 4, tiene que ser $G \cong C_4 \times C_4$.

iii. $g^2 = xy^2$.
En este caso, llamando $x' = xy^2$, $y' = y$, tenemos igualmente que $A = \langle x', y'\rangle$, pero ahora $g^2 = x'$, luego estamos en el caso ii.

Esto completa todas las posibilidades. ∎

3.6 La teoría de Sylow

Presentamos ahora unos resultados fundamentales sobre existencia de subgrupos en grupos finitos. Hemos visto que el grupo alternado A_4 tiene orden 12, pero no tiene subgrupos de orden 6. Sin embargo, ahora vamos a probar que todo grupo finito tiene subgrupos de cualquier orden potencia de primo que divida a su orden, es decir, el resultado que anunciábamos en la introducción a este capítulo y que termina la demostración del teorema [Al 5.50]. Para ello conviene dar esta definición:

Definición 3.26 Sea G un grupo finito y p un número primo. Sea $|G| = p^n \cdot m$, con $(p, m) = 1$ (quizá con $n = 0$). Un subgrupo H de G de orden p^n se llama *p-subgrupo de Sylow* de G.

Teorema 3.27 (Primer teorema de Sylow) *Si G es un grupo finito y p un número primo, entonces G tiene un p-subgrupo de Sylow.*

Demostración: Por inducción sobre el orden de G. Si G tiene orden 1 es obvio. Supongamos que todos los grupos de orden menor que $|G|$ tienen p-subgrupos de Sylow y demostremos que G también los tiene.

Si $p \nmid |G|$, entonces el subgrupo trivial es un p-subgrupo de Sylow de G. Supongamos, pues, que $p \mid |G|$. Sea $|G| = p^n \cdot m$, con $(p, m) = 1$.

Distinguimos dos casos:

Caso 1 Existe un subgrupo $H < G$ tal que $p \nmid |G : H|$.

Entonces $p^n \mid |H|$ y por hipótesis de inducción H tiene un p-subgrupo de Sylow P de orden p^n, y así, P es también un p-subgrupo de Sylow de G.

Caso 2 Para todo subgrupo $H < G$, se cumple que $p \mid |G : H|$.

Entonces la ecuación de clases nos da que $p \mid |Z(G)|$. Como se trata de un grupo abeliano, tiene un elemento de orden p o, lo que es lo mismo, tiene un subgrupo $H \leq Z(G)$ de orden p. Como los elementos de H conmutan con todos los elementos de G, es evidente que $H^g = H$ para todo $g \in G$, o sea, $H \trianglelefteq G$.

Se cumple que $|G/H| = p^{n-1} \cdot m$ y tiene un subgrupo de Sylow P/H que cumplirá $|P/H| = p^{n-1}$, luego $|P| = p^n$, luego P es un subgrupo de Sylow. ∎

Como todo p-grupo tiene subgrupos de todos los órdenes posibles, es claro que, tal y como habíamos anunciado, todo grupo finito tiene subgrupos de todos los órdenes potencia de primo que dividan a su orden.

Veamos algunas aplicaciones sencillas. En la sección 3.4 hemos visto que si p y q son primos tales que $p \mid q - 1$, existen grupos no abelianos de orden pq. Ahora probamos que la condición es necesaria:

Teorema 3.28 *Si $p < q$ son primos y $p \nmid q-1$, entonces todo grupo de orden pq es cíclico.*

DEMOSTRACIÓN: Sea G un grupo de orden pq y sea $N \trianglelefteq G$ un q-subgrupo de Sylow, que es normal por 2.27. Sea H un p-subgrupo de Sylow. Entonces $N \cap H = 1$, luego $|NH| = pq$, luego $G = NH$. Consideramos el homomorfismo $f : H \longrightarrow \mathrm{Aut}(N)$ que a cada $h \in H$ le asigna la conjugación por h. Por 1.17 tenemos que $|\mathrm{Aut}(N)| = q-1$, luego $\mathrm{N}(f) \neq 1$, luego $\mathrm{N}(f) = H$, y esto significa que si $n \in N$ y $h \in H$ entonces $n^h = n$, es decir, que N y H conmutan elemento a elemento, luego G es abeliano, luego es cíclico. ∎

Por ejemplo, todo grupo de orden 15 es cíclico.

Teorema 3.29 *Todo grupo de orden* 30 *es isomorfo a uno de los grupos siguientes:*

$$C_{30}, \qquad D_{30}, \qquad C_3 \times D_{10}, \qquad C_5 \times D_6.$$

DEMOSTRACIÓN: Si G es un grupo de orden 30, por el teorema 2.28 sabemos que G tiene un subgrupo N de orden 15 (normal, por tener índice 2) y acabamos de probar que tiene que ser cíclico. Por el mismo teorema (o por el teorema de Sylow), también tiene un subgrupo H de orden 2. Claramente entonces $G \cong H[N]$, donde el producto semidirecto es el asociado a la acción de H sobre N por conjugación. Según 1.17, tenemos que $\mathrm{Aut}(N) \cong U_{15} \cong C_2 \times C_4$, y este grupo tiene tres elementos de orden 2, luego hay cuatro homomorfismos $\alpha : H \longrightarrow \mathrm{Aut}(N)$ (contando el trivial), luego a lo sumo hay cuatro grupos no isomorfos de orden 30. Ahora basta observar que los cuatro grupos del enunciado no son isomorfos entre sí, con lo que podemos asegurar que cualquier otro será isomorfo a uno de ellos. Para ello notamos que cada uno tiene un número distinto de elementos de orden 2, el primero 1, el segundo 15, el tercero 5 y el cuarto 3. ∎

La hipótesis de no divisibilidad del teorema 3.28 es necesaria:

Teorema 3.30 *Si p y q son primos tales que $p \mid q-1$, todo grupo de orden pq es isomorfo a C_{pq} o bien a*

$$\left\langle a, b \mid a^q = b^p = 1,\, a^b = a^u \right\rangle,$$

donde u es una unidad módulo q de orden p. (El grupo no depende de la elección de u.)

DEMOSTRACIÓN: Sea G un grupo de orden pq. Sean $P = \langle b \rangle$ y $Q = \langle a \rangle$ subgrupos de Sylow de G de órdenes p y q, respectivamente. Como Q tiene índice p, el teorema 2.27 nos da que $Q \lhd G$. Por consiguiente, $a^b = a^u$, para cierto u, que tiene que ser $u = 1$ o bien una unidad módulo p de orden q. Si $u = 1$ entonces $G = Q \times P$ es cíclico. En caso contrario es claro que G tiene la presentación indicada, y no depende de u, porque si v es otra unidad de orden p, tenemos que, en U_q, se cumple $\langle [u] \rangle = \langle [v] \rangle$, luego existe un r tal que $v = u^r$, y entonces $a^{b^r} = a^{u^r} = a^v$, luego $b' = b^r \neq 1$ y $\langle b' \rangle = \langle b \rangle$, luego $G = \langle a, b' \rangle$ y satisface la presentación con v en lugar de u. ∎

Por ejemplo, existe un único grupo no abeliano de orden 21, y es fácil ver que es el menor grupo no abeliano de orden impar.

Volviendo a la teoría de Sylow, el teorema siguiente nos da la relación entre los subgrupos de Sylow de un subgrupo normal o de un cociente:

Teorema 3.31 *Si G es un grupo finito, $N \trianglelefteq G$ y P es un p-subgrupo de Sylow de G, entonces $P \cap N$ es un p-subgrupo de Sylow[3] de N y PN/N es un p-subgrupo de Sylow de G/N.*

DEMOSTRACIÓN: Si $|G| = p^n m$, $|N| = p^r m'$, entonces

$$|G/N : PN/N| = |G : PN| = \frac{|G||P \cap N|}{|P||N|} = \frac{m|P \cap N|}{p^r m'}.$$

Para que el cociente sea entero es necesario que $p^r \mid |P \cap N|$, lo que prueba que p^r es un p-subgrupo de Sylow de N, así como que p no divide al índice de PN/N, que es obviamente un p-grupo, luego es un p-subgrupo de Sylow de G/N. ∎

He aquí un refinamiento del teorema de Sylow:

Teorema 3.32 (Segundo teorema de Sylow) *Si G es un grupo finito, todo p-subgrupo de G está contenido en un p-subgrupo de Sylow y dos p-subgrupos de Sylow cualesquiera son conjugados.*

DEMOSTRACIÓN: Sea P un p-subgrupo de Sylow de G y sea Q un p-subgrupo arbitrario. Entonces Q actúa sobre $\Omega = (G/P)_d$ por multiplicación a derecha. El teorema 2.2 nos da que las órbitas de los elementos de Ω tienen cardinal potencia de p, sin excluir la posibilidad de que alguna tenga cardinal $p^0 = 1$. De hecho, concluimos que alguna órbita ha de tener cardinal igual a 1, pues, de lo contrario, el cardinal de Ω, que es $|G : P|$, sería suma de potencias (no triviales) de p, luego sería múltiplo de p.

Así pues, existe un $g \in G$ tal que la clase $x = Pg$ forma una órbita trivial, con x como único elemento. Más explícitamente, $Pgq = Pg$ para todo $q \in Q$. En particular $gq \in Pg$, luego $q \in P^g$, para todo $q \in Q$. Concluimos que $Q \leq P^g$ y P^g es también un subgrupo de Sylow de G.

Si Q es también un p-subgrupo de Sylow de G, entonces ha de darse la igualdad $Q = P^g$, pues tenemos una inclusión y ambos grupos tienen el mismo orden. ∎

Nota Con esto ya podemos completar la prueba del teorema 3.22: teníamos un grupo $G = H[V]$, donde $V \cong C_p \times C_p$, y $H = \langle y \rangle \cong C_p$, para cierta acción no trivial $\alpha : \langle y \rangle \longrightarrow \operatorname{Aut} V$, de modo que α_y tiene que tener orden p.

Si $k = \mathbb{Z}/p\mathbb{Z}$ es el cuerpo de p elementos, un grupo de tipo $C_p \times C_p$ es isomorfo al grupo aditivo del k-espacio vectorial $V = k^2$, y es claro que sus automorfismos como grupo coinciden con sus automorfismos como k-espacio vectorial. Fijada una base v_1, v_2 de V, cada automorfismo α está determinado

[3]Si N no es normal esto no es necesariamente cierto. Por ejemplo, $\Sigma_3 \leq \Sigma_4$ contiene uno solo del los 3-subgrupos de Sylow de Σ_4, luego $P \cap \Sigma_3 = 1$ no es un 3-subgrupo de Sylow de Σ_3 salvo para un 3-subgrupo de Sylow P en concreto de Σ_4.

por el par $(\alpha(v_1), \alpha(v_2))$, que tiene que ser también una base de V. Podemos tomar como $\alpha(v_1)$ cualquier elemento no nulo de V, lo que nos da p^2-1 posibilidades, mientras que α_2 hay que elegirlo en $V \setminus \langle \alpha(v_1)\rangle$, para lo cual tenemos p^2-p posibilidades. Esto implica que

$$|\operatorname{Aut} V| = (p^2-1)(p^2-p) = (p-1)^2 p(p+1),$$

luego los p-subgrupos de Sylow de $\operatorname{Aut} V$ tienen orden p. Así pues, la imagen de la acción α será un p-subgrupo de Sylow de $\operatorname{Aut} V$, y hemos probado que dos cualesquiera de ellos son conjugados, por lo que la observación tras la definición 3.23 prueba que la estructura de G no cambia si suponemos que $\operatorname{Im}\alpha$ es un p-subgrupo de Sylow en concreto de $\operatorname{Aut} V$ y, teniendo en cuenta que $\alpha_{y^r} = (\alpha_y)^r$, cambiando y por un y^r adecuado, no perdemos generalidad si suponemos que α_y es un elemento de orden p prefijado de $\operatorname{Aut} V$, que es justo lo que nos faltaba para completar la prueba del teorema 3.22. ∎

Los p-subgrupos de Sylow forman una órbita en la acción de G por conjugación en el conjunto de todos sus subgrupos, luego si P es un p-subgrupo de Sylow, el número total de ellos es $|G : N_G(P)|$, que es un divisor del orden de G (e incluso de $|G : P|$). Esto forma parte del tercer teorema de Sylow:

Teorema 3.33 (Tercer teorema de Sylow) *El número ν_p de p-subgrupos de Sylow de un grupo finito cumple $\nu_p = |G : N_G(P)|$, $\nu_p \equiv 1$ (mód p).*

Demostración: Sea G un grupo finito, sea Ω el conjunto de sus p-subgrupos de Sylow, sea $P \in \Omega$ y consideremos la acción de P en Ω por conjugación. Ya hemos probado que $\nu_p = |G : N_G(P)|$. Obviamente, $P^g = P$ para todo $g \in P$, luego la órbita de P es trivial. Veamos que es la única. Si $Q \in \Omega$, cumple que $Q^g = Q$ para todo $g \in P$, entonces $P \leq N_G(Q)$, pero entonces P y Q son p-subgrupos de Sylow de $N_G(Q)$, luego son conjugados en $N_G(Q)$, es decir, existe $g \in N_G(Q)$ tal que $P = Q^g = Q$.

Las órbitas que P forma en Ω tienen cardinal potencia de P, y hemos visto que la única que tiene cardinal 1 es la de P, luego $\nu_p = |\Omega| \equiv 1$ (mód p). ∎

En particular G tiene un único p-subgrupo de Sylow si y sólo si tiene un p-subgrupo de Sylow normal (que, de hecho, será característico en G).

Los normalizadores de los subgrupos de Sylow tienen propiedades que conviene tener en cuenta:

Teorema 3.34 *Si G es un grupo finito y P es un p-subgrupo de Sylow, entonces $N_G(N_G(P)) = N_G(P)$. En particular, si $N_G(P) \trianglelefteq G$, es que $P \trianglelefteq G$.*

Demostración: Si $g \in N_G(N_G(P))$, entonces $p^g \leq N_G(P)^g = N_G(P)$, luego P y P^g son p-subgrupos de Sylow de $N_G(P)$, pero $P \trianglelefteq N_G(P)$, luego P es el único es un $p-$subgrupo de Sylow de $N_G(P)$, luego $P^g = P$, lo que prueba que $g \in N_G(P)$. ∎

Teorema 3.35 *Si G es un grupo finito y P, Q son dos p-subgrupos de Sylow, entonces $P \cap N_G(Q) = P \cap Q$.*

DEMOSTRACIÓN: Si llamamos $H = P \cap N_G(Q)$, se cumple que $QH = HQ$, pues $qh = hq^h \in HQ$ y $hq = q^{h^{-1}}h \in HQ$, luego $QH \leq G$ por 1.34 y

$$|QH| = \frac{|Q||H|}{|Q \cap H|}$$

se traduce en que

$$p^n = \frac{p^n|H|}{|Q \cap H|},$$

luego $H = Q \cap H = P \cap Q \cap N_G(Q) = P \cap Q$. ∎

Esto significa que los únicos elementos de P que normalizan a Q son los que están en Q. En otros términos, si consideramos la acción de P sobre los p-subgrupos de Sylow de G, el estabilizador de Q es $P \cap N_G(Q) = P \cap Q$, por lo que el cardinal de la órbita de Q es $|P : P \cap Q|$. De aquí obtenemos un refinamiento del tercer teorema de Sylow:

Teorema 3.36 *Si G es un grupo finito de orden $p^n m$, donde $p \nmid m$ y la intersección de dos p-subgrupos de Sylow de G (distintos) tiene orden a lo sumo p^k, entonces el número ν_p de p-subgrupos de Sylow de G cumple $\nu_p \equiv 1 \pmod{p^{n-k}}$.*

Basta tener en cuenta que, según hemos visto, la acción de P sobre el conjunto de los p-subgrupos de Sylow de G, cada órbita tiene cardinal $|P : P \cap Q|$, y esto vale 1 cuando $Q = P$ y es un múltiplo de p^{n-k} cuando $P \neq Q$, lo cual nos da la congruencia indicada.

Nota Conviene observar que el "a lo sumo" del teorema anterior es necesario porque un grupo finito G puede tener p-subgrupos de Sylow P_1, P_2, P_3, P_4 de modo que $|P_1 \cap P_2| \neq |P_3 \cap P_4|$. Basta pensar en (casi) cualquier producto, como $G = \Sigma_3 \times \Sigma_3$. Si llamamos P_1, P_2, P_3 a los tres 2-subgrupos de Sylow de Σ_3, entonces $P_1 \times P_1$ y $P_1 \times P_2$ son 2-subgrupos de Sylow de G cuya intersección tiene orden 2, mientras que $P_1 \times P_1$ y $P_2 \times P_2$ son 2-subgrupos de Sylow cuya intersección es trivial. ∎

Teorema 3.37 (Argumento de Frattini) *Si $K \trianglelefteq G$ y Q es un q-subgrupo de Sylow de K, entonces $G = KN_G(Q)$.*

DEMOSTRACIÓN: Si $g \in G$, entonces $Q^g \leq K^g = K$ es un q-subgrupo de Sylow de K, luego existe $k \in K$ tal que $Q^g = Q^k$, luego $gk^{-1} \in N_G(Q)$, luego $g \in KN_G(Q)$. ∎

Veamos algunas aplicaciones:

Teorema 3.38 *Si p es un primo $p \equiv -1 \pmod 4$, entonces todo grupo no abeliano de orden $4p$ es isomorfo a D_{4p} o a Q_{4p} (o a A_4 en el caso $p = 3$).*

DEMOSTRACIÓN: Sea G un grupo no abeliano de orden $4p$, tenemos que $\nu_p \mid 4$ y $\nu_p \equiv 1 \pmod{4p}$. La única posibilidad es $\nu_p = 1$ salvo si $p = 3$, en cuyo caso puede ser $\nu_p = 4$. Vamos a considerar este caso particular. Sea P

un 3-subgrupo de Sylow de G y supongamos que no es normal. Entonces la acción por multiplicación de G sobre el conjunto $\Omega = (G/P)_d$ determina un homomorfismo $\tau : G \longrightarrow \Sigma_\Omega$ tal que $\mathrm{N}(\tau) \leq P$. Como P no es normal, tiene que ser $\mathrm{N}(\tau) = 1$, luego G es isomorfo a un subgrupo de Σ_4 de orden 12, luego $G \cong A_4$.

A partir de aquí volvemos al caso de un primo p arbitrario, pero ahora podemos suponer que G tiene un p-subgrupo de Sylow normal $P = \langle a \rangle$. Sea además Q un 2-subgrupo de Sylow. Entonces $G \cong Q[P]$, donde el producto semidirecto se calcula respecto de la acción de Q sobre P por conjugación. Para que G sea no abeliano es necesario que esta acción no sea trivial, es decir, que venga determinada por un homomorfismo $\alpha : Q \longrightarrow \mathrm{Aut}(P)$ no trivial.

Tenemos que $\mathrm{Aut}(P) \cong U_p \cong C_{p-1}$ y, por hipótesis $4 \nmid p-1$, luego $\mathrm{Aut}(P)$ no tiene elementos de orden 4 y tiene un único automorfismo σ de orden 2, que es el dado por $\sigma(a) = a^{-1}$.

Hay dos posibilidades, según si $Q \cong C_4$ o si $Q \cong C_2 \times C_2$, pero en ambos casos hay un único homomorfismo α posible. En el primero, si $Q = \langle b \rangle$, tiene que ser $\alpha(b) = \sigma$, y en el segundo, el núcleo de α será un subgrupo de orden 2, digamos $\langle c \rangle$, y $H = \langle b, c \rangle$, donde $\alpha(b) = \sigma$.

Podríamos analizar los productos semidirectos determinados por estas acciones para concluir que el primero es isomorfo a Q_{4p} y el segundo a D_{4p}, pero no es necesario. Nos basta con el hecho de que sólo hay dos posibilidades, luego no puede haber más que dos grupos no abelianos de orden $4p$ no isomorfos entre sí (o tres si $p = 3$). Para terminar observamos que los grupos D_{4p} y Q_{4p} no son isomorfos entre sí (ni son isomorfos a A_{12} en el caso $p = 3$). En efecto, en Q_{4p} hay elementos de orden 4, mientras que en D_{4p} no los hay (y en A_4 tampoco y A_4 no tiene elementos de orden 6, mientras que D_{12} sí que los tiene). Esto implica que los grupos considerados son los únicos grupos de orden $4p$ salvo isomorfismo. ∎

Teorema 3.39 *Si p es un primo $p \equiv 1 \pmod 4$, entonces todo grupo no abeliano de orden $4p$ es isomorfo a D_{4p}, Q_{4p} o al dado por la presentación*

$$\left\langle a, b \mid a^p = b^4 = 1,\ a^b = a^r \right\rangle,$$

donde r cumple $o_p(r) = 4$ (pero elecciones distintas de r dan lugar a grupos isomorfos, por lo que sólo hay 3 grupos en total).

Demostración: Si G tiene orden $4p$, el tercer teorema de Sylow nos da que $\nu_p \mid 4$ y $\nu_p \equiv 1 \pmod p$, luego la única posibilidad es $\nu_p = 1$, con lo que G tiene un p-subgrupo de Sylow normal, digamos N. Sea H un 2-subgrupo de Sylow, de modo que $G \cong H[N]$, donde el producto semidirecto se construye respecto de la acción de H sobre N por conjugación. Para que G sea no abeliano la acción tiene que ser distinta de la trivial. Tenemos que $\mathrm{Aut}\, N \cong U_p \cong C_{p-1}$. Concretamente, si $N = \langle a \rangle$, entonces $\mathrm{Aut}(N)$ posee dos únicos elementos de orden 4 (mutuamente inversos), determinados por que $\sigma(a) = a^r$ (y entonces $\sigma^2(a) = a^{-1}$ es el único automorfismo de orden 2).

Si $H \cong C_2 \times C_2$, una acción no trivial $\alpha : H \longrightarrow \mathrm{Aut}(N)$ tendrá un núcleo de orden 2, digamos $\langle z\rangle$, de modo que $H = \langle y, z\rangle$, donde $\alpha(y) = \sigma^2$, $\alpha(z) = 1$. Esto equivale a que $a^y = a^{-1}$, $a^z = a$. Como $az = za$, resulta que $x = az$ tiene orden $2p$ y $x^y = a^y z^y = a^{-1}z^{-1} = (az)^{-1} = x^{-1}$ (donde hemos usado que a y z conmutan). Así pues, $G = \langle a, y\rangle$, donde $x^{10} = y^2 = 1$, $x^y = x^{-1}$, lo cual prueba que $G \cong D_{4p}$.

Si $H \cong C_4 = \langle b\rangle$ hay dos homomorfismos no triviales $\alpha : H \longrightarrow \mathrm{Aut}(N)$, según si $\alpha(b) = \sigma$ o $\alpha(b) = \sigma^2$. En el primer caso G satisface las relaciones de la presentación del enunciado. En principio, tendríamos dos grupos, según si tomamos el exponente r o $-r$, pero cambiando a por a^{-1} siempre podemos elegir el generador de P para que r sea cualquiera de los dos posibles sin cambiar de grupo.

Es fácil ver que el grupo G^* determinado por dicha presentación tiene orden a lo sumo $4p$, pues todos sus elementos pueden expresarse en la forma $a^i b^j$, con $0 \le i < p$, $0 \le j < 4$. Por el teorema de von Dyck 3.18 existe un epimorfismo $G^* \longrightarrow H[N]$, luego $|G^*| = 4p$ y $H[N] \cong G^*$.

Ahora podríamos analizar el producto semidirecto correspondiente a la acción dada por $\alpha(b) = \sigma^2$, pero no es necesario, pues ya sabemos que a lo sumo hay un tercer grupo no abeliano no isomorfo a los dos que hemos encontrado, y basta observar que el grupo dicíclico Q_{4p} está en ese caso, pues tiene $2p$ elementos de orden 4, mientras que D_{4p} no tiene ninguno y, por otra parte, D_{4p} y Q_{4p} tienen elementos de orden $2p$ y el grupo dado por la presentación no tiene ninguno (sus elementos tienen orden $1, 2, 4, p$). ∎

Teorema 3.40 *Todo grupo simple de orden* 60 *es isomorfo a* A_5.

Demostración: Sea G un grupo simple de orden $|G| = 2^2 \cdot 3 \cdot 5$. Por el tercer teorema de Sylow, tenemos que $\nu_2 = 1, 3, 5, 15$, pero descartamos $\nu_2 = 1$ porque entonces G tendría un 2-subgrupo de Sylow normal, y también $\nu_2 = 3$ por el teorema 2.29, ya que ν_2 es el índice del normalizador de un 2-subgrupo de Sylow.

Basta probar que G tiene un subgrupo H de índice 5, pues entonces el teorema de Cayley nos da un monomorfismo $G \longrightarrow \Sigma_5$, de donde se sigue que G es isomorfo al único subgrupo de Σ_5 de índice 2, que es A_5.

Si $\nu_2 = 5$, entonces el normalizador de un 2-subgrupo de Sylow es el subgrupo buscado, así que podemos suponer que $\nu_2 = 15$ (en realidad este caso no puede darse, porque A_5 cumple que $\nu_2 = 5$).

Por otro lado, $\nu_5 \mid 12$ y $\nu_5 \equiv 1$ (mód 5), luego $\nu_5 = 1, 6$, pero tiene que ser $\nu_5 = 6$, ya que no puede haber un 5-subgrupo de Sylow normal. Como dos 5-subgrupos de Sylow tienen intersección trivial, cada uno de ellos contiene 4 elementos de orden 5 distintos, luego G tiene un total de $6 \cdot 4 = 24$ elementos de orden 5.

Si todos los 2-subgrupos de Sylow tuvieran intersección trivial, habría un total de $15 \cdot 3 = 45$ elementos de orden 2 o 4, pero $24 + 45 = 69 > 60$, luego tiene que haber dos 2-subgrupos de Sylow P y Q tales que $|P \cap Q| = 2$. Como los grupos de orden 4 son abelianos, $P \cap Q$ es invariante por conjugación tanto

por elementos de P como de Q, luego $P \cap Q \trianglelefteq H = \langle P, Q\rangle$. Esto hace que $H < G$, y $|H| \geq |PQ| = 8$, luego $|H| = 24$ (ya que H no puede tener índice 3) y tenemos igualmente un subgrupo de índice 5. ∎

Podemos mejorar sustancialmente el teorema anterior:

Teorema 3.41 *Todo grupo simple no abeliano de orden menor o igual que* 100 *es isomorfo a* A_5.

Demostración: Sea G un grupo simple no abeliano tal que $|G| \leq 100$ y sea p el mayor primo que divida a $|G|$. Si $p \geq 11$, entonces $\nu_p \geq 1 + p \geq 12$, luego, si P es un p-subgrupo de Sylow,

$$|G| = |N_G(P)||G : N_G(P)| \geq p(1 + p) \geq 11 \cdot 12 = 132,$$

lo cual es imposible, así que $p \leq 7$.

Si $p = 7$, entonces $\nu_7 = 7k + 1$, luego si P es un 7-subgrupo de Sylow,

$$7(7k + 1) \leq |N_G(P)||G : N_G(P)| = |G| \leq 100,$$

lo que obliga a que $k = 1$, luego $\nu_7 = 8$. Así $7 \cdot 8 \mid |G| \leq 100$, luego de hecho $|G| = 56$. Además G tiene exactamente $8 \cdot 6 = 48$ elementos de orden 7, pero tiene que haber más de un 2-subgrupo de Sylow, luego tiene que haber al menos 9 elementos más (los 8 de un 2-subgrupo de Sylow y alguno de otro 2-subgrupo de Sylow) y esto ya suma $48 + 8 + 1 = 57 > 56$.

Si $p = 5$, ahora las posibilidades son $\nu_5 = 6, 11, 16$, pero descartamos $\nu_5 = 11$, ya que 5 es el mayor primo que divide a $|G|$. También descartamos $\nu_5 = 16$, pues entonces $5 \cdot 16 = 80 \mid |G| \leq 100$, luego $|G| = 80$ y un 2-subgrupo de Sylow tiene índice 5, luego el teorema de Cayley nos da un monomorfismo $G \longrightarrow \Sigma_5$, lo cual es imposible, pues 80 no divide a $|\Sigma_5|$.

Si $\nu_5 = 6$, entonces $6 \cdot 5 = 30 \mid |G|$, luego $|G| = 30, 60, 90$, pero descartamos $30 = 2 \cdot 16$ y $90 = 2 \cdot 45$ por 2.28, luego tiene que ser $|G| = 60$ y el teorema anterior prueba que $G \cong A_5$.

Consideramos finalmente el caso $p = 3$, de modo que $|G| = 2^a 3^b$, donde $a \geq 3$ porque G no puede ser un 3-grupo ni tener un 3-subgrupo de Sylow de índice 2 o 4. Por lo tanto $b \leq 2$, pero no puede ser $b = 1$, porque entonces un 2-subgrupo de Sylow tendría índice 3, luego es $|G| = 2^3 \cdot 3^2 = 72$.

El tercer teorema de Sylow, teniendo en cuenta que tiene que ser $9 \cdot \nu_3 \leq 72$, nos da que $\nu_3 = 4$, pero esto es imposible, porque G no puede tener subgrupos de índice 4. ∎

Ahora vamos a caracterizar los números naturales para los que sólo hay grupos abelianos de ese orden, para lo cual necesitamos un resultado previo:

Teorema 3.42 *Si G es un grupo finito no abeliano cuyos subgrupos propios sean todos abelianos, entonces $|G|$ es divisible a lo sumo entre dos primos.*

DEMOSTRACIÓN: Veamos en primer lugar que G no es simple, es decir, que tiene subgrupos normales propios.

Un subgrupo M de G se dice maximal si $M < G$ y no existe ningún subgrupo intermedio $M < H < G$. Obviamente, todo grupo finito tiene subgrupos maximales. Si 1 es maximal, eso significa que G no tiene subgrupos propios, lo cual implica que es cíclico (pues el subgrupo generado por cualquier elemento no trivial tiene que ser G) y de hecho $G \cong C_p$, porque un grupo cíclico de orden no primo sí que tiene subgrupos.

Si partimos de que G es no abeliano, sus subgrupos maximales no son triviales. Vamos a probar que G tiene subgrupos normales propios. En caso contrario sería $Z(G) = 1$. Sean M_1 y M_2 dos subgrupos maximales de G y veamos que $M_1 \cap M_2 = 1$.

En efecto, si $g \in M_1 \cap M_2$, como ambos grupos son abelianos, se cumple que $M_1, M_2 \leq C_G(g)$, luego $C_G(g)$ contiene estrictamente a ambos grupos, luego por la maximalidad $C_G(g) = G$, luego $g \in Z(g) = 1$.

Si M es un subgrupo maximal

$$\left| \bigcup_{g \in G} M^g \right| = |G| - |G : M| + 1.$$

En efecto, los subgrupos M^g son todos maximales, y hemos probado que la intersección de dos de ellos es trivial, y el número de conjugados distintos es $|G : N_G(M)|$, pero, $M \leq N_G(M) \leq G$ y estamos suponiendo que M no es normal en G, luego por la maximalidad tiene que ser $N_G(M) = M$, luego hay $|G_M|$ conjugados M^g distintos, y en cada uno de ellos hay $|M| - 1$ elementos distintos, luego en la unión hay $|G : M|(|M| - 1)$ elementos distintos más el neutro, lo que da el valor indicado.

Como $|M| \geq 2$, tenemos que

$$|G| > |G| - |G : M| + 1 \geq |G| - |G|/2 + 1 = |G|/2 + 1.$$

En particular, la unión $\bigcup_{g \in G} M^g$ no puede ser todo G, luego podemos tomar $g \in G$ que no esté en la unión. Como G no es cíclico, $\langle g \rangle < G$, luego podemos tomar un subgrupo maximal $\langle g \rangle \leq M' < G$. Hemos visto que $M^g \cap M'^{g'} = 1$, luego también

$$\bigcup_{g \in G} M^g \cap \bigcup_{g \in G} M'^g = 1,$$

pero cada unión tiene al menos $|G|/2 + 1$ elementos, luego la unión

$$\bigcup_{g \in G} M^g \cup \bigcup_{g \in G} M'^g$$

tiene, además del neutro 1, al menos $|G|/2$ elementos de la primera unión y otros $|G|/2$ elementos distintos en la segunda unión, lo que hace un total de $|G| + 1$ elementos en la unión completa, lo cual es imposible.

Con esto tenemos la existencia de un subgrupo normal $1 < N \lhd G$. Podemos tomarlo del mayor orden posible, lo que se traduce en que no hay subgrupos

normales $N < N' < G$ o, lo que es lo mismo, tal que el cocienteG/N es simple, y todos sus subgrupos son abelianos. Aplicando a G/N lo que hemos probado, G/N tiene que ser abeliano y, como no tiene subgrupos propios, tiene que ser cíclico de orden primo p.

Además N es abeliano. Si $q \mid |G|$, $q \neq p$, sea Q un q-subgrupo de Sylow de N, que será también un q-subgrupo de Sylow de G, pero, como N es abeliano, $N \leq N_G(Q) \leq G$, pero, por el teorema 3.34, no puede ser $N_G(Q) = N \lhd G$, luego tiene que ser $N_G(Q) = G$ (porque $|G : N| = p$, luego no hay subgrupos intermedios). Así pues, $Q \lhd G$, es decir, todos los subgrupos de Sylow de G son normales salvo tal vez los p-subgrupos.

Si G tuviera un p-subgrupo de Sylow normal, entonces G sería el producto directo de sus p-subgrupos de Sylow (que son abelianos, por hipótesis), luego sería abeliano. Así pues, G tiene al menos dos p-subgrupos de Sylow distintos, P y P'.

El grupo $\langle P, P'\rangle$ no puede ser abeliano, porque tendría dos p-subgrupos de Sylow distintos, luego, por hipótesis $G = \langle P, P'\rangle$. Sea P_1 un p-subgrupo de Sylow de N, de modo que $P_1 = P \cap N$. Si $g \in P \setminus P_1$, entonces $p \notin N$, luego $\langle N, g\rangle = G$ (porque no hay subgrupos intermedios).

Como N es el producto directo de sus subgrupos de Sylow, si g conmutara con los elementos de cada subgrupo de Sylow, entonces conmutaría con todos los elementos de N, luego $G = \langle N, g\rangle$ sería abeliano. Por lo tanto, hay un q-subgrupo de Sylow Q de N tal que g no conmuta con todos los elementos de Q. No puede ser $q = p$, porque entonces $Q = P_1$, pero $g \in P$ sí que conmuta con los elementos de P_1, porque P es abeliano.

Así pues, $G = \langle Q, g\rangle$, porque el subgrupo de la derecha no es abeliano, pero $Q \lhd G$, luego $G = Q\langle g\rangle$ y $|G| = |Q||\langle g\rangle|$, donde el primer factor es potencia de q y el segundo es potencia de p. ∎

Con esto podemos probar:

Teorema 3.43 *Los números naturales n tales que todo grupo de orden n es abeliano son exactamente los de la forma $n = p_1^{e_1} \cdots p_r^{e_r}$, donde los primos p_i son distintos dos a dos, los exponentes cumplen $0 \leq e_i \leq 2$ y $p_i \nmid p_j^{e_j} - 1$, para todo i, j.*

Demostración: Veamos en primer lugar que si n tiene la forma indicada todos los grupos de orden n son abelianos. Si no es así, podemos tomar el menor número natural n de la forma indicada para el que existe un grupo G no abeliano de orden n. Entonces todos los subgrupos propios de G son del mismo tipo, pues si $p \nmid q^2 - 1 = (q+1)(q-1)$, también $p \nmid q - 1$, luego todo subgrupo propio de G es abeliano. Por el teorema anterior $|G|$ es divisible a lo sumo entre dos primos. No puede ser $|G| = p$ o $|G| = p^2$, porque entonces G sería abeliano (teorema 2.6), ni tampoco $|G| = pq$ por 3.28. Así pues, las únicas posibilidades son $|G| = p^2q$ o bien $|G| = p^2q^2$. Sólo tenemos que descartar estos casos.

Si $|G| = p^2q$, el número de p-subgrupos de Sylow cumple las relaciones $\nu_p \mid q$ y $\nu_p \equiv 1 \pmod p$, y por hipótesis $p \nmid q - 1$, luego tiene que ser $\nu_p = 1$.

Similarmente, $\nu_q \mid p^2$ y $\nu_q \equiv 1 \pmod q$, pero $q \nmid p^2 - 1$, luego también $q \nmid p - 1$, luego tiene que ser $\nu_q = 1$.

Por lo tanto, G tiene subgrupos de Sylow normales P y Q de órdenes p^2 y q^2, luego $G = P \times Q$ es abeliano. El caso p^2q^2 se descarta igualmente.

Ahora veamos que si todos los grupos de orden n son abelianos, se tienen que cumplir las condiciones del enunciado. Sea $n = p_1^{e_1} \cdots p_r^{e_r}$. Si $e_i > 2$, hemos visto en la sección 3.4 que existe un grupo no abeliano H de orden p_i^3, y sólo tenemos que multiplicarlo por cualquier grupo de orden n/p_i^3 (por ejemplo, un grupo cíclico) para obtener un grupo no abeliano de orden n.

Si $p_i \mid p_j^{e_j} - 1$ distinguimos dos casos: si $e_j = 1$, tenemos que $p_i \mid p_j - 1$, y en la sección 3.4 hemos visto que existe un grupo no abeliano de orden p_ip_j. Multiplicándolo por un grupo de orden n/p_ip_j obtenemos un grupo no abeliano de orden n.

Si $e_j = 2$, tenemos que $p_i \mid p_j^2 - 1 = (p_j + 1)(p_j - 1)$. Si $p_i \mid p_j - 1$ estamos en el caso anterior, luego podemos suponer que $p_i \mid p_j + 1$. Simplificando la notación, tenemos que $q \mid p + 1$ y basta probar que existe un grupo no abeliano de orden p^2q.

Sea $k = \mathbb{Z}/p\mathbb{Z}$, que es un cuerpo de p elementos y sea $V = k^2$, que es un k-espacio vectorial de dimensión 2. Su grupo aditivo es isomorfo al producto $C_p \times C_p$. Según hemos razonado en la nota tras el teorema 3.32, se cumple que $|\operatorname{Aut} V| = p(p-1)^2(p+1)$ y, como $q \mid p + 1$, la teoría de Sylow nos da que existe $\tau \in \operatorname{Aut} V$ de orden q, luego, llamando $H = \langle\tau\rangle$, tenemos un grupo C_q que actúa no trivialmente sobre $V \cong C_p \times C_p$, luego el producto semidirecto $H[V]$ es un grupo no abeliano de orden p^2q. ∎

Este teorema se aplica a los órdenes

$$2, 3, 4, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 29, 31, 33, 35, 37, 41, 43, 45, 47, 49, \ldots$$

3.7 Ejemplo: El grupo LG(2, 3)

Como aplicación de los resultados que hemos obtenido en este capítulo vamos a estudiar el grupo $G = \mathrm{LG}(2, 3)$ formado por las matrices regulares 2×2 sobre el cuerpo $k = \mathbb{Z}/3\mathbb{Z}$ de 3 elementos.

Como en el caso de $\mathrm{LG}(2, 5)$ que hemos estudiado en la sección 3.3, el orden de G es el número de bases de k^2. Para elegir el primer vector de una base tenemos $9-1 = 8$ posibilidades y, para elegir el segundo, $9-3 = 6$ posibilidades, luego $|G| = 8 \cdot 6 = 2^4 \cdot 3 = 48$.

Los elementos de G son matrices 2×2 con coeficientes 0 y ± 1, sujetas a la condición de que su determinante sea no nulo, que equivale a la regularidad de las matrices [ITAl 11.7].

Según [Al 4.39], tenemos que $Z(G) = \{\pm I\}$. Por otra parte, podemos considerar el epimorfismo $\det : G \longrightarrow \{\pm 1\}$ que a cada matriz le asigna su determinante. Su núcleo, el subgrupo formado por las matrices de determinante 1, es el grupo *lineal especial* $E = \mathrm{LE}(2, 3)$, análogo al grupo $\mathrm{LE}(2, 5)$ cuya presentación hemos calculado antes. Así, $|\mathrm{LE}(2, 3)| = 24$.

Es fácil ver que las matrices triangulares superiores o inferiores, es decir, las de la forma

$$\begin{pmatrix} \pm 1 & \alpha \\ 0 & \pm 1 \end{pmatrix} \quad \text{o} \quad \begin{pmatrix} \pm 1 & 0 \\ \alpha & \pm 1 \end{pmatrix}, \qquad \alpha = -1, 0, 1,$$

forman, respectivamente, dos subgrupos de orden 12. Si los llamamos T_s y T_i, vemos que contienen matrices de determinante -1, por lo que las intersecciones $T_s \cap E$ y $T_i \cap E$ son subgrupos de orden 6, y son cíclicos, pues están generados por

$$\sigma_s = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_i = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix},$$

que tienen orden 6.

La intersección $\langle \sigma_s \rangle \cap \langle \sigma_i \rangle$ está formada por matrices que son a la vez triangulares superiores e inferiores, luego son diagonales, y tienen determinante 1, luego tiene que ser $\langle \sigma_s \rangle \cap \langle \sigma_i \rangle = Z(G)$. Por lo tanto,

$$|\langle \sigma_s \rangle \langle \sigma_i \rangle| = \frac{6 \cdot 6}{2} = 18.$$

Como $\langle \sigma_s \rangle \langle \sigma_i \rangle \subset \langle \sigma_s, \sigma_i \rangle \leq E$, el subgrupo generado por σ_s, σ_i tiene orden divisor de 24 y mayor o igual que 18. La única posibilidad es que $E = \langle \sigma_s, \sigma_i \rangle$. Notemos que en este caso el producto $\langle \sigma_s \rangle \langle \sigma_i \rangle$ no es un subgrupo.

Por otro lado,

$$i = \sigma_s \sigma_i = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \quad j = \sigma_i \sigma_s = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad k = ij = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

son elementos de E de orden 4, pues se comprueba que $i^2 = j^2 = k^2 = -I$. Esto sugiere que $Q = \langle i, j \rangle$ es un grupo de tipo Q_8. Podemos justificarlo sin apenas necesidad de ningún cálculo adicional. En efecto, sólo tenemos que observar que $E/Z(G)$ es un grupo de orden 12 generado por las clases $x = \sigma_s Z(G)$, $y = \sigma_i Z(G)$, que cumplen

$$x^3 = y^3 = (xy)^2 = 1.$$

En efecto, $x^3 = \sigma_s^3 Z(G) = -IZ(G) = 1Z(G)$, e igualmente $y^3 = 1$, y

$$(xy)^2 = i^2 Z(G) = -IZ(G) = 1Z(G).$$

En virtud de la presentación que hemos obtenido de A_4, podemos concluir que $E/Z(G) \cong A_4$, y esto nos aporta mucha información.

Para empezar, sabemos que A_4 tiene un único subgrupo normal de orden 4, de tipo $C_2 \times C_2$, formado por todos sus elementos de orden 2, luego en $E/Z(G)$ dicho subgrupo tiene que ser $Q/Z(G)$, donde $Q = \langle i, j \rangle$ es necesariamente un grupo de orden 8 (no es necesario comprobar nada, sino que ya sabemos que tiene que ser así).

Sin más que comprobar que $ij \neq ji$, concluimos que Q es un grupo no abeliano de orden 8 con al menos tres elementos de orden 4, luego tiene que

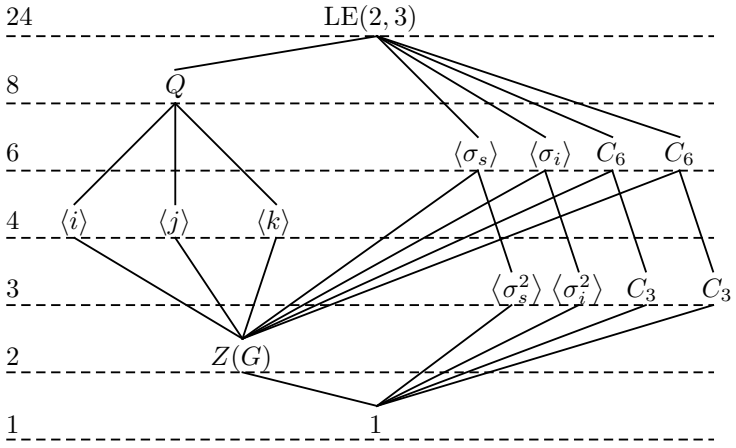
ser $Q \cong Q_8$. Más aún, $Q/Z(G)$ es el único subgrupo de orden 4 de $E/Z(G)$, luego Q es el único subgrupo de orden 8 de E que contiene a $Z(G)$. De hecho, Q es el único subgrupo de orden 8 de E, pues si hubiera otro, digamos Q', sería $|Q'Z(G)/Z(G)| = 8$, con lo que $E/Z(G)$ sería un grupo de orden 12 con un subgrupo de orden 8. Como Q es el único subgrupo de E de orden 8, es característico en E y, como $E \trianglelefteq G$, tenemos que $Q \trianglelefteq G$, luego es el único 2-subgrupo de Sylow de E.

También sabemos que A_4 no tiene subgrupos de orden 6, luego E no tiene subgrupos de orden 12. Esto implica a su vez que E es el único subgrupo de G de índice 2, pues si hubiera otro, digamos E^*, tendría que ser

$$|E/(E \cap E^*)| = EE^*/E^* \leq G/E^*,$$

luego $|E : E \cap E^*| = 2$, y ya hemos visto que no se da el caso.

Sabemos que $\langle\sigma_s\rangle$ no es normal en E, pues hemos visto que el producto $\langle\sigma_s\rangle\langle\sigma_i\rangle$ no es un subgrupo. Por lo tanto, $\langle\sigma_s\rangle \leq N_E(\langle\sigma_s\rangle) < E$. Como E no tiene subgrupos de orden 6, tiene que ser $N_E(\langle\sigma_s\rangle) = \langle\sigma_s\rangle$, luego resulta que $|E : N_E(\langle\sigma_s\rangle)| = 4$ es el número de subgrupos de E conjugados con $\langle\sigma_s\rangle$. Como A_4 tiene 4 subgrupos de orden 3, concluimos que estos cuatro subgrupos de orden 6 son todos los que tiene E, y así tenemos completamente determinada la estructura de E, reflejada en el esquema siguiente:



Observemos que los cuatro subgrupos C_6 contienen 2 elementos de orden 6 cada uno, lo que hace un total de 12 elementos de orden 6. La intersección de dos de ellos contiene a $Z(G)$, luego tiene que ser justamente $Z(G)$, luego en cada uno hay 3 elementos de orden 2 distintos de los de los demás subgrupos, lo que hace un total de 8 elementos de orden 3, que determinan 4 subgrupos de tipo C_3. Si sumamos los 6 elementos de orden 4 que hay en Q, tenemos ya los 24 elementos de E:

orden	1	2	3	4	6
cantidad	1	1	8	6	8

La intersección $V = T_s \cap T_i$ está formada por las cuatro matrices diagonales, las dos de $Z(G)$ y otras dos de determinante negativo:

$$\tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \tau^* = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Se trata de un subgrupo de tipo $C_2 \times C_2$. Trivialmente, $G = EV = \langle \sigma_s, \sigma_i, \tau \rangle$.

Como $Q \trianglelefteq G$, podemos formar el subgrupo $S = QV$, que tiene orden 16, luego es un 2-subgrupo de Sylow de G. Uno de sus elementos es

$$\alpha = i\tau = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

y resulta que tiene orden 8, pues podemos calcular $\alpha^2 = -k$, que tiene orden 4.

Así pues, G también tiene elementos de orden 8. Si se cumpliera que $\alpha^\tau = \alpha^{-1}$ tendríamos que $S \cong D_{16}$, pero no es exactamente así. Una simple comprobación muestra que $\alpha^\tau = \alpha^3$, por lo que $S \cong C_2[C_8]_3$. No es el único 2-subgrupo de Sylow, pues al clasificar los grupos de orden 16 hemos visto que tiene 5 elementos de orden 2 y G tiene más, ya que tiene subgrupos D_{12}, cada uno de los cuales tiene 7 elementos de orden 2. Como no puede haber subgrupos intermedios, tiene que ser $N_G(S) = S$, luego S tiene exactamente 3 subgrupos conjugados. La intersección de dos cualesquiera de ellos tiene que ser Q (porque es normal, y está en todos los conjugados), luego cada uno tiene 4 elementos de orden 8 distintos, lo que hace un total de 12 elementos de orden 8 en G. De los 5 elementos de orden 2 que tiene cada subgrupo de Sylow, el único común a todos ellos es $-I$, luego en G hay otros 12 elementos más de orden 2, y esto completa los 48 elementos de G:

orden	1	2	3	4	6	8
cantidad	1	13	8	6	8	12

La tabla muestra que si a los 24 elementos de E que ya teníamos identificados les sumamos los 12 nuevos elementos de orden 2 y los 12 de orden 8 tenemos ya los 48 elementos, luego no hay más.

A partir de aquí ya pura rutina concluir que los subgrupos de G son:

- El propio $\mathrm{LG}(2,3)$, de orden 48.
- $\mathrm{LE}(2,3)$, que es el único subgrupo de orden 24.
- Los 3 subgrupos de Sylow de orden 16, isomorfos a $C_2[C_8]_3$.
- 4 subgrupos D_{12}, conjugados entre sí (porque $N_G(D_{12}) = D_{12}$).
- 1 subgrupo Q_8, el 2-subgrupo de Sylow normal de $\mathrm{LE}(2,3)$.
- 3 subgrupos C_8, conjugados entre sí, contenidos uno en cada 2-sylow.
- 3 subgrupos D_8 conjugados entre sí, contenidos uno en cada 2-Sylow.

- 4 subgrupos C_6, uno contenido en cada D_{12} y conjugados entre sí (su normalizador es D_{12}).
- 8 subgrupos D_6, contenidos dos en cada D_{12}. Su normalizador es D_{12}, que tiene índice 4, por lo que forman dos clases de conjugación de 4 subgrupos cada una.
- 3 subgrupos C_4, conjugados entre sí, contenidos en Q.
- 6 subgrupos $C_2 \times C_2$. Cada uno contiene a $-I$ y otros dos elementos de orden 2. Todos son conjugados con el subgrupo V de las matrices diagonales (pues $N_G(V) = D_8$).
- 12 subgrupos C_2 conjugados entre sí, más $Z(G)$, que es normal. Son conjugados porque sus normalizadores son los $C_2 \times C_2$.
- El subgrupo trivial 1.

Como aplicación podemos clasificar los grupos de orden 18:

Teorema 3.44 *Todo grupo de orden* 18 *es isomorfo a uno de los cinco grupos siguientes:*

1. C_{18},
2. $C_2 \times C_3 \times C_3 \cong C_3 \times C_6$,
3. D_{18}
4. $D_6 \times C_3$
5. $\langle a, b, c \mid a^3 = b^3 = c^2 = 1, ab = ba, a^c = a^{-1}, b^c = b^{-1}\rangle$.

DEMOSTRACIÓN: Si G tiene orden 18, obviamente tiene un 3-subgrupo de Sylow normal N, que puede ser isomorfo a C_9 o a $C_3 \times C_3$. Si $H = \langle c\rangle$ es un 2-subgrupo de Sylow, entonces $G \cong H[N]$, donde el producto semidirecto se calcula respecto de la acción de H sobre N por conjugación.

Si $N \cong C_9$, entonces $\mathrm{Aut}(N) \cong U_9 \cong C_6$, luego sólo hay un automorfismo de orden 2, luego hay dos acciones posibles $\alpha : H \longrightarrow \mathrm{Aut}(N)$, la trivial, que nos da $G \cong C_9 \times C_2 \cong C_{18}$, y la dada por $\alpha(c)(g) = g^{-1}$ que nos da $G \cong D_{18}$.

Supongamos, pues que $N \cong C_3 \times C_3$, que puede verse como un espacio vectorial de dimensión 2 sobre el cuerpo $\mathbb{Z}/3\mathbb{Z}$. Como la multiplicación está determinada por la suma, los automorfismos como espacio vectorial coinciden claramente con los automorfismos como grupo, por lo que $\mathrm{Aut}(N) \cong \mathrm{LG}(2,3)$. Según hemos visto, existen 14 homomorfismos posibles $\alpha : H \longrightarrow \mathrm{Aut}(N)$, el trivial da lugar a $G = C_3 \times C_3 \times C_2$, y los restantes tienen por imagen uno de los 13 subgrupos de orden 2 de $\mathrm{LG}(2,3)$.

Si dicha imagen es el centro, generado por la matriz $-I$, es decir, que $\alpha(c)(v) = -v$, el producto semidirecto que obtenemos cumple que $v^c = v^{-1}$

para todo $v \in N$. Si $N = \langle a, b\rangle$, entonces $G = \langle a, b, c\rangle$ y claramente se cumplen todas las relaciones del grupo 5) del enunciado. Un análisis análogo al que hemos hecho con la presentación del grupo diédrico muestra que el grupo del enunciado tiene a lo sumo 18 elementos (de la forma $a^i b^j c^k$, con $0 \leq 1 < 3$, $0 \leq j < 3$, $0 \leq k < 2$), luego tiene que ser el producto semidirecto que acabamos de construir.

El caso restante es que la imagen de α sea uno de los 12 subgrupos conjugados de orden 2 que tiene $\mathrm{LG}(2,3)$ aparte de su centro, pero las 12 acciones correspondientes son conjugadas en el sentido de la definición 3.23, y esto implica que los productos semidirectos que definen son isomorfos. Por lo tanto, en realidad sólo hay una alternativa más a las cuatro que ya hemos encontrado. Podríamos analizar la cualquiera de estas doce acciones para identificar el grupo, pero no es necesario, sino que basta observar que $D_6 \times C_3$ es un grupo de orden 18 distinto de los cuatro que hemos encontrado, con lo que necesariamente debe corresponderse con la única posibilidad que nos falta por analizar.

En efecto, $D_6 \times C_3$ no es abeliano, luego no puede ser isomorfo a ninguno de los dos grupos abelianos que hemos encontrado, sus elementos tienen órdenes $1, 2, 3, 6$, luego no es isomorfo a D_{18}, que tiene elementos de orden 9, ni tampoco al quinto grupo del enunciado, pues es fácil ver que sólo tiene elementos de órdenes $1, 2, 3$ (las relaciones implican que todos los de la forma $a^i b^i c$ tienen orden 2). ∎

El grupo $\mathrm{LE}(2,3)$ aparece en la clasificación de los grupos de orden 24 simplemente porque es uno de tales grupos:

Teorema 3.45 *Todo grupo de orden* 24 *es isomorfo a uno de los quince grupos siguientes (los cuales no son isomorfos entre sí):*

1. C_{24}, $C_2 \times C_{12}$, $C_2 \times C_2 \times C_6$,
2. Σ_4, D_{24}, Q_{24}, $\mathrm{LE}(2,3)$,
3. $C_4 \times D_6$, $C_3 \times D_8$, $C_3 \times Q_8$, $C_2 \times A_4$, $C_2 \times D_{12}$, $C_2 \times Q_{12}$,
4. $\langle a, b \mid a^3 = b^8 = 1, a^b = a^{-1}\rangle$,
5. $\langle a, b, c \mid a^3 = b^4 = c^2 = 1, \quad b^c = b^{-1}, \quad a^b = a^{-1}, \quad ac = ca\rangle$.

Demostración: Supongamos que $|G| = 24 = 2^3 \cdot 3$. La teoría de Sylow nos da que $\nu_2 = 1, 3$ y $\nu_3 = 1, 4$. Analizamos en primer lugar el caso en que $\nu_2 = 3$ y $\nu_3 = 4$, es decir, el caso en que G no tiene subgrupos de Sylow normales. Vamos a probar que, necesariamente, $G \cong \Sigma_4$.

Sea $\Omega = \{Q_1, Q_2, Q_3, Q_4\}$ el conjunto de los 3-subgrupos de Sylow, de modo que G actúa sobre Ω por conjugación, es decir, tenemos un homomorfismo de grupos $\alpha : G \longrightarrow \Sigma_\Omega$. Llamamos N a su núcleo, y sólo tenemos que probar que $N = 1$, pues entonces α es un isomorfismo.

El normalizador $N_G(Q_1)$ no contiene ningún otro Q_i, pues entonces tendría dos 2-subgrupos de Sylow con uno de ellos normal, luego $K = N_G(Q_1) \cap N_G(Q_2)$ no contiene ningún 3-subgrupo de Sylow, y es un subgrupo de $N_G(Q_1)$, que tiene orden 6, luego $|K| = 1, 2$.

Por otra parte, $N_G(Q_i)$ está formado por los elementos de G que fijan a Q_i, luego

$$N \leq \bigcap_{i=1}^{4} N_G(Q_i) \leq K.$$

Así pues, sólo necesitamos probar que $K = 1$. En caso contrario, es claro que K es un subgrupo característico, luego en particular es normal en G, y G/N es un grupo de orden 12 que tiene cuatro 3-subgrupos de Sylow Q_iN/N (pues los 8 elementos de orden 3 en G siguen siendo de orden 3 en G/N). Por lo tanto, $G/N \cong A_{12}$, luego G/N tiene un 2-subgrupo de Sylow normal P/N, luego P es un 2-subgrupo de Sylow normal en G, en contra de lo supuesto.

Supongamos ahora que $\nu_2 = 1$, es decir, que G posee un 2-subgrupo de Sylow normal P, de orden 8. Si Q es un 3-subgrupo de Sylow, tenemos que $G \cong Q[P]$, donde el producto semidirecto se construye con la acción de Q sobre P por conjugación. Vamos a distinguir casos según el tipo de P:

1. Si $P \cong C_8$, entonces $\mathrm{Aut}(P) \cong C_7$ y no tiene elementos de orden 3, luego la única acción posible de Q sobre P es la trivial, que da lugar a $G \cong C_8 \times C_3 \cong C_{24}$.

2. Si $P \cong C_2 \times C_4$, al final de la sección 3.3 hemos visto que $\mathrm{Aut}(P) \cong D_8$, que tampoco tiene elementos de orden 3, luego el producto es directo y $G \cong C_3 \times C_4 \times C_3 \cong C_2 \times C_{12}$.

3. Si $P \equiv C_2 \times C_2 \times C_2$, podemos ver a P como (el grupo aditivo de) un espacio vectorial de dimensión 3 sobre el cuerpo $k = \mathbb{Z}/2\mathbb{Z}$ de dos elementos, y el grupo de automorfismos de P como grupo coincide con el grupo de automorfismos como espacio vectorial. Sea $\sigma \in \mathrm{Aut}(P)$ tal que $\sigma^3 = 1$. Consideramos a P como $k[x]$-módulo según [Al 6.24]. Entonces tenemos que $(x^3 - 1)P = 0$ y, por las observaciones tras la definición [Al 6.29], el polinomio mínimo de σ es el menor polinomio que anula a P, luego $\mathrm{pol\,mín}\,\sigma \mid x^3 - 1 = (x-1)(x^2+x+1)$. Por lo tanto, los factores invariantes de σ tienen que ser $x-1, x-1, x-1$, o bien $(x-1)(x^2+x+1)$.

   En el primer caso $\sigma = 1$, luego si σ tiene orden 3 sus factores invariantes están unívocamente determinados. Ahora bien, según la observación tras [Al 6.31], dos matrices del grupo $\mathrm{LG}(3,k)$ son semejantes (es decir, conjugadas, en el lenguaje de la teoría de grupos) si y sólo si tienen la misma primera forma canónica o, lo que es lo mismo, dos automorfismos son conjugados si y sólo si tienen los mismos factores invariantes. En nuestro caso hemos llegado a que todos los automorfismos de P de orden 3 son conjugados. Aunque no nos hace falta, más concretamente, podemos decir que es posible fijar una base en P respecto a la cual σ venga determinado por la matriz

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Por las observaciones tras la definición 3.23, concluimos que todas las acciones no triviales de Q en P son conjugadas, luego, además del producto directo, que da lugar al grupo $G \cong C_2 \times C_2 \times C_2 \times C_6 \cong C_2 \times C_2 \times C_6$, hay un único grupo no abeliano en este caso. Podríamos llegar a una descripción explícita de G a partir de la forma canónica anterior, pero no es necesario. Podemos concluir que $G \cong C_2 \times A_4$ sin más que observar que este grupo está en el caso que estamos considerando (tiene un 2-subgrupo de Sylow normal isomorfo a $C_2 \times C_2 \times C_2$) y teniendo en cuenta que hemos probado que todos los grupos en este caso son isomorfos.

4. Si $P \cong D_8$, al final de la sección 3.3 hemos visto que $\mathrm{Aut}(P) \cong D_8$, luego la acción de Q sobre P tiene que ser trivial y $G \cong C_3 \times D_8$.

5. Si $P \cong Q_8$, en la sección [G 4.3] hemos probado que $\mathrm{Aut}(Q_8) \cong \Sigma_4$, luego, como en el caso anterior, todos los automorfismos de orden 3 son conjugados, luego sólo hay dos productos semidirectos posibles $Q[P]$, el producto directo, que nos da $G \cong C_3 \times Q_8$, y un producto semidirecto que podríamos describir, pero, sabiendo que sólo hay una posibilidad de grupo de orden 24 con un 2-subgrupo de Sylow normal isomorfo a Q_8 y que no sea $C_3 \times Q_8$, basta observar que otro grupo que cumple esto es $\mathrm{LE}(2,3)$.

Con esto hemos encontrado todos los grupos de orden 24 con un 2-subgrupo de Sylow normal (hay 3 abelianos y 3 no abelianos). Ahora suponemos que $\nu_3 = 1$, de modo que G tiene un 3-subgrupo de Sylow normal $Q = \langle a \rangle$, con lo que $G \cong P[Q]$. Observemos que ahora $\mathrm{Aut}(Q) \cong C_2$ está generado por el automorfismo dado por $\sigma(a) = a^{-1}$. Volvemos a distinguir casos según el tipo de P:

1. Si $P \cong C_8$, entonces $G \cong C_8[C_3]$, donde el producto semidirecto se construye con respecto a la única acción no trivial $\alpha : C_8 \longrightarrow \mathrm{Aut}(C_3)$ que envía a σ los generadores de C_8. Es fácil ver que

$$G = \left\langle a, b \mid a^3 = b^8 = 1, a^b = a^{-1} \right\rangle.$$

   (Con la acción trivial volveríamos a obtener C_{24}, pues este grupo tiene tanto un 3-subgrupo de Sylow normal como un 2-subgrupo de Sylow normal).

2. Si $P \cong C_2 \times C_4$, tenemos que estudiar las acciones $\alpha : C_2 \times C_4 \longrightarrow \mathrm{Aut}(C_3)$. La acción trivial nos da de nuevo $C_2 \times C_4 \times C_3 \cong C_2 \times C_{12}$.

   Si el núcleo de α es cíclico (de orden 4), digamos que está generado por $c \in P$, podemos tomar otro elemento b de orden 2 que no esté en $\langle c \rangle$, y así $P = \langle b, c \rangle$, con $\alpha(b) = \sigma$, luego $G = \langle a, b, c \rangle$, de modo que $\alpha(b) = \sigma$ se traduce en que $a^b = a^{-1}$, mientras que $\alpha(c) = 1$ se traduce en que $ac = ca$.

   El subgrupo $\langle a, b \rangle$ satisface las relaciones de D_6 y contiene un elemento de orden 2 y otro de orden 3, luego tiene que ser $\langle a, b \rangle \cong D_6$. Como c conmuta con a y b, tiene que ser $\langle a, b \rangle \trianglelefteq G$ y $\langle c \rangle \trianglelefteq G$, luego $G \cong C_4 \times D_6$.

La única posibilidad restante es que el núcleo de α sea $C_2 \times C_2$, de modo que ahora $P = \langle b, c\rangle$, donde $o(b) = 2$, $o(c) = 4$, pero $\alpha(b) = 1$, $\alpha(c) = \sigma$. Así $G = \langle a, b, c\rangle$ de modo que

$$a^3 = b^2 = c^4 = 1, \quad ab = ba, \quad bc = cb, \quad a^c = a^{-1}.$$

De la última relación se sigue que $a^{c^2} = a$, es decir, que a y c^2 conmutan. Llamemos $x = ac^2$, $y = c$, con lo que $x^3 = c^6 = c^2 = y^2$ (luego $o(x) = 6$), y además $x^y = a^c c^2 = a^{-1}c^2 = (ac^2)^{-1} = y^{-1}$. Así pues, $\langle x, y\rangle$ satisface las relaciones del grupo dicíclico

$$Q_{12} = \langle x, y \mid x^6 = 1,\ y^2 = x^3,\ y^{-1}xy = x^{-1}\rangle$$

y contiene elementos de orden 3 y 4, luego tiene que ser $\langle x, y\rangle \cong Q_{12}$. Además $\langle x, y\rangle = \langle a, c\rangle \trianglelefteq G$, $\langle b\rangle \trianglelefteq G$, pues b conmuta con a y c, luego $G = \langle x, y, b\rangle \cong C_2 \times Q_{12}$.

3. Si $P \cong C_2 \times C_2 \times C_2$, el núcleo de α tiene que ser de tipo $C_2 \times C_2$, y podemos expresar $P = \langle b, c, d\rangle$ de modo que $\alpha(b) = \sigma$, $\alpha(c) = \alpha(d) = 1$. Por consiguiente, $G = \langle a, b, c, d\rangle$, de modo que

$$a^3 = b^2 = c^2 = d^2 = 1, \quad a^b = a^{-1}, \quad ac = ca, \quad ad = da,$$

y además b, c, d conmutan entre sí. Ahora llamamos $x = ac$, $y = b$, de modo que $o(x) = 6$ y $x^y = x^{-1}$, de donde, razonando como en el caso anterior, llegamos a que $\langle x, y\rangle \cong D_{12}$ y a que $G = \langle x, y\rangle \times \langle d\rangle \cong C_2 \times D_{12}$.

4. Si $P \cong D_8$, pongamos que $P = \langle b, c\rangle$, de modo que $b^4 = c^2 = 1$, $b^c = b^{-1}$. Estudiamos las acciones $\alpha : D_8 \longrightarrow \mathrm{Aut}(C_3)$. La trivial nos da el un grupo $G \cong C_3 \times D_8$, que es un tipo que ya nos había aparecido en el caso $\nu_2 = 1$.

   Si el núcleo de α es cíclico (de orden 4), tiene que ser $\alpha(x) = 1$, $\alpha(y) = \sigma$, de modo que $G = \langle a, b, b\rangle$, con

$$a^3 = b^4 = c^2 = 1, \quad ab = ba, \quad a^c = a^{-1}.$$

   Llamamos $u = ab$, $v = c$, de modo que $o(u) = 12$ y $u^v = u^{-1}$, por lo que $\langle u, v\rangle \cong D_{24}$ y tiene que ser $G \cong D_{24}$.

   Sólo queda la posibilidad de que el núcleo de α sea de tipo $C_2 \times C_2$. Eligiendo los generadores de P, esto se traduce en que $\alpha(b) = \sigma$, $\alpha(c) = 1$, con lo que $G = \langle a, b, c\rangle$ con

$$a^3 = b^4 = c^2 = 1, \quad b^c = b^{-1}, \quad a^b = a^{-1}, \quad ac = ca,$$

   y es fácil ver que

$$G = \langle a, b, c \mid a^3 = b^4 = c^2 = 1, \quad b^c = b^{-1}, \quad a^b = a^{-1}, \quad ac = ca\rangle$$

   (esto supone comprobar que el grupo dado por la presentación tiene orden a lo sumo 24, lo cual es inmediato).

5. Si $P \cong Q_8$, pongamos que $P = \langle i, j\rangle$ con las relaciones usuales de Q_8. Consideramos una acción $\alpha : Q_8 \longrightarrow \mathrm{Aut}(C_3)$. La acción trivial nos da de nuevo $G \cong C_3 \times Q_8$. Ahora la única alternativa es que el núcleo de α sea un subgrupo cíclico de orden 4 y, cambiando de generador si es preciso, no perdemos generalidad si suponemos que está generado por i. Entonces $\alpha(i) = 1$, $\alpha(j) = \sigma$, luego $G = \langle a, i, j\rangle$, con

$$a^3 = i^4 = j^4 = 1, \quad ai = ia, \quad a^j = a^{-1},$$

y además i, j cumplen las relaciones de Q_8. Llamamos $x = ai$, $y = j$, de modo que $o(x) = 12$, con lo que el subgrupo $\langle x, y\rangle$ satisface las relaciones del grupo dicíclico

$$Q_{24} = \left\langle a, b \mid a^{12} = 1,\ b^2 = a^6,\ b^{-1}ab = a^{-1}\right\rangle,$$

de donde se concluye sin dificultad que $G \cong Q_{24}$.

La tabla siguiente muestra en qué caso hemos obtenido cada uno de los grupos no abelianos, y justifica que no hay dos que sean isomorfos entre sí salvo a lo sumo en dos casos. Ahora bien, no puede ser que $C_4 \times D_6 \cong C_2 \times Q_{12}$ porque el primero tiene 8 elementos de orden 4, mientras que el segundo tiene 12, y tampoco puede ocurrir que $D_{24} \cong D_8[C_3]$ (el último grupo del enunciado), porque el primero tiene 2 elementos de orden 4 y el segundo tiene 6. ∎

	2-Sylow	$\nu_2 = 1$	$\nu_3 = 1$
$C_8[C_3]$	C_8	no	sí
$C_4 \times D_6$	$C_2 \times C_4$	no	sí
$C_2 \times Q_{12}$		no	sí
$C_2 \times A_4$	$C_2 \times C_2 \times C_2$	sí	no
$C_2 \times D_{12}$		no	sí
Σ_4	D_8	no	no
$C_3 \times D_8$		sí	sí
D_{24}		no	sí
$D_8[C_3]$		no	sí
$C_3 \times Q_8$	Q_8	sí	sí
$\mathrm{LE}(2,3)$		sí	no
Q_{24}		no	sí

3.8 Grupos de orden menor que 32

Con los resultados que hemos obtenido tenemos clasificados todos los grupos de orden menor que 32, según se resume en la tabla de la página siguiente:

Tabla 3.1: Grupos de orden menor que 32

orden	grupos	nota	ref.
1	1		
2	C_2	orden p	1.23
3	C_3	orden p	1.23
4	$C_4,\ C_2 \times C_2$	orden p^2	2.6
5	C_5	orden p	1.23
6	$C_6,\ D_6$	orden $2p$	1.39
7	C_7	orden p	1.23
8	$C_8,\ C_2 \times C_4,\ C_2 \times C_2 \times C_2,\ D_8,\ Q_8$	orden 8	1.40
9	$C_9,\ C_3 \times C_3$	orden p^2	2.6
10	$C_{10},\ D_{10}$	orden $2p$	1.39
11	C_{11}	orden p	1.23
12	$C_{12},\ C_2 \times C_6,\ A_4,\ D_{12},\ Q_{12}$	orden $4p$	3.38
13	C_{13}	orden p	1.23
14	$C_{14},\ D_{14}$	orden $2p$	1.39
15	C_{15}	orden pq	3.28
16	14 grupos	orden 16	3.24
17	C_{17}	orden p	1.23
18	C_{18}, $C_3 \times C_6$, D_{18}, $D_6 \times C_3$, $D_6[C_3]$	orden 18	3.44
19	C_{19}	orden p	1.23
20	C_{20}, $C_2 \times C_{10}$, D_{20}, $Q_{20}, C_4[C_5]$	orden $4p$	3.39
21	C_{21}, $C_p[C_q]$	orden pq	3.30
22	C_{22}, D_{22}	orden $2p$	1.39
23	C_{23}	orden p	1.23
24	15 grupos	orden 24	3.45
25	C_{25}, $C_5 \times C_5$	orden p^2	2.6
26	C_{26}, D_{26}	orden $2p$	1.39
27	5 grupos	orden p^3	3.22
28	C_{28}, $C_2 \times C_{14}$, D_{28}, Q_{28}	orden $4p$	3.38
29	C_{29}	orden p	1.23
30	C_{30}, D_{30}, $C_3 \times D_{10}$, $C_5 \times D_6$	orden 30	3.29
31	C_{31}	orden p	1.23

Capítulo IV

Grupos resolubles

Introducimos ahora el concepto de resolubilidad de grupos, que, según hemos explicado en la introducción y como probaremos en el capítulo VII de [Al], permite caracterizar los polinomios resolubles por radicales. Tal vez el lector prefiera empezar a leer dicho capítulo y volver a éste cuando necesite el concepto de resolubilidad, para conocer así la motivación que lleva a su estudio. En realidad lo único que vamos a necesitar de este capítulo es el contenido de la primera sección.

4.1 Hechos básicos

Definición 4.1 Una *serie* en un grupo G es una sucesión de subgrupos

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

Los subgrupos G_i se llaman *términos* de la serie y los cocientes G_{i+1}/G_i se llaman *factores* de la serie. Una serie es *abeliana, cíclica,* etc. si todos sus factores son grupos abelianos, cíclicos, etc.

La serie se dice *ascendente* si empieza en $G_0 = 1$ y termina en $G_n = G$, pero a veces conviene considerar series *descendentes* que empiecen en $G_0 = G$ y terminen en $G_n = 1$. No obstante, hay que tener presente que la diferencia es meramente notacional.

Por ejemplo, un grupo G es *resoluble* si tiene una serie abeliana, y es obvio que ésta será ascendente o descendente según cómo decidamos numerar sus términos.

Así, todo grupo abeliano G es obviamente resoluble, sin más que considerar la serie $1 \trianglelefteq G$, pero también hay grupos no abelianos resolubles, como Σ_3 o Σ_4, en virtud de las series

$$1 \trianglelefteq A_3 \trianglelefteq \Sigma_3, \qquad 1 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq \Sigma_4,$$

cuyos factores son

$$A_3/1 \cong C_3, \quad \Sigma_3/A_3 \cong C_2, \qquad V_4/1 \cong C_2 \times C_2, \quad A_4/V_4 \cong C_3, \quad \Sigma_4/A_4 \cong C_2.$$

Otra familia de grupos resolubles es la de los p-grupos. En efecto, en virtud del teorema 3.6 (véase la observación posterior) es inmediato el teorema siguiente:

Teorema 4.2 *Si p es un número primo, todo p-grupo es resoluble.*

La clase de los grupos resolubles es muy amplia, lo cual se debe en gran medida a que la resolubilidad se conserva por la mayoría de las operaciones que pueden realizarse con grupos. El teorema siguiente da cuenta de ello.

Teorema 4.3 *Se cumple:*

1. *Si G es un grupo resoluble y $H \leq G$, entonces H es resoluble.*
2. *Si G es un grupo resoluble y $N \trianglelefteq G$, entonces G/N es resoluble.*
3. *Si G es un grupo y N es un subgrupo normal de G tal que N y G/N son resolubles, entonces G es resoluble.*
4. *Si H y K son subgrupos resolubles de un grupo G y $H \trianglelefteq G$, entonces HK es resoluble. En particular el producto directo de grupos resolubles es resoluble.*

Demostración: 1) Sea $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ una serie abeliana de G. Entonces

$$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_n \cap H = H$$

es una serie abeliana de H, pues, por el segundo teorema de isomorfía,

$$\begin{aligned} (G_{i+1} \cap H)\Big/(G_i \cap H) &= (G_{i+1} \cap H)\Big/\big(G_i \cap (G_{i+1} \cap H)\big) \\ &\cong G_i(G_{i+1} \cap H)\Big/G_i \leq G_{i+1}/G_i, \end{aligned}$$

y como el último grupo es abeliano, el primero también lo es. Por lo tanto H es resoluble.

2) Si $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ es una serie abeliana de G entonces

$$1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \cdots \trianglelefteq G_nN/N = G/N$$

es una serie abeliana de G/N, pues por los teoremas de isomorfía

$$\begin{aligned} \big(G_{i+1}N/N\big)\Big/(G_iN/N) &\cong G_{i+1}N\Big/G_iN = G_{i+1}(G_iN)\Big/G_iN \\ &\cong G_{i+1}\Big/(G_{i+1} \cap G_iN) \\ &\cong (G_{i+1}/G_i)\Big/\big((G_{i+1} \cap G_iN)/G_i\big), \end{aligned}$$

y el último grupo es un cociente del grupo abeliano G_{i+1}/G_i. Por lo tanto G/N es resoluble.

3) Sean

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N$$

y

$$1 = H_0/N \trianglelefteq H_1/N \trianglelefteq \cdots \trianglelefteq H_m/N = G/N$$

series abelianas de N y G/N respectivamente. Entonces una serie abeliana de G es claramente

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G.$$

4) Por el teorema de isomorfía, $HK/H \cong K/(H \cap K)$, que es resoluble por ser cociente de K. Como H también es resoluble, por el apartado anterior HK también lo es. ∎

Observemos que si G es un grupo simple, su única serie es $1 \trianglelefteq G$, por lo que no será resoluble a menos que sea abeliano, y un grupo simple y abeliano tiene que ser claramente cíclico de orden primo. Así pues, los grupos simples no abelianos, como los grupos A_n con $n \geq 5$ (teorema 2.22), no son resolubles, y en virtud del teorema anterior, tampoco lo es ningún grupo que tenga un subgrupo simple no abeliano. En particular:

Teorema 4.4 *Los grupos Σ_n y A_n son resolubles únicamente para $n \leq 4$.*

La relación entre los grupos simples y los grupos finitos resolubles se puede precisar un poco más:

Teorema 4.5 *Todo grupo finito admite una serie con factores simples. Un grupo finito es resoluble si y sólo si admite una serie con factores simples abelianos, es decir, cíclicos de orden primo.*

Demostración: Sea G un grupo finito, que podemos suponer no trivial y consideremos en él una serie cualquiera (siempre podemos tomar la serie $1 \trianglelefteq G$) o, si es resoluble, partimos de una serie abeliana. Eliminando términos repetidos podemos suponer que es estricta, es decir, que los términos cumplen $G_i \lhd G_{i+1}$.

Si uno de los factores no es simple, eso significa que tiene un subgrupo normal propio, que será de la forma N/G_i, para cierto $N \lhd G_{i+1}$, con lo que la serie se puede extender intercalando N así: $G_i \lhd N \lhd G_{i+1}$. Si el factor era abeliano, entonces el primero de los dos factores nuevos, N/G_i, es abeliano por ser subgrupo de G_{i+1}/G_i, y el segundo $G_{i+1}/N \cong (G_{i+1}/G_i) \,/\, (N/G_i)$ es abeliano por ser cociente de un grupo abeliano.

Repitiendo este proceso, tras un número finito de pasos tenemos que llegar a una serie en la que todos los factores sean simples, y abelianos si la serie original era abeliana. ∎

Así pues, un grupo resoluble admite una serie, no sólo abeliana, sino cíclica. Del teorema 3.41 se sigue ahora que A_5 es el menor grupo no resoluble, y es el único de orden menor que 120.

La serie descrita en el teorema 4.5 para un grupo resoluble tiene la mayor longitud posible, pues tiene tantos factores como primos aparecen en el orden de G. Su interés reside en que sus factores son los más sencillos posibles, pero a veces interesa todo lo contrario, es decir, trabajar con una serie abeliana de longitud mínima. Para construirla partiremos de G y en cada paso tomaremos el menor subgrupo que podamos sin que el cociente deje de ser abeliano, es decir, el subgrupo derivado del grupo anterior.

Definimos el *derivado* i-simo $G^{i)}$ de un grupo G mediante

$$G^{0)} = G, \qquad G^{i+1)} = \left(G^{i)}\right)'.$$

Claramente, todos estos subgrupos son característicos en G. Si existe un número n tal que $G^{n)} = 1$ entonces la serie derivada

$$1 = G^{n)} \quad \trianglelefteq \quad \cdots \quad \trianglelefteq \quad G^{1)} \quad \trianglelefteq \quad G^{0)} \quad = \quad G.$$

es abeliana, luego G es resoluble. Recíprocamente, si G es resoluble y

$$1 = H_n \quad \trianglelefteq \quad \cdots \quad \trianglelefteq \quad H_1 \quad \trianglelefteq \quad H_0 = G$$

es una serie abeliana de G, aplicando repetidamente el teorema 1.43 obtenemos que $G^{i)} \leq H_i$ para $i = 1, \ldots, n$. En efecto, si vale para i, como H_i/H_{i+1} es abeliano tenemos que $G^{i+1)} = \left(G^{i)}\right)' \leq H_i' \leq H_{i+1}$.

Así concluimos que $G^{n)} = 1$ y que la longitud de la serie derivada es menor o igual que la longitud de la serie dada. Así pues:

Teorema 4.6 *Un grupo G es resoluble si y sólo si existe un n tal que $G^{n)} = 1$, y en tal caso la serie derivada tiene longitud menor o igual que cualquier otra serie abeliana de G.*

Grupos infinitos El concepto de resolubilidad se aplica igualmente a grupos infinitos. De hecho, observemos que las propiedades del teorema 4.3 no requieren la hipótesis de que los grupos considerados sean finitos. Usando dichas propiedades es fácil probar lo siguiente:

Teorema 4.7 *Todo grupo libre de rango ≥ 2 no es resoluble.*

Demostración: Todo grupo libre de rango ≥ 2 tiene un subgrupo libre de rango 2 (el generado por dos elementos de una base), luego basta probar que los grupos libres de rango 2 no son resolubles, pero por el teorema 3.14 tenemos que un grupo libre de rango 2 tiene un subgrupo de rango numerable, luego basta probar que los grupos libres de rango numerable no son resolubles, pero la prueba del teorema 3.15 muestra que todo grupo finito es cociente de un grupo libre de rango numerable, luego si los grupos libres de rango numerable fueran resolubles, todo grupo finito lo sería. ∎

Veamos finalmente un ejemplo de grupo resoluble no abeliano infinito:

Ejemplo: Las isometrías de un espacio euclídeo De acuerdo con la discusión tras [G 5.17], si E es un espacio afín euclídeo (sobre el cuerpo $\mathbb{R}$ de los números reales), tenemos un epimorfismo $\mathrm{Is}(E) \longrightarrow \mathrm{O}(\vec{E})$ del grupo de las isometrías de E en el grupo de las isometrías lineales de $\vec{E}$, cuyo núcleo es el subgrupo $G_1 = \mathrm{T}(E) \cong \vec{E}$ de las traslaciones de E.

Por otra parte, $\mathrm{O}(\vec{E}) \cong \mathrm{O}(n,\mathbb{R})$, el grupo de las matrices ortogonales $n \times n$. Según [G 5.33], la aplicación determinante induce un epimorfismo de grupos $\mathrm{O}(n,\mathbb{R}) \longrightarrow \{\pm 1\}$ cuyo núcleo es el grupo $\mathrm{O}^+(n,\mathbb{R})$ de las matrices ortogonales de determinante 1 que es isomorfo al grupo de las isometrías lineales directas. Así obtenemos una serie

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq G_3 = \mathrm{Is}(E)$$

donde

$$G_1/G_0 \cong \mathbb{R}^n, \quad G_2/G_1 \cong \mathrm{O}^+(n,\mathbb{R}), \quad G_3/G_2 \cong C_2.$$

El primer y el último factor son abelianos. En la clasificación de las isometrías de la recta, el plano y el espacio (tridimensional) euclídeo que hemos presentado en la sección [G 5.5] hemos visto que

$$\mathrm{O}^+(1,\mathbb{R}) = 1, \qquad \mathrm{O}^+(2,\mathbb{R}) \cong \mathbb{R}/\langle 2\pi \rangle$$

son grupos abelianos, por lo que los grupos de isometrías de la recta y del plano son resolubles. En cambio, el grupo $\mathrm{O}^+(3,\mathbb{R})$ es isomorfo al grupo $\mathrm{Is}^+_O(E)$ de los giros respecto de ejes que pasan por un punto O, y es un grupo no abeliano. De hecho, no es resoluble. Esto es consecuencia de que contiene un subgrupo libre de rango 2, según hemos visto en el ejemplo de la página 93 (nótese la nota al pie, que señala que las matrices consideradas son giros, luego el grupo libre construido es isomorfo a un subgrupo de $\mathrm{Is}^+_O(E)$) o, alternativamente, también es consecuencia de que $\mathrm{Is}^+_O(E)$ contiene un subgrupo isomorfo a A_5 (el grupo de las simetrías directas de un icosaedro, según hemos visto en la sección 2.6). ∎

4.2 El teorema de Frobenius

Vamos a probar un resultado del que deduciremos una condición suficiente muy sencilla para que un grupo sea resoluble.

Teorema 4.8 (Frobenius) *Si G es un grupo finito y $d \mid |G|$, entonces el número de soluciones en G de la ecuación $x^d = 1$ es múltiplo de d.*

Definimos $G[d] = \{x \in G \mid x^d = 1\}$, de modo que el teorema de Frobenius afirma que $d \mid |G[d]|$.

Nota Frobenius conjeturó que, siempre bajo la hipótesis de que $d \mid |G|$, si $|G[d]| = d$, entonces $G[d] \trianglelefteq G$. Esta conjetura se ha demostrado usando la clasificación de los grupos simples finitos. ∎

Necesitamos un resultado técnico:

Teorema 4.9 *Si G es un grupo finito y n es cualquier número natural, el número de elementos de G de orden n es divisible entre $\phi(n)$. Si $d \mid |G|$, $d = p^k m$, con $p \nmid m$ y $p^{k+1} \mid |G|$, entonces $|G[dp] \setminus G[d]|$ es múltiplo de $\phi(p^{k+1})$.*

DEMOSTRACIÓN: Consideremos en G la relación de equivalencia dada por $x \sim y$ si y sólo si $\langle x\rangle = \langle y\rangle$. En virtud del teorema 1.16, un grupo cíclico de orden n tiene $\phi(n)$ generadores, luego la clase de equivalencia de un $x \in G$ tiene $\phi(o(x))$ elementos. Como dos elementos relacionados tienen el mismo orden, el conjunto de todos los elementos de G de orden n es unión de clases de equivalencia de cardinal $\phi(n)$, luego su cardinal es múltiplo de $\phi(n)$.

Ahora observamos que $G[dp]\setminus G[d] = \{x \in G \mid o(x) = p^{k+1}s,\ s \mid m\}$. Si es un conjunto no vacío, es unión de clases de equivalencia y, por la parte ya probada, la clase de equivalencia de un x con $o(x) = p^{k+1}s$ tiene cardinal múltiplo de $\phi(p^{k+1})\phi(s)$, luego todas las clases de equivalencia tienen cardinal múltiplo de $\phi(p^{k+1})$, luego $G[dp] \setminus G[d]$ también. ∎

DEMOSTRACIÓN (del teorema de Frobenius): Si el teorema fuera falso, podríamos tomar un grupo G del menor orden posible que no lo cumpliera. Notemos que $|G| > 1$, pues $G = 1$ cumple trivialmente el teorema. Por otro lado, si $d = |G|$ entonces $G[d] = G$ y el teorema se cumple trivialmente, luego el mayor $d \mid |G|$ que incumple el teorema es $d < |G|$.

Así pues, $|G|/d \neq 1$, luego podemos tomar un primo p que divida a $|G|/d$. Digamos que $d = p^k m$, donde $p \nmid m$ y así $p^{k+1} \mid |G|$. Sea $A = G[dp]\setminus G[d]$. Por la maximalidad de d tenemos que $pd \mid |G[dp]|$. Obviamente, $|G[dp]| = |G[d]| + |A|$, luego si probamos que $d \mid |A|$, tendremos que $d \mid |G[d]|$ en contradicción con la elección de d. Esto sucede trivialmente si $A = \varnothing$, luego podemos suponer lo contrario. Por el teorema anterior $\phi(p^{k+1}) = (p-1)p^k \mid |A|$, luego basta probar que $m \mid |A|$.

Según hemos visto en la demostración del teorema anterior, todo $x \in A$ cumple que $o(x) = p^{k+1}s$, con $s \mid m$. Tomamos enteros tales que $up^{k+1} + vs = 1$, con lo que $y = x^{vs}$, $z = x^{up^{k+1}}$ cumplen que $x = yz = zy$, $o(y) = p^{k+1}$, $o(z) = m$ (en principio $o(y) \mid p^{k+1}$, $o(z) \mid m$, pero $o(x) = o(y)o(z)$, luego tienen que darse las igualdades).

Para cada $a \in G$ tal que $o(a) = p^{k+1}$, definimos

$$S_a = \{ab \mid b \in C_G(a),\ b^m = 1\}.$$

Así, acabamos de probar que A es la unión de todos los conjuntos S_a. Vamos a ver que la unión es disjunta. Para ello tomamos dos elementos $a_1, a_2 \in G$ de orden p^{k+1} y supongamos que hay un elemento en $S_{a_1} \cap S_{a_2}$, que será de la forma $a_1b_1 = a_2b_2$, con $b_i \in C_G(a_i)$, $b_i^m = 1$. Entonces, como a_i y b_i conmutan,

$$a_1^m = (a_1b_1)^m = (a_2b_2)^m = a_2^m,$$

y elevando al inverso de m módulo p^{k+1} llegamos a que $a_1 = a_2$, luego, en efecto, la unión es disjunta.

Ahora observamos que si $g \in G$, entonces $(S_a)^g = S_{a^g}$, pues $(ab)^g = a^g b^g$, donde $b^g \in C_G(a^g)$ y $(b^g)^m = 1$, luego, si llamamos S_a^* a la unión de todos los conjuntos S_{a^g}, tenemos que $|S_a^*| = |\mathrm{cl}(a)||S_a|$ y $|A|$ es la suma de un número finito de cardinales $|S_a^*|$. Si probamos que $m \mid |S_a^*|$, tendremos que $m \mid |A|$, como queremos probar.

Sea $G^* = C_G(a)/\langle a\rangle$. Sea $r = |G^*| < |G|$ y $e = (m, r)$. Entonces, la aplicación

$$S_a \longrightarrow \{x \in G^* \mid x^m = 1\} = \{x \in G^* \mid x^e = 1\} = G^*[e].$$

dada por $ab \mapsto b\langle a\rangle$ es biyectiva. En efecto:

Si $b\langle a\rangle = b'\langle a\rangle$ es que $b' = a^i b$, luego $b'^{p^{k+1}} = b^{p^{k+1}}$ y elevando al inverso de p^{k+1} módulo m resulta que $b' = b$, lo que prueba la inyectividad.

Si $x = u\langle a\rangle \in G^*$ cumple $x^m = 1$, como $\langle a\rangle = \langle a^m\rangle$, tenemos que $u^m = a^{mi}$, para cierto i, luego $(ba^{-i})^m = 1$, luego $b = ba^{-i}$ cumple que $x = b\langle a\rangle$ y $b^m = 1$, luego x es la imagen de $ab \in S_a$ y la aplicación es suprayectiva.

Por la minimalidad de G, tenemos que $e \mid |G^*[e]| = |S_a|$, luego

$$|S_a^*| = |\mathrm{cl}(a)||S_a| = |G : C_G(a)||S_a| = \frac{|G||S_a|}{|C_G(a) : \langle a\rangle \,|\, p^{k+1}} = \frac{|G|}{(r/e)p^{k+1}}\frac{|S_a|}{e}.$$

Ahora bien, $mr/e = \mathrm{mcm}(r, m)$ y, tanto r como m dividen a $|G|$, luego $mr/e \mid |G|$, luego $m \mid |G|/(r/e)$, pero $p^{k+1} \mid |G|$ y, como $(m, p^{k+1}) = 1$, de hecho

$$m \mid \frac{|G|}{(r/e)p^{k+1}} \mid |S_a^*|.$$

∎

Como consecuencia:

Teorema 4.10 *Sea G un grupo finito y sea q el mayor primo que divide a su orden. Si todos los subgrupos de Sylow de G son cíclicos, entonces G tiene un único q-subgrupo de Sylow (normal).*

Demostración: Sea $|G| = p_1^{e_1} \cdots p_r^{e_r}$, con $p_1 < p_2 < \cdots < p_r = q$ y vamos a considerar los números de la forma $d = p_s^{f_s} p_{s+1}^{e_{s+1}} \cdots p_r^{e_r}$, con $0 \le f_s \le e_s$. Vamos a demostrar que cualquier d de esta forma cumple $|G[d]| = d$. En caso contrario, sea d el mayor divisor de $|G|$ de esta forma para el que no sea cierto. No puede ser $d = |G|$, pues entonces la igualdad se da trivialmente, luego $d < |G|$.

Sea p el mayor primo que divida a $|G|/d$ y sea $A = G[dp] - G[d]$. Como los p-subgrupos de Sylow son cíclicos, si $d = p^k m$, donde $p \nmid m$, en G existen elementos de orden p^{k+1}, y cualquiera de ellos está en A, luego $A \neq \varnothing$.

Por la maximalidad de d tenemos que $|G[dp]| = dp$, y por el teorema de Frobenius sabemos que $|G[d]| = du$, para cierto $1 \le u < p$ (pues $G[d] \subsetneq G[dp]$). Por el teorema 4.9 sabemos que $(p-1)p^k = \phi(p^{k+1}) \mid |A| = d(p-u)$.

Pero, por la forma de d y la elección de p, todo divisor primo de d es mayor o igual que p, luego $p - 1$ es primo con d, luego $p - 1 \mid p - u$, lo cual sólo es posible si $u = 1$, luego $|G[d]| = d$, en contra de lo supuesto.

En particular hemos probado que $|G[q^{e_r}]| = q^{e_r}$. Esto significa que hay exactamente q^{e_r} elementos $x \in G$ que cumplen $x^{q^{e_r}} = 1$, pero eso tienen que cumplirlo los q^{e_r} elementos de un q-subgrupo de Sylow de G, luego sólo puede haber uno, que será normal. ∎

Finalmente observamos que este teorema puede aplicarse sucesivamente: si G_1 es el q-subgrupo de Sylow normal, entonces G/G_1 tiene subgrupos de Sylow cíclicos, luego uno de ellos, digamos G_2/G_1 es normal, y podemos continuar hasta que $G/G_n = 1$, con lo que obtenemos una serie cíclica para G. En definitiva:

Teorema 4.11 *Todo grupo finito con subgrupos de Sylow cíclicos (en particular, todo grupo de orden libre de cuadrados) es resoluble.*

4.3 Subgrupos de Hall

Vamos a ver ahora que los grupos resolubles satisfacen una generalización de la teoría de Sylow.

Definición 4.12 Si G es un grupo finito, un *subgrupo de Hall* es un subgrupo $H \leq G$ tal que $|H|$ y $|G : H|$ son primos entre sí.

Si π es un conjunto de primos, un *π-subgrupo* (resp. un *π'-subgrupo*) de G es un subgrupo cuyo orden es divisible únicamente entre primos de π (resp. no es divisible entre primos de π), y es un *π-subgrupo de Hall* (resp. π'-subgrupo de Hall) si además su índice no es divisible entre primos de π (resp. sólo es divisible entre primos de π).

Así, si dividimos los primos que dividen a $|G|$ en dos conjuntos disjuntos π y ρ, entonces los π-subgrupos (de Hall) de G coinciden con sus ρ'-subgrupos (de Hall).

Claramente, todo π-subgrupo (resp. π'-subgrupo) de Hall de un grupo G es un subgrupo de Hall, y todo subgrupo de Hall es un π-subgrupo de Hall (resp. un π'-subgrupo de Hall), donde π es el conjunto de primos que dividen a su orden (resp. el conjunto de primos que dividen a $|G : H|$).

Obviamente los p-subgrupos de Sylow son $\{p\}$-subgrupos de Hall. Los p'-subgrupos de Hall se llaman también *p-complementos* de un grupo.

Observemos que se cumple el teorema análogo a 3.31:

Teorema 4.13 *Si G es un grupo finito, $N \trianglelefteq G$ y H es un π-subgrupo de Hall de G, entonces $H \cap N$ es un π-subgrupo de Hall de N y HN/N es un π-subgrupo de Hall de G/N.*

Demostración: Si $p \in \pi$, entonces un p-subgrupo de Sylow P de H lo es también de G y, como $H \cap N \trianglelefteq H$, por 3.31 tenemos que $P \cap N = P \cap (H \cap N)$ es un p-subgrupo de Sylow de N y de $H \cap N$, luego p divide a $|H \cap N|$ y a $|N|$ con el mismo exponente. Por el contrario, si $p \notin \pi$, entonces $p \nmid |H|$, luego $p \nmid |H \cap N|$. Esto prueba que $H \cap N$ es un π-subgrupo de Hall de N.

Similarmente, si $p \in \pi$ tenemos que PN/N es un p-subgrupo de Sylow de G/N, luego también de HN/N, luego p divide a los órdenes de ambos grupos con el mismo exponente, mientras que si $p \notin \pi$, entonces p no divide al orden $|HN/N| = |H : H \cap N|$, luego HN/N es un π-subgrupo de Hall de G/N. ∎

Un grupo arbitrario no tiene por qué tener π-subgrupos de Hall. Por ejemplo, $|A_5| = 60$, pero no tiene $\{3,5\}$-subgrupos de Hall, ni $\{2,5\}$-subgrupos de Hall, pues serían subgrupos de orden 15 o 20, luego tendrían índice 4 o 3, pero A_5 es simple y el teorema 2.29 afirma que no puede tener tales subgrupos. Sin embargo, la existencia de subgrupos de Hall está asegurada en los grupos resolubles:

Teorema 4.14 (Hall) *Sea G un grupo finito resoluble y π un conjunto de primos que dividen a $|G|$, entonces:*

1. *G tiene π-subgrupos de Hall.*
2. *Dos π-subgrupos de Hall cualesquiera son conjugados.*
3. *Todo π-subgrupo de G está contenido en un π-subgrupo de Hall.*

Observemos que A_5 no tiene subgrupos[1] de orden 15 o 20, es decir, que no tiene $\{3,5\}$-subgrupos de Hall ni $\{2,5\}$-subgrupos de Hall, por lo que vemos que la hipótesis de resolubilidad es necesaria.

Para probar el teorema de Hall necesitamos un resultado previo. Nos bastaría con su particularización al caso de grupos resolubles, pero es interesante demostrarlo en general:

Grupos característicamente simples Un grupo G es *característicamente simple* si sus únicos subgrupos característicos son 1 y G.

Si G es un grupo, un subgrupo *normal minimal* de G es un subgrupo $N \trianglelefteq G$ no trivial que no contiene subgrupos propios normales en G.

Como todo subgrupo característico de N es normal en G, es inmediato que los subgrupos normales minimales de un grupo G son característicamente simples.

El teorema que necesitamos es el siguiente:

Teorema 4.15 *Un grupo finito G es característicamente simple si y sólo si es producto directo de un número finito de grupos simples isomorfos entre sí.*

En particular, si el grupo es resoluble, los subgrupos simples tienen que ser también resolubles, luego tienen que ser cíclicos de orden primo, luego los grupos

[1] En general, un grupo simple no abeliano G no puede tener un subgrupo H de índice $n = 2, 3, 4$, pues en tal caso el teorema de Cayley nos daría un homomorfismo $G \longrightarrow \Sigma_n$ que tendría que ser inyectivo, por la simplicidad de G, pero Σ_n es resoluble y no posee subgrupos simples no abelianos.

característicamente simples resolubles son los de la forma $C_p \times \cdots \times C_p$. Estos grupos se llaman *grupos abelianos elementales.*

DEMOSTRACIÓN: Supongamos en primer lugar que $G = H_1 \times \cdots \times H_n$, donde los grupos H_i son simples e isomorfos entre sí. Tenemos que probar que G es característicamente simple. Si los grupos H_i son abelianos (es decir, cíclicos de orden primo p), la conclusión es muy sencilla. Podemos ver a G como un espacio vectorial de dimensión n sobre el cuerpo $k = \mathbb{Z}/p\mathbb{Z}$, de modo que los subgrupos de G coinciden con sus subespacios vectoriales.

Si $V \leq G$ es un subgrupo / subespacio vectorial distinto de 0 o de G, tendrá una base $v_1, \ldots, v_d$, con $1 \leq d < n$ y, tomando $w_d \in G \setminus V$, podemos completar dos bases de G de la forma $v_1, \ldots, v_d, v_{d+1}, \ldots, v_n$ y $v_1, \ldots, v_{d-1}, w_d, \ldots, w_n$, a partir de las cuales podemos definir $\alpha \in Aut(G)$ (notemos que los automorfismos como grupo coinciden con los automorfismos como espacio vectorial) que transforme una base en otra, y así $\alpha[V] \neq V$, pues $w_d \in \alpha[V] \setminus V$. Esto prueba que V no es característico y que G es característicamente simple.

Consideremos ahora el caso en que los grupos H_i son simples no abelianos. Si $1 < N \lhd G$ es un subgrupo normal propio de G, no puede ser que $N \cap H_i = 1$ para todo i, pues entonces N conmutaría con todos los H_i elemento a elemento (teorema 3.1) y $N \leq Z(G) = Z(H_1) \times \cdots \times Z(H_n) = 1$.

Así pues, existe un i tal que $N \cap H_i \neq 1$, pero la intersección es normal en H_i, que es simple, luego tiene que ser $N \cap H_i = H_i$, es decir, $H_i \leq N$. Pero N no puede contener a todos los H_i, ya que entonces sería $N = G$, luego existe un índice j tal que $H_j \cap N = 1$. No perdemos generalidad si suponemos que $i = 1$ y $j = 2$.

A partir de un isomorfismo $\alpha : H_1 \longrightarrow H_2$ podemos definir un automorfismo $\bar{\alpha} : G \longrightarrow G$ dado por

$$\bar{\alpha}(h_1, \ldots, h_n) = (\alpha^{-1}(h_2), \alpha(h_1), h_3, \ldots, h_n).$$

Así $\bar{\alpha}[H_1] = H_2$, luego $\bar{\alpha}[N] \neq N$, lo que prueba que N no es característico en G.

Para probar el recíproco observemos en primer lugar que si N y M son subgrupos normales de un grupo G y N es minimal, entonces $N \trianglelefteq M$ o bien $NM = N \times M$.

En efecto, se cumple que $N \cap M \trianglelefteq G$ y $N \cap M \leq N$, luego la minimalidad de N obliga a que $N \cap M = N$ (en cuyo caso $N \trianglelefteq M$) o bien $N \cap M = 1$, en cuyo caso el producto de M y N es directo.

Supongamos ahora que G es característicamente simple y sea H_1 un subgrupo normal minimal de G (notemos que la definición no excluye la posibilidad $H_1 = G$).

Para cada $\alpha \in \mathrm{Aut}(G)$, tenemos que $\alpha[H_1]$ es también un subgrupo normal minimal de G, luego, por la observación precedente, o bien $\alpha[H_1] \leq H_1$, o bien $H_1\alpha[H_1] = H_1 \times \alpha[H_1]$.

Si hay un automorfismo α para el que se dé el segundo caso, llamamos $H_2 = \alpha[H_1]$ y $L_2 = H_1 \times H_2 \trianglelefteq G$. Nuevamente, para cada $\alpha \in \mathrm{Aut}(G)$, tenemos que $\alpha[H_1] \leq L_2$ o bien $L_2\alpha[H_1[= L_2 \times \alpha[H_1]$. Si hay un α para el que se da el segundo caso, llamamos $T_3 = \alpha[T_1]$ y $L_3 = H_1 \times H_2 \times H_3 \trianglelefteq G$.

Tras un número finito de pasos tenemos que llegar a un subgrupo

$$L = H_1 \times \cdots \times H_n \trianglelefteq G,$$

donde todos los factores son de la forma $H_i = \alpha_i[H_1]$, para cierto $\alpha_i \in \mathrm{Aut}(G)$ y, para todo $\alpha \in \mathrm{Aut}(G)$, se cumple que $\alpha[H_1] \leq L$. Más aún, se cumple que $\alpha[H_i] = (\alpha_i\alpha)[H_1] \leq L$, y esto implica que $\alpha[L] \leq L$, luego, al ser un conjunto finito, $\alpha[L] = L$. Así pues, L es un subgrupo característico de G, luego tiene que ser

$$G = L = H_1 \times \cdots \times H_n.$$

Finalmente, H_1 tiene que ser simple, pues si tuviera un subgrupo normal propio $K \trianglelefteq H_1$, como H_1 conmuta con los demás H_i, se cumpliría que $K \trianglelefteq G$, pero H_1 es normal minimal en G y tenemos una contradicción. ∎

En particular:

Teorema 4.16 *Si N es un subgrupo normal minimal de un grupo finito G, entonces N es producto directo de grupos simples conjugados en G.*

Nota Conviene observar que este caso podemos decir un poco más: los factores son conjugados en G. La razón es que, al aplicar a N el argumento que prueba el teorema precedente, es decir, partiendo de un subgrupo normal minimal H_1 de N, podemos razonar únicamente con automorfismos $\alpha \in \mathrm{Aut}(N)$ de la forma $\alpha(n) = n^g$, para $g \in G$, de modo que llegamos a un producto

$$L = H_1 \times \cdots \times H_n \trianglelefteq N$$

en el que $H_i = H_1^{g_i}$, para cierto $g_i \in G$ y de modo que, para todo $g \in G$, se cumple que $H_1^g \leq L$, de donde se sigue como antes que $H_i^g \leq L$, luego $L^g = L$ y así $L \trianglelefteq G$, pero, como N es normal minimal, tiene que ser $N = L$, e igualmente se concluye que los H_i son simples. ∎

En particular, si el grupo G es resoluble, los únicos subgrupos simples que puede tener son abelianos, es decir, isomorfos a C_p, para un primo p. Los grupos de la forma $C_p \times \cdots \times C_p$ se llaman *grupos abelianos elementales.* Así pues:

Teorema 4.17 *Los subgrupos normales minimales de un grupo finito resoluble son elementales abelianos.*

Con esto ya podemos probar el resultado principal:

Demostración (del teorema de Hall): Razonamos por inducción sobre el orden de G, es decir, suponemos que el teorema es válido para grupos de orden menor que $|G|$ y vamos a probarlo para G.

Sea π un conjunto de primos que dividen a $|G|$, de modo que podemos descomponer $|G| = ab$, donde a es divisible sólo entre primos de π y b sólo entre primos que no están en π. Tenemos que probar que G tiene subgrupos de orden a y que dos cualesquiera de ellos son conjugados.

Sea H un subgrupo normal minimal de G. Por el teorema anterior es un p-grupo abeliano elemental. Pongamos que $|H| = p^m$.

Supongamos en primer lugar que $p^m \mid a$. Por hipótesis de inducción G/H tiene un π-subgrupo de Hall A/H, y entonces es claro que A es un π-subgrupo de Hall de G. Además, si A^* es otro π-subgrupo de Hall, entonces $H \leq A^*$, pues en caso contrario HA^* sería un π-subgrupo de G de orden mayor que A^*, lo cual es imposible. A su vez, esto implica que A^*/H es un π-subgrupo de Hall de G/H, luego por hipótesis de inducción A/H y A^*/H son conjugados, pero esto implica que A y A^* son conjugados también.

Si A^* es un π-subgrupo de G, para probar que está contenido en un π-subgrupo de Hall podemos sustituirlo por A^*H, que también es un π-subgrupo, y así podemos suponer que $H \leq A^*$, con lo que A^*/H es un π-subgrupo de G/H, que por hipótesis de inducción está contenido en un π-subgrupo de Hall A/H, con lo que A^* está contenido en el π-subgrupo de Hall A de G.

Supongamos ahora que $p^m \mid b$, pero que $p^m < b$. Entonces, por hipótesis de inducción, G/H tiene un π-subgrupo de Hall B/H, es decir, un subgrupo de orden a, pero esto significa que $|B| = ap^m$. Como $p^m < b$, se cumple que $|B| < |G|$, luego podemos aplicar de nuevo la hipótesis de inducción para encontrar en B un π-subgrupo de Hall A, que obviamente es también un π-subgrupo de Hall de G.

Si A^* es otro π-subgrupo de Hall de G, entonces A^*H/H es un π-subgrupo de Hall de G/H, luego por hipótesis de inducción es conjugado con B/H. Como en el caso anterior concluimos que A^*H es conjugado con B, luego A^* es conjugado con un subgrupo B^* de B (que será un π-subgrupo de Hall), pero por hipótesis de inducción dos π-subgrupos de Hall de B son conjugados, luego B^* es conjugado con A, luego también A^* es conjugado con A.

Si A^* es un π-subgrupo de G, entonces A^*H/H es un π-subgrupo de G/H, luego por hipótesis de inducción está contenido en un π-subgrupo de Hall B/H de G/H, luego $A^* \leq B$, luego por hipótesis de inducción A^* está contenido en un π-subgrupo de Hall de B, que es también un π-subgrupo de Hall de G.

Por último, suponemos que $p^m = b$. Entonces H es un p-subgrupo de Sylow de G, y es normal, luego es único. Podemos suponer además que H es el único subgrupo normal minimal de G, pues si hubiera otro, no podría tener orden p^m (ya que H es el único subgrupo de ese orden), luego estaría en el primer caso y eso probaría el teorema para G.

Sea K/H un subgrupo normal minimal de G/H, que tiene que ser un q-grupo abeliano elemental. Pongamos que $|K| = p^m q^n$. Sea $Q \leq K$ un q-subgrupo de Sylow. Entonces $K = QH$ y $Q \cap H = 1$. Vamos a probar que el normalizador $N_G(Q)$ es un π-subgrupo de Hall de G.

Por el argumento de Frattini 3.37, tenemos que $G = KN_G(Q)$, pero

$$G = KN_G(Q) = HQN_G(Q) = HN_G(Q),$$

luego basta probar que $H \cap N_G(Q) = 1$, ya que entonces $|N_G(Q)| = |G : H| = a$.

Para ello probamos en primer lugar que $H \cap N_G(Q) \leq Z(K)$ y luego veremos que el centro es trivial.

En efecto, si $z \in H \cap N_G(Q)$, como H es abeliano, z conmuta con todos los elementos de H. Como $K = HQ$, basta probar que z conmuta con todo $x \in Q$. Ahora bien,

$$[x, z] = x^{-1}(z^{-1}xz) = (x^{-1}z^{-1}x)z \in Q \cap H = 1.$$

Ahora, $Z(K)$ es característico en K, luego $Z(K) \trianglelefteq G$. Si $Z(K) \neq 1$, contendría un subgrupo normal minimal de G, pero estamos suponiendo que el único es H.

Así pues, sería $H \leq Z(K)$, luego $Q \trianglelefteq K$, pero entonces Q sería el único q-subgrupo de Sylow de K, luego sería característico en K, luego $Q \trianglelefteq G$, luego Q contendría un subgrupo normal minimal de G, que no podría ser H, en contradicción con que H es el único.

Veamos que si A es otro π-subgrupo de Hall, entonces A es conjugado con $N_G(Q)$. Como $|AK|$ es divisible entre a y entre $p^m = b$, tiene que ser $G = AK$. Por el teorema de isomorfía:

$$p^m = |G : A| = |K : A \cap K|,$$

luego $|A \cap K| = q^n$, luego $A \cap K$ es un q-subgrupo de Sylow de K, luego es conjugado con Q, luego $N_G(A \cap K)$ es conjugado con $N_G(Q)$, que es un π-subgrupo de Hall, luego tiene índice p^m, pero A normaliza a $A \cap K$ y tiene índice p^m, luego tiene que ser $A = N_G(A \cap K)$ y tenemos que A es conjugado con $N_G(Q)$.

Sea ahora A un π-subgrupo de G, de modo que $|A| \mid a$ y $|H| = p^m$, luego $A \cap H = 1$, luego $|AH| = |A|p^m$.

Como $G = HN_G(Q)$, también $G = N_G(Q)(AH)$, luego

$$ap^m = |G| = \frac{|N_G(Q)AH|}{|N_G(Q) \cap AH|} = \frac{a|A|p^m}{|N_G(Q) \cap AH|},$$

luego $B = N_G(Q) \cap AH$ tiene orden $|B| = |A|$. Esto implica que A y B son π-subgrupos de Hall de AH, luego son conjugados. Así, $A = B^g \leq N_G(Q)^g$, y el último grupo es un π-subgrupo de Hall de G. ∎

Recíprocamente, si un grupo tiene p-complementos, para todos los primos que dividen a su orden, entonces es resoluble. En la prueba usaremos el teorema 6.40 de Burnside, que afirma que todo grupo de orden $p^a q^b$ es resoluble. Necesitamos también dos hechos sencillos:

Teorema 4.18 *Todo grupo finito resoluble no trivial contiene un p-subgrupo característico no trivial, para cierto primo p.*

DEMOSTRACIÓN: Sea G un grupo finito resoluble y su serie derivada termina en $G^{n)} = 1$, entonces $G^{n-1)}$ es un subgrupo característico abeliano no trivial, luego tiene un p-subgrupo de Sylow $P \trianglelefteq G^{n-1)}$ y, al ser el único p-subgrupo de Sylow de $G^{n-1)}$, será característico en $G^{n-1)}$, luego también en G. ∎

Teorema 4.19 *Sea $|G| = p_1^{e_1} \cdots p_r^{e_r}$ y sean $H, K \leq G$ tales que cada $p_i^{e_i}$ divide a $|H|$ o a $|K|$. Entonces $G = HK$ y $|H \cap K| = (|H|, |K|)$.*

DEMOSTRACIÓN: Se cumple que $|HK||H \cap K| = |H||K|$. Si $p_i^{e_i}$ divide sólo a $|H|$ o sólo a $|K|$, entonces no divide a $|H \cap K|$, luego tiene que dividir a $|HK|$. Si divide a los órdenes de ambos subgrupos, entonces $p_i^{2e_i} \mid |HK||H \cap K|$, pero p_i sólo divide a $|H \cap K|$ con exponente e_i, luego igualmente $p_i^{e_i} \mid |HK|$. Esto implica que $|G| \mid |HK|$, luego tiene que ser $G = HK$.

Además, $|H \cap K|$ es divisible exactamente entre las potencias $p_i^{e_i}$ que dividen a los órdenes de ambos subgrupos, de donde se sigue la segunda afirmación del enunciado. ∎

Teorema 4.20 *Si un grupo finito G posee p-complementos para todos los primos que dividen a su orden, entonces es resoluble.*

DEMOSTRACIÓN: Si el resultado es falso, sea G un contraejemplo del menor orden posible. Pongamos que $|G| = p_1^{e_1} \cdots p_r^{e_r}$ y sea H_i un p_i-complemento de G, es decir, un subgrupo tal que $|G : H_i| = p_i^{e_i}$. No puede ser $r \leq 2$, pues entonces G sería resoluble por el teorema de Burnside 6.40. Así pues, $r \geq 3$.

Fijado un índice i, para todo $j \neq i$ tenemos que H_i y H_j están en las hipótesis del teorema anterior, luego $|H_i \cap H_j|$ es el producto de todos los $p_k^{e_k}$ con $k \neq i, j$ y en particular $|H_i : H_i \cap H_j| = p_j^{e_j}$. Esto significa que cada H_i satisface las hipótesis del teorema, luego, por la minimalidad de G, todos los H_i son resolubles.

Por 4.18 podemos tomar un subgrupo $P \trianglelefteq H_1$ de orden $|P| = p_i^e$, para cierto $i > 1$. Reordenando los primos (y teniendo en cuenta que $r \geq 3$) podemos suponer que $|P| = p_3^e$. Entonces $|H_1 \cap H_2| = p_3^{e_3} \cdots p_r^{e_r}$, luego $H_1 \cap H_2$ contiene un p_3-subgrupo de Sylow de H_1 y, como $P \trianglelefteq H_1$, está contenido todos ellos, luego $P \leq H_1 \cap H_2$. Además, por el teorema anterior $G = H_2H_1$, y esto hace que el núcleo normal de H_2 en G sea

$$\mathrm{nn}_G(H_2) = \bigcap_{g \in G} H_2^g = \bigcap_{h \in H_1} H_2^h.$$

Por lo tanto, $1 < P \leq \mathrm{nn}_G(H_2) \leq H_2 < G$, luego $N = \mathrm{nn}_G(H_2)$ es un subgrupo normal propio de G, pero el teorema 4.13 nos da que N y G/N satisfacen las hipótesis del teorema (es decir, la existencia de ciertos subgrupos de Hall), luego por la minimalidad de G ambos son resolubles, lo que implica que G también lo es, y tenemos una contradicción. ∎

4.4 El teorema de Schur-Zassenhaus

Probamos ahora un resultado sobre existencia de subgrupos de Hall en grupos no necesariamente resolubles:

Teorema 4.21 *Si G es un grupo finito y $N \trianglelefteq G$ es un subgrupo de Hall normal, existe otro subgrupo de Hall $H \leq G$ tal que $G = NH$ y $N \cap H = 1$. Si N o G/N es resoluble, entonces dos subgrupos H y H' cualesquiera que cumplan lo requerido son conjugados en G.*

Nota El teorema de Feit-Thompson afirma que todo grupo de orden impar es resoluble, por lo que, en las hipótesis del teorema, necesariamente uno de los grupos N o G/N tendrá orden impar, luego será resoluble, lo que significa que la hipótesis de resolubilidad es redundante. ∎

Demostración: Llamemos $Q = G/N$, $n = |N|$, $m = |G/N|$, de modo que $(m, n) = 1$. Vamos a considerar en primer lugar el caso en que N es abeliano. Entonces Q actúa sobre N (como grupo, es decir, en el sentido de 3.19) mediante $a^{gN} = a^g$.

Para cada $x \in Q$, elijamos un representante t_x, de modo que $x = t_x N$. Entonces

$$t_{xy}N = t_x N t_y N = t_x t_y N,$$

luego existe un $c(x, y) \in N$ tal que $t_x t_y = t_{xy} c(x, y)$. La propiedad asociativa $(t_x t_y)t_z = t_x(t_y t_z)$ se traduce en que

$$t_{xy} c(x, y) t_z = t_x t_{yz} c(y, z),$$

luego $t_{xy} t_z c(x, y)^{t_z} = t_x t_{yz} c(y, z)$, o también

$$t_{xyz} c(xy, z) c(x, y)^z = t_{xyz} c(x, yz) c(y, z),$$

luego

$$c(xy, z) c(x, y)^z = c(x, yz) c(y, z).$$

LLamamos

$$d(y) = \prod_{x \in Q} c(x, y) \in N.$$

Teniendo en cuenta que N es abeliano, al multiplicar la igualdad precedente para todos los $x \in Q$ obtenemos

$$d(z) d(y)^z = d(yz) c(y, z)^m.$$

Equivalentemente, $d(yz) = d(y)^z d(z) c(y, z)^{-m}$.

Como $(m, n) = 1$, existen enteros tales que $-1 = km + ln$, y entonces

$$d(y)^{-1} = (d(y)^k)^m,$$

luego llamando $e(y) = d(y)^k$ tenemos que $d(y)^{-1} = e(y)^m$. Aplicando esto a la relación que hemos obtenido resulta

$$e(yz)^{-m} = (e(y)^z e(z)c(y,z))^{-m},$$

de donde se sigue que $e(yz) = e(y)^z e(z)c(y,z)$. (En general, si $a^{-m} = b^{-m}$, con $a, b \in N$, tenemos que $(ab^{-1})^m = 1$, pero, expresando $1 = km + ln$, resulta que $ab^{-1} = (ab^{-1})^{km+ln} = 1$.)

Ahora definimos $\theta : Q \longrightarrow G$ mediante $\theta(x) = t_x e(x)$ y vemos que se trata de un homomorfismo de grupos:

$$\theta(y)\theta(z) = t_y e(y) t_z e(z) = t_y t_z e(y)^z e(z)$$

$$= t_{yz} c(y,z) e(y)^z e(z) = t_{yz} e(yz) = \theta(yz).$$

Más aún, es un monomorfismo, pues si $\theta(x) = 1$, entonces $t_x e(x) = 1$, luego $t_x = e(x)^{-1} \in N$, luego $x = t_x N = 1N$. Esto hace que $H = \theta[Q] \leq G$ sea un subgrupo de orden m, luego necesariamente cumple lo requerido.

Supongamos ahora que H y H^* son dos subgrupos de G de orden m, de modo que $G = NH = NH^*$ con $N \cap H = N \cap H^* = 1$. Tenemos entonces isomorfismos canónicos

$$\pi : G/N = NH/N \longrightarrow H, \qquad \pi^* : G/N = NH^*/N \longrightarrow H^*.$$

Así, todo $x \in G/N$ se expresa como $x = \pi(x)N = \pi^*(x)N$, luego existe $a(x) \in N$ tal que $\pi^*(x) = \pi(x)a(x)$. Tenemos que

$$\pi^*(xy) = \pi^*(x)\pi^*(y) = \pi(x)a(x)\pi(y)a(y) = \pi(x)\pi(y)a(x)^{\pi(y)}a(y)$$

$$= \pi(xy)a(x)^{\pi(y)N}a(y) = \pi(xy)a(x)^y a(y).$$

Por lo tanto, $a(xy) = a(x)^y a(y)$. Llamemos $b = \prod_{x \in Q} a(x) \in N$.

Multiplicando la igualdad que hemos obtenido para todo $x \in Q$ resulta que $b = b^y a(y)^m$. Como $(m,n) = 1$, podemos expresar $b = c^m$, para cierto $c \in N$, con lo que $c^m = (c^y a(y))^m$, luego $c = c^y a(y)$ o, equivalentemente, $a(y) = c^{-y}c$. En consecuencia:

$$\pi^*(y) = \pi(y)a(y) = \pi(y)c^{-y}c = \pi(y)(c^{-1})^{\pi(y)} = c^{-1}\pi(y)c = \pi(y)^c,$$

donde hemos usado que $c^{-y} = (c^{-1})^y = (c^{-1})^{\pi(y)}$. Por lo tanto, $H^* = H^c$.

Esto termina la prueba en el caso en que N es abeliano. En general probamos la existencia de H por inducción sobre $|G|$. Obviamente podemos suponer que $N \neq 1$, luego podemos tomar un primo p tal que $p \mid |N|$. Sea P un p-subgrupo de Sylow de N, sea $L = N_G(P)$, sea $Z = Z(P) \neq 1$ y sea $M = N_G(Z)$. Entonces $L \leq N_G(Z)$, pues Z es característico en P. El argumento de Frattini 3.37 nos da que $G = NL$, luego también $G = MN$.

Sea $N_1 = N \cap M \trianglelefteq M$. Además $|M : N_1| = |G : N| = m$. Aplicamos la hipótesis de inducción al grupo M/Z, que tiene orden menor que $|G|$ y tiene el

subgrupo normal N_1/Z tal que $|M/Z : N_1/Z| = m$, luego existe un subgrupo $H^*/Z \leq M/Z$ tal que $|H^* : Z| = m$, que es primo con $|Z|$. Por el caso abeliano ya demostrado, podemos concluir que H^* tiene un subgrupo H de orden M.

Ahora probamos la conjugación de los subgrupos H bajo el supuesto de que G/N sea resoluble. Si el resultado es falso, podemos tomar un grupo G de orden mínimo que no lo cumpla. Sea π el conjunto de todos los primos que dividen a m y llamemos R al producto de todos los π-subgrupos normales de G, que obviamente es un π-subgrupo normal.

Si $H, K \leq G$ son subgrupos de orden m, entonces RH y RK son π-subgrupos de G, luego necesariamente $RH = H$ y $KH = K$, es decir, $R \leq H \cap K$. Así, $NR/R \trianglelefteq G/R$ es un subgrupo normal de orden n y H/R, K/R son dos π-subgrupos de Hall de G/R, luego si $R \neq 1$, la minimalidad de G implica que H/R y K/R son conjugados en G/R, lo que implica que H y K son conjugados en G.

Por lo tanto, tiene que ser $R = 1$, es decir, que G no tiene π-subgrupos normales no triviales.

Sea L/N un subgrupo normal minimal de G/N. Como el cociente es resoluble, el teorema 4.17 nos da que L/N es un p-grupo, para cierto primo $p \mid m$. Por lo tanto, $H \cap L \cong (H \cap L)N/N \leq L/N$ es un p-grupo y

$$|L : H \cap L| = |HL : L| = n$$

(pues $G = NH = LH$). Por lo tanto $S = H \cap L$ es un p-subgrupo de Sylow de L (en particular $S \neq 1$). Igualmente concluimos que $K \cap L$ es un p-subgrupo de Sylow, luego existe un $g \in G$ tal que $S = (K \cap L)^g = K^g \cap L$. Esto implica que $S \trianglelefteq \langle H, K^g \rangle = J$. No puede ser $J = G$, pues entonces S sería un π-subgrupo normal, luego sería $S = 1$. Por lo tanto, J cumple el teorema, lo que implica que H y K^g son conjugados en J, luego H y K son conjugados en G.

Finalmente probamos la unicidad bajo el supuesto de que N sea resoluble. Si el resultado no fuera cierto, podríamos tomar un grupo G que no lo cumpliera con N (resoluble) del menor orden posible. La resolubilidad de N implica que $N' < N$ y $N' \trianglelefteq G$, porque N' es característico en N. Sean H y K dos subgrupos de G de orden m. El cociente G/N' cumple las hipótesis del teorema con N/N' abeliano y los subgrupos HN'/N', KN'/N', luego por el caso abeliano ya demostrado tenemos que son conjugados, lo cual se traduce en que existe un $g \in G$ tal que $H^g \leq KN'$. Podemos aplicar la hipótesis de minimalidad al grupo $G^* = KN'$, con el subgrupo N', resoluble de orden menor que N y los subgrupos H^g y K, con lo que obtenemos que H^g y K son conjugados en KN', luego H y K son conjugados en G. ∎

4.5 Factores principales y de composición

El contenido de esta sección no tiene que ver realmente con grupos resolubles, sino que se aplica a grupos arbitrarios, pero tiene que ver con el concepto de "serie" cuya relevancia ha puesto de manifiesto el concepto de resolubilidad, y

además muestra mejor cómo encajan los grupos resolubles en el contexto de los grupos arbitrarios.

Recordemos que una serie de un grupo G es una sucesión de subgrupos

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

(que podemos numerar ascendente o descendentemente). La serie es *propia* si cada término es un subgrupo propio del siguiente y es *normal* si cada factor es normal en G. La *longitud* de la serie es el número n de factores G_i/G_{i-1} que determina, es decir, una unidad menos que su número de términos.

Un *refinamiento* de una serie es otra serie que resulta de intercalar más términos entre pares de términos consecutivos.

Una *serie de composición* de un grupo G es una serie propia que no admite ningún refinamiento propio de mayor longitud.

Una *serie principal* de un grupo G es una serie normal propia que no admite ningún refinamiento normal propio de mayor longitud.

Por ejemplo,

$$1 \lhd C_2 \lhd V_4 \lhd A_4 \lhd \Sigma_4$$

es una serie de composición de Σ_4. No es posible refinarla porque todos los factores tienen orden primo, luego no es posible intercalar ninguno más. Un ejemplo de serie normal es

$$1 \lhd V_4 \lhd A_4 \lhd \Sigma_4,$$

pues ahora todos los términos son normales en Σ_4 y no es posible intercalar ningún término más de modo que la serie siga siendo normal, ya que V_4 es un subgrupo normal minimal de Σ_4 (sus tres subgrupos de orden 2 son conjugados entre sí, luego ninguno de ellos es normal en Σ_4).

En general, es claro que una serie propia es de composición si y sólo si sus factores son simples, pues que G_i/G_{i-1} sea simple equivale a que no existan grupos $G_{i-1} \lhd H \lhd G_i$ que permitan refinar la serie. Similarmente, una serie normal propia es principal si y sólo cada factor G_i/G_{i-1} es normal minimal en G/G_{i-1} (lo cual implica que G_i/G_{i-1} es característicamente simple), pues que G_i/G_{i-1} sea normal minimal equivale a que no existan grupos $G_{i-1} \lhd H \lhd G_i$ normales en G que permitan refinar la serie sin perder la normalidad.

Nota Es evidente que todo grupo finito no trivial admite una serie de composición y una serie normal. Sólo tenemos que partir de la serie $1 \lhd G$ y refinarla todo lo posible (con términos normales si queremos llegar a una serie principal). No obstante, los conceptos de serie principal o de composición tienen sentido también para grupos infinitos. Aunque nos va a interesar exclusivamente el caso finito, es fácil adaptar (simplificar, de hecho) los argumentos del teorema 4.3 (eliminando toda referencia a que los factores sean abelianos) para probar que si un grupo tiene serie de composición (principal) lo mismo les sucede a todos sus subgrupos y cocientes, y que, recíprocamente, si N y G/N admiten una serie de composición (principal) lo mismo le sucede a G, etc. ∎

Es claro que un mismo grupo puede tener series de composición distintas, como por ejemplo,

$$1 \lhd C_2 \lhd C_6, \qquad 1 \lhd C_3 \lhd C_6,$$

pero vemos que ambas series tienen dos factores, uno C_2 y otro C_3. En el caso de los grupos resolubles, los factores de una serie de composición son necesariamente grupos simples y resolubles, es decir, cíclicos de orden primo, luego cada $|G_i|$ tiene un único factor primo adicional frente a $|G_{i-1}|$, y esto implica que todas las series de composición de un grupo resoluble G tienen la misma longitud, igual al número de divisores primos de $|G|$ (contando multiplicidades) y, aunque los factores puedan aparecer en un orden diferente en cada una, tiene que haber un factor C_p por cada primo p que divida a $|G|$ (repetido tantas veces como indique la multiplicidad de p en $|G|$).

Lo que no es trivial es que esto mismo vale para grupos arbitrarios, y que también es cierto para series principales. Esto es justamente lo que vamos a demostrar en esta sección. Empezamos demostrando un resultado elemental que resultará útil a menudo:

Teorema 4.22 (Identidad de Dedekind) *Si $A, B, C \leq G$ con $B \leq A$, entonces*

$$A \cap (BC) = B(A \cap C).$$

Demostración: Notemos que el teorema no presupone que BC o $B(A\cap C)$ sean subgrupos de G. Si $a \in A \cap (BC)$, entonces $a = bc$, con $b \in B$ y $c \in C$, luego $b^{-1}a = c \in A\cap C$, pues $B \leq A$, luego $a \in B(A\cap C)$. La inclusión opuesta es trivial. ∎

Teorema 4.23 *Si $B \trianglelefteq A \leq G$ y $C \trianglelefteq G$, entonces $BC \trianglelefteq AC$ y*

$$AC/BC \cong A \,/\, B(A \cap C).$$

Demostración: Claramente $BC \leq AC \leq G$. Si tomamos $bc \in BC$ y $ac' \in AC$, entonces $(bc)^{ac'} = b^{ac'}c^{ac'} = b'^{c'}c''$, donde $b' \in B$, porque $B \trianglelefteq A$ y $c'' \in C$, porque $C \trianglelefteq G$. Es claro entonces que $(bc)^{ac'} \in BC$, luego $BC \trianglelefteq AC$. Por otra parte,

$$AC/BC = A(BC)/BC \cong A \,/\, (BC \cap A) = A \,/\, B(A \cap C),$$

por el teorema anterior. ∎

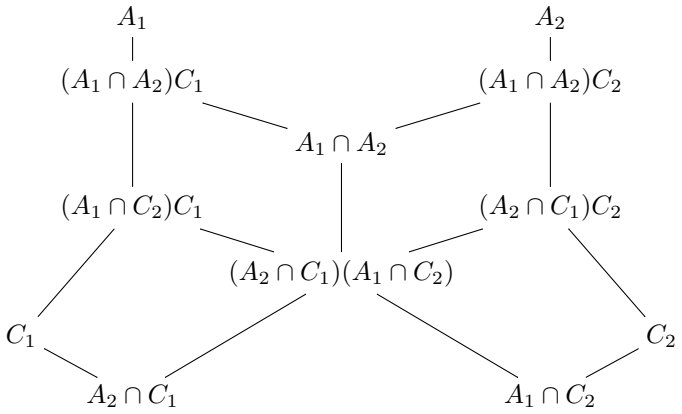
Teorema 4.24 (Lema de Zassenhaus) *Si $C_1 \trianglelefteq A_1 \leq G$ y $C_2 \trianglelefteq A_2 \leq G$, entonces*

$$(A_1 \cap C_2)C_1 \trianglelefteq (A_1 \cap A_2)C_1, \qquad (A_2 \cap C_1)C_2 \trianglelefteq (A_1 \cap A_2)C_2$$

y

$$(A_1 \cap A_2)C_1 \,/\, (A_1 \cap C_2)C_1 \cong (A_1 \cap A_2)C_2 \,/\, (A_2 \cap C_1)C_2.$$

DEMOSTRACIÓN: El esquema siguiente muestra la disposición de los distintos subgrupos que intervienen en la prueba, y hace que este resultado sea conocido también como el "lema de la mariposa":



Tenemos que

$$A_1 \cap C_2 = (A_1 \cap A_2) \cap C_2 \trianglelefteq A_1 \cap A_2,$$

pues $C_2 \trianglelefteq A_2$, e igualmente $A_2 \cap C_1 \trianglelefteq A_1 \cap A_2$. Como $C_1 \trianglelefteq A_1$, el teorema anterior nos da que $(A_1 \cap C_2)C_1 \trianglelefteq (A_1 \cap A_2)C_1$ y

$$(A_1 \cap A_2)C_1 \,/\, (A_1 \cap C_2)C_1 \cong A_1 \cap A_2 \,/\, (A_1 \cap C_2)(A_1 \cap A_2 \cap C_1) =$$

$$A_1 \cap A_2 \,/\, (A_1 \cap C_2)(A_2 \cap C_1),$$

pero análogamente llegamos a que $(A_2 \cap C_1)C_2 \trianglelefteq (A_1 \cap A_2)C_2$ y al isomorfismo

$$(A_1 \cap A_2)C_2 \,/\, (A_2 \cap C_1)C_2 \cong A_1 \cap A_2 \,/\, (A_1 \cap C_2)(A_2 \cap C_1),$$

de donde se sigue el isomorfismo del enunciado. ∎

Con esto ya podemos demostrar el resultado principal:

Definición 4.25 Dos series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G$$

son *equivalentes* si tienen la misma longitud $m = n$ y existe una permutación $\sigma \in \Sigma_n$ tal que

$$G_i/G_{i-1} \cong H_{\sigma(i)}/H_{\sigma(i-1)},$$

es decir, si ambas series tienen los mismos factores, tal vez en orden distinto.

Teorema 4.26 (Teorema de refinamiento de Schreier) *Dos series (normales) cualesquiera de un mismo grupo G admiten refinramientos (normales) equivalentes.*

DEMOSTRACIÓN: Sean

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G$$

dos series (normales) de G y definamos

$$G_{ij} = (G_i \cap H_j)G_{i-1}, \qquad H_{ij} = (H_j \cap G_i)H_{j-1}.$$

Como $G_i \cap H_j \leq G_i$ y $G_{i-1} \trianglelefteq G_i$, el teorema 4.23 nos da que

$$G_{ij} = (G_i \cap H_j)G_{i-1} \leq G_i \leq G,$$

y análogamente $H_{ij} \leq G$. Si las series dadas son normales, es inmediato que $G_{ij} \trianglelefteq G$ y $H_{ij} \trianglelefteq G$. Observemos que

$$G_{i0} = (G_i \cap H_0)G_{i-1} = G_{i-1}, \qquad H_{0j} = (H_j \cap G_0)H_{j-1} = H_{j-1},$$

$$G_{im} = (G_i \cap H_m)G_{i-1} = G_i, \qquad H_{nj} = (H_j \cap G_n)H_{j-1} = H_j.$$

Por lo tanto,

$$G_{i-1} = G_{i_0} \leq G_{i1} \leq \cdots \leq G_{im} = G_i,$$

$$H_{j-1} = H_{0j} \leq H_{1j} \leq \cdots \leq H_{nj} = H_j.$$

Además, el lema de Zassenhaus, tomando $C_1 = G_{i-1}$, $A_1 = G_i$, $C_2 = H_{j-1}$, $A_2 = H_j$ nos da que

$$G_{i,j-1} \trianglelefteq G_{ij}, \quad H_{i-1,j} \trianglelefteq H_{ij}, \quad G_{ij}/G_{i,j-1} \cong H_{ij}/H_{i-1,j}.$$

Por lo tanto, los subgrupos que hemos definido determinan refinamientos (normales) equivalentes de las dos series dadas. ∎

Como consecuencia:

Teorema 4.27 *Si un grupo G admite una serie de composición (principal) entonces toda serie (normal) propia de G puede refinarse hasta una serie de composición (principal).*

DEMOSTRACIÓN: Sea S una serie de composición (principal) de G y sea T una serie (normal) propia de G. Por el teorema anterior las series admiten refinamientos (normales) equivalentes S^* y T^*. En particular, ambas tendrán el mismo número de factores triviales. Si eliminamos estos factores triviales (eliminando los términos que los producen) obtenemos dos series (normales) propias S^{**} y T^{**} que siguen siendo equivalentes (pues hemos eliminado el mismo número de factores triviales en cada una) y siguen refinando a las series de partida, pues eran propias. Ahora bien, S no admite refinamientos (normales) propios de mayor longitud, luego S^{**} tiene que coincidir con S, luego se trata de una serie de composición (principal), luego T^{**} también lo es, y refina a la serie dada T. ∎

Por último:

Teorema 4.28 (de Jordan Hölder) *Dos series de composición (principales) de un mismo grupo son equivalentes.*

DEMOSTRACIÓN: Si S y T son dos series de composición (principales) de un mismo grupo, la prueba del teorema anterior muestra que admiten refinamientos (normales) propios equivalentes, pero ninguna de las dos admite refinamientos (normales) propios de mayor longitud, luego ellas mismas tienen que ser ya equivalentes. ∎

Definición 4.29 Si un grupo G admite una serie de composición (resp. principal), en particular si G es un grupo finito, se llama *longitud de composición* (resp. *longitud principal*) de G a la longitud de cualquier serie de composición (resp. principal) de G.

Los factores de una serie de composición (resp. principal) de G se llaman *factores de composición* (resp. *principales*) de G, y están unívocamente determinados, en el sentido de que en cualquier serie aparecerán los mismos, aunque sea en orden distinto.

Por ejemplo, los factores principales de Σ_4 son C_2, C_2, C_2, C_3, mientras que sus factores principales son C_2, $C_2 \times C_2$ y C_3.

En general, los factores de composición de un grupo son siempre grupos simples, y los factores principales son característicamente simples. En estos términos, podemos decir que un grupo es resoluble si y sólo si sus factores de composición son abelianos.

Capítulo V

Grupos nilpotentes

En este capítulo estudiaremos en primer lugar la clase de los grupos nilpotentes, que extiende a la clase de los p-grupos, y después estudiaremos los grupos p-nilpotentes. Veremos que un grupo es nilpotente si y sólo si es p-nilpotente para todo primo p. No obstante, veremos que la p-nilpotencia tiene interés por sí misma.

5.1 Grupos nilpotentes

Recordemos que un grupo G es resoluble si tiene una serie

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

cuyos factores G_{i+1}/G_i son abelianos. Un factor de una serie se dice *central* si cumple que

$$G_{i+1}/G_i \leq Z(G/G_i).$$

Una serie es *central* si sus factores son centrales (con lo que en particular son abelianos).

Definición 5.1 Un grupo G es *nilpotente* si tiene una serie central.

Obviamente, todo grupo abeliano es nilpotente y todo grupo nilpotente es resoluble.

A la hora de trabajar con series centrales es conveniente caracterizarlas en términos del conmutador de dos subgrupos, que se define como

$$[H, K] = \langle [h, k] \mid h \in H,\ k \in K \rangle .$$

Teorema 5.2 *Sea $K \leq H \leq G$. Se cumple que $K \trianglelefteq G$ y $H/K \leq Z(G/K)$ si y sólo si $[H, G] \leq K$.*

DEMOSTRACIÓN: Si $K \trianglelefteq G$ y $H/K \leq Z(G/K)$, tomamos $h \in H$ y $g \in G$, de modo que $hKgK = gKhK$, luego $h^{-1}g^{-1}hg \in K$, es decir, que $[h,g] \in K$, luego $[H,G] \leq K$.

Si $[H,G] \leq K$ y $h \in H$, $g \in G$, tenemos que $[h,g] \in [H,G] \leq K$, luego $h^{-1}g^{-1}hg = h^{-1}h^g \in K$.

En particular, si $h \in K$, concluimos que $h^g \in K$, lo que prueba que $K \trianglelefteq G$. En general, con $h \in H$ arbitrario, tenemos que $hKgK = gKhK$, luego se cumple $H/K \leq Z(G/K)$. ∎

Así, una serie de un grupo G es central si y sólo si cumple $[G_{i+1}, G] \leq G_i$.

El teorema siguiente recoge las propiedades básicas de los grupos nilpotentes:

Teorema 5.3 *Se cumple:*

1. *Si G es un grupo nilpotente y $H \leq G$, entonces H es nilpotente.*
2. *Si G es un grupo nilpotente y $N \trianglelefteq G$, entonces G/N es nilpotente.*
3. *Si G es un grupo y $G/Z(G)$ es nilpotente, entonces G es nilpotente.*
4. *Si H y K son grupos nilpotentes, entonces $H \times K$ es nilpotente.*

DEMOSTRACIÓN: 1) Si

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

es una serie central de G, entonces

$$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_n \cap H = H$$

es una serie central de H, pues

$$[H \cap G_{i+1}, H] \leq H \cap [G_{i+1}, G] \leq H \cap G_i.$$

2) En este caso la serie

$$1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \cdots \trianglelefteq G_nN/N = G/N$$

es central, pues

$$[G_{i+1}N/N, G/N] = [G_{i+1}, G]N/N \leq G_iN/N.$$

3) Ahora suponemos que existe una serie central

$$1 = G_0/Z(G) \trianglelefteq G_1/Z(G) \trianglelefteq \cdots G_n/Z(G) = G/Z(G)$$

y observamos que

$$1 \trianglelefteq Z(G) \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

también es una serie central, pues ciertamente $[Z(G), G] = 1 \leq 1$ y, por otra parte,

$$[G_{i+1}/Z(G), G/Z(G)] = [G_{i+1}, G]Z(G)/Z(G) \leq G_i/Z(G),$$

luego $[G_{i+1}, G] \leq G_i$.

4) En este caso tenemos dos series centrales

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H,$$

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_n = K.$$

Podemos suponerlas de la misma longitud, pues si una es más corta la prolongamos añadiendo subgrupos triviales. Entonces

$$1 = H_0 \times K_0 \trianglelefteq H_1 \times K_1 \trianglelefteq \cdots \trianglelefteq H_n \times K_n = H \times K$$

es una serie central, pues

$$[H_{i+1} \times K_{i+1}, H \times K] = [H_{i+1}, H] \times [K_{i+1}, K] \leq H_i \times K_i. \qquad \blacksquare$$

Nota Si comparamos con el teorema 4.3, vemos que, en el caso de los grupos nilpotentes, la tercera propiedad sólo vale cuando el subgrupo es $Z(G)$, y la cuarta sólo vale para productos directos (pero véase el teorema 5.8). Un contraejemplo lo proporciona Σ_3, que no es nilpotente por el teorema siguiente, mientras que Σ_3/A_3 y A_3 son nilpotentes, porque son abelianos, y $\Sigma_3 = A_3\langle(1,2)\rangle$ es un producto de subgrupos nilpotentes que no es nilpotente. $\blacksquare$

Si G es un grupo nilpotente no trivial, tiene una serie central, en la que podemos exigir que $G_1 \neq 1$, y $G_1/1 \leq Z(G/1)$, luego $1 < G_1 \leq Z(G)$. Así pues:

Teorema 5.4 *Si G es un grupo nilpotente no trivial, entonces $Z(G) \neq 1$.*

Este teorema generaliza al teorema 2.5 en virtud del teorema siguiente:

Teorema 5.5 *Todo p-grupo es nilpotente.*

Demostración: Si el resultado es falso, sea G un p-grupo que no sea nilpotente del menor orden posible. Por 2.5 sabemos que $Z(G) \neq 1$, luego $G/Z(G)$ es un p-grupo de orden menor, luego es nilpotente por la minimalidad de G, luego G también lo es por el teorema 5.3. $\blacksquare$

Por consiguiente, todo producto directo de p-grupos (para primos no necesariamente iguales) es nilpotente. Vamos a probar que no hay más posibilidades, es decir, que los grupos nilpotentes son precisamente los productos directos de p-grupos. Para ello nos basaremos en el teorema siguiente:

Teorema 5.6 *Si G es un grupo nilpotente y $H < G$, entonces $H < N_G(H)$.*

Demostración: Consideremos una serie central

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

Se cumple que $G_0 = 1 \leq H$, pero $G_n \not\leq H$, luego existe un índice i tal que $G_i \leq H$, $G_{i+1} \not\leq H$. Entonces

$$[G_{i+1}, H] \leq [G_{i+1}, G] \leq G_i \leq H,$$

y esto implica que $G_{i+1} \leq N_G(H)$, pues si $g \in G_{i+1}$, $h \in H$, entonces

$$g^{-1}hgh^{-1} = [g, h^{-1}] \in [G_{i+1}, H] \leq H,$$

luego $h^g \in H$. Así pues, $N_G(H)$ contiene elementos que no están en H. $\blacksquare$

Teorema 5.7 *Si G es un grupo finito, las afirmaciones siguientes son equivalentes:*

1. *G es nilpotente.*
2. *Los subgrupos de Sylow de G son normales.*
3. *G es producto directo de p-grupos (con primos p no necesariamente iguales).*

DEMOSTRACIÓN: 1) $\Rightarrow$ 2). Sea P un p-subgrupo de Sylow de G y sea $H = N_G(P)$. Por 3.34 tenemos que $N_G(H) = H$, luego el teorema anterior nos da que $H = G$, es decir, que $P \trianglelefteq G$.

2) $\Rightarrow$ 3) Es claro que el producto de los subgrupos de Sylow es directo, pues son normales (luego hay uno solo para cada primo) y uno de ellos tiene orden primo con el orden de del producto de los demás, luego la intersección de uno con el producto de los demás es trivial.

3) $\Rightarrow$ 1) Si G es producto directo de p-grupos entonces es nilpotente, porque los p-grupos son nilpotentes y el producto directo de grupos nilpotentes es nilpotente. ∎

Teorema 5.8 *Si N_1 y N_2 son subgrupos normales nilpotentes de un grupo G, entonces N_1N_2 es nilpotente.*

DEMOSTRACIÓN: Pongamos que $N_1 = P_1 \times \cdots \times P_n$, $N_2 = Q_1 \times \cdots \times Q_n$, donde $|P_i| = p_i^{e_i}$, $|Q_i| = p_i^{f_i}$, donde $p_i \neq p_j$ si $i \neq j$. Podemos suponer que los primos son los mismos en ambos subgrupos admitiendo que los exponentes puedan ser $e_i = 0$ o $f_i = 0$.

Cada P_i es el único p_i-subgrupo de Sylow de N_1, luego es característico en N_1 y normal en G. Igualmente Q_i es normal en G, luego $R_i = P_iQ_i$ es un p_i-subgrupo normal de G y $N_1N_2 = R_1 \cdots R_n$, pero el producto es directo, ya que cada uno de los R_i es normal en G (luego en el producto) y su intersección con el producto de los restantes es trivial, ya que es la intersección de dos grupos de órdenes primos entre sí. Por lo tanto, N_1N_2 es producto directo de grupos nilpotentes, luego es nilpotente. ∎

Todo grupo resoluble tiene una serie abeliana de longitud mínima, que es la serie derivada. Igualmente, todo grupo nilpotente tiene dos series centrales de longitud mínima, una ascendente y otra descendente:

Definición 5.9 Si G es un grupo, definimos los subgrupos $\Gamma_i(G)$ y $Z_i(G)$ mediante las relaciones recurrentes:

$$\Gamma_1(G) = G, \quad \Gamma_{i+1}(G) = [\Gamma_i(G), G],$$

$$Z_0(G) = 1, \quad Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

Tenemos así dos sucesiones de subgrupos característicos de G:

$$\cdots \trianglelefteq \Gamma_3(G) \trianglelefteq \Gamma_2(G) \trianglelefteq \Gamma_1(G) = G$$

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

Teorema 5.10 *Si G es un grupo, las afirmaciones siguientes son equivalentes:*

1. *G es nilpotente.*
2. *Existe un n tal que $\Gamma_n(G) = 1$.*
3. *Existe un n tal que $Z_n(G) = G$.*

Además, en tal caso el menor natural c tal que $\Gamma_{c+1}(G) = 1$ coincide con el menor natural c tal que $Z_c(G) = G$, y es la menor longitud de cualquier serie central de G.

Demostración: Es obvio que 2) y 3) implican 1), pues en tal caso tenemos una de las series

$$1 = \Gamma_{c+1}(G) \trianglelefteq \cdots \trianglelefteq \Gamma_2(G) \trianglelefteq \Gamma_1(G) = G$$

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \cdots \trianglelefteq Z_c(G) = G$$

que es obviamente central. Veamos ahora que 1) implica 2) y 3). Si G es nilpotente, tenemos una serie central

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

y vamos a probar por inducción que $G_i \leq Z_i(G)$. Esto implica que $Z_n(G) = G$, luego la longitud de la serie definida por los subgrupos $Z_i(G)$ es menor o igual que la de la serie dada.

Obviamente $1 = G_0 = Z_0(G)$. Supongamos que $G_i \leq Z_i(G)$. Entonces tenemos un epimorfismo

$$G/G_i \longrightarrow G/Z_i(G).$$

Como $G_{i+1}/G_i \leq Z(G/G_i)$, la imagen de G_{i+1}/G_i por el epimorfismo está contenida en el centro de la imagen, es decir,

$$G_{i+1}Z_i(G)/Z_i(G) \leq Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G),$$

luego $G_{i+1} \leq Z_{i+1}(G)$.

Ahora probamos que $\Gamma_{i+1}(G) \leq G_{n-i}$. Para $i = 0$ es $\Gamma_1(G) = G = G_n$. Supuesto cierto para i, tenemos que $[G_{n-i}, G] \leq G_{n-i-1}$, luego

$$\Gamma_{i+2}(G) = [\Gamma_{i+1}(G), G] \leq [G_{n-i}, G] \leq G_{n-(i+1)}.$$

Por lo tanto, $\Gamma_{n+1}(G) \leq G_0 = 1$ y G es nilpotente. Además, la longitud de la serie definida por los subgrupos $\Gamma_i(G)$ es menor o igual que la de la serie dada.

Esto implica que las dos series que estamos considerando tienen que tener la misma longitud, ya que ésta es en ambos casos la menor longitud posible de una serie central de G. ∎

Definición 5.11 Si G es un grupo nilpotente, las series

$$1 = \Gamma_{c+1}(G) \trianglelefteq \cdots \trianglelefteq \Gamma_2(G) \trianglelefteq \Gamma_1(G) = G$$

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \cdots \trianglelefteq Z_c(G) = G$$

se llaman *serie central descendente* y *serie central ascendente* de G, respectivamente y, según acabamos de probar, tienen la misma longitud c, que es la menor longitud posible de una serie central de G.

Como aplicación obtenemos una generalización de 5.4:

Teorema 5.12 *Si G es un grupo nilpotente y $1 < N \trianglelefteq G$, entonces*

$$N \cap Z(G) \neq 1, \qquad [N, G] < N.$$

Demostración: Sea $N_1 = N$ y $N_{i+1} = [N_i, G]$. Veamos por inducción que $N_i \leq \Gamma_i(G)$. Claramente $N_1 \leq G = \Gamma_1(G)$. Supuesto cierto para i, tenemos que

$$N_{i+1} = [N_i, G] \leq [\Gamma_i(G), G)] = \Gamma_{i+1}(G).$$

Como existe un n tal que $\Gamma_n(G) = 1$, también $N_n = 1$. Sea $k > 1$ el menor natural tal que $N_k = 1$. Entonces $N_k = [N_{k-1}, G] = 1$, luego $N_{k-1} \leq Z(G)$ y así $1 \neq N_{k-1} \leq N \cap Z(G)$.

Además, si fuera $[N, G] = N$, entonces sería $N_i = N$ para todo i, en contra de lo que hemos probado. ∎

Veamos a su vez una aplicación de este teorema. Para ello introducimos el concepto siguiente:

Definición 5.13 Si G es un grupo, una *serie principal* de G es una serie

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

con la propiedad de que todos sus términos son normales en G y que no es posible extenderla intercalando términos, es decir, que no existe ningún subgrupo $G_{i+1} \lhd N \lhd G_i$ con $N \lhd G$.

Obviamente, todo grupo finito tiene una serie principal, pues, si no es trivial, sólo tenemos que partir de la serie $1 \lhd G$ y extenderla todo lo posible intercalando subgrupos.

Notemos que la condición para que una serie sea principal es que G_{i+1}/G_i no contenga subgrupos propios normales en G/G_i o, lo que es lo mismo, que G_{i+1}/G_i sea un subgrupo normal minimal de G/G_i.

Teorema 5.14 *Toda serie principal de un grupo nilpotente es central.*

DEMOSTRACIÓN: Sea G un grupo nilpotente y tomemos una serie central:

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G.$$

Entonces, $N = G_{i+1}/G_i$ es un subgrupo normal minimal de G/G_i, que es un grupo nilpotente, luego el teorema 5.12 nos da que $N \cap Z(G/G_i) \neq 1$, pero la intersección es normal en G/G_i, luego por la minimalidad de N tiene que ser $N \cap Z(G/G_i) = N$, es decir, $N \leq Z(G/G_i)$, y esto significa que la serie es central. ∎

Así pues, para comprobar si un grupo es nilpotente, podemos estudiar cualquiera de sus series centrales.

Grupos p-nilpotentes Sabemos que un grupo finito es nilpotente si y sólo si sus subgrupos de Sylow son normales. Ahora vamos a ver que esto es equivalente a que tenga p-complementos normales:

Definición 5.15 Si p es un número primo, un grupo finito G es p-nilpotente si posee un p-complemento normal, es decir, un subgrupo normal N tal que $p \nmid |H|$ y $|G : N|$ es potencia de p.

Si G es un grupo finito nilpotente, entonces es producto directo de sus subgrupos de Sylow, luego el producto de todos los subgrupos de Sylow correspondientes a primos distintos de p es un p-complemento normal en G. Así pues, todo grupo finito nilpotente es p-nilpotente para todo primo p. Enseguida probaremos el recíproco, pero antes conviene probar un hecho básico:

Teorema 5.16 *Todo subgrupo y todo cociente de un grupo p-nilpotente es p-nilpotente.*

DEMOSTRACIÓN: Sea G un grupo p-nilpotente y $H \leq G$. Sea C un p-complemento normal de G y P un p-subgrupo de Sylow de G, de modo que $G = PC$, $P \cap C = 1$. Entonces

$$H/(H \cap C) \cong HC/C \leq PC/C \cong P/(P \cap C) \cong P,$$

luego $|H : H \cap C|$ es potencia de p y $p \nmid |H \cap C|$, luego $H \cap C$ es un p-complemento normal en H.

Si $N \trianglelefteq G$, entonces, por 4.13, sabemos que CN/N es un p'-subgrupo de Hall normal de G/N, es decir, es un p-complemento normal de G/N. ∎

Teorema 5.17 *Si G es un grupo finito p-nilpotente, los factores de cualquier serie principal de G de orden divisible entre p son centrales.*

DEMOSTRACIÓN: Sea

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

una serie principal de G y supongamos que $p \mid |G_{i+1} : G_i|$. Sabemos que $L = G_{i+1}/G_i$ es un subgrupo normal minimal de $\bar{G} = G/G_i$. Este grupo es p-nilpotente por el teorema anterior. Sea P un p-subgrupo de Sylow de $\bar{G}$ y sea C un complemento normal, de modo que $\bar{G} = PC$ con $P \cap C = 1$.

Entonces $L \cap C \trianglelefteq \bar{G}$, luego por la minimalidad de L tiene que ser $L \cap C = 1$ o bien $L \cap C = L$, pero en el segundo caso $L \leq C$, luego $p \mid |C|$, contradicción. Así pues, $L \cap C = 1$, luego L y C conmutan elemento a elemento, por 3.1.

Por otro lado, $L \cap P$ es un p-subgrupo de Sylow de L, luego $L \cap P \neq 1$, ya que $p \mid |L|$. Como P es nilpotente, el teorema 5.12 nos da que

$$L \cap P \cap Z(P) = L \cap Z(P) \neq 1.$$

Tomemos, pues, $g \in L \cap Z(P)$, $g \neq 1$. Así g conmuta con los elementos de P y también con los de C y, como $\bar{G} = PC$, concluimos que $g \in L \cap Z(\bar{G}) \neq 1$.

Tenemos entonces que $L \cap Z(\bar{G}) \trianglelefteq \bar{G}$, luego, por la minimalidad de L, tiene que ser $L \cap Z(\bar{G}) = L$, es decir, $L \leq Z(\bar{G})$, lo que siginifica que L es un factor central de la serie dada. ∎

Ahora ya es inmediato el teorema que habíamos anunciado:

Teorema 5.18 *Un grupo finito G es nilpotente si y sólo si es p-nilpotente para todo primo p.*

Sin embargo, no es evidente que se cumpla el recíproco del teorema 5.17. Para probar éste y otros hechos sobre grupos p-nilpotentes necesitamos una técnica que expondremos en la sección siguiente.

5.2 Transferencias

En esta sección demostraremos un teorema sobre existencia de subgrupos de Hall normales:

Teorema 5.19 *Si G es un grupo finito y H es un π-subgrupo de Hall abeliano, entonces G tiene un π'-subgrupo de Hall normal si y sólo si en H no hay ningún par de elementos distintos conjugados en G.*

La prueba de este teorema no es trivial, y en ella emplearemos lo que se conoce como "aplicación de transferencia" de G a H. Probaremos únicamente los resultados sobre transferencias que necesitaremos para probar el teorema anterior.

De momento supondremos únicamente que G es un grupo y que $H \leq G$ es un subgrupo abeliano de índice finito $|G : H| = n$.

Una *transversal derecha* de H en G es un conjunto T que conste de un único elemento de cada clase del cociente $(G/H)_d$. Claramente entonces se cumple que $|T| = |G : H| = n$ y $HT = G$.

Si T es una transversal derecha, $g \in G$ y $h \in H$, es claro que hT y Tg son también transversales derechas.

Si T y U son dos transversales derechas, podemos numerar sus elementos

$$T = \{t_1, \ldots, t_n\}, \qquad Y = \{u_1, \ldots, u_n\}$$

de modo que $Ht_i = Hu_i$, con lo que $t_i u_i^{-1} \in H$, y entonces definimos

$$T/U = \prod_{i=1}^{n} t_i u_i^{-1} \in H.$$

Como H es abeliano, T/U no depende del orden en que se enumeran los elementos de las transversales.

Teorema 5.20 *Si T, U, V son transversales derechas de H en G, entonces*

1. $T/T = 1$.
2. $U/T = (T/U)^{-1}$.
3. $(T/U)(U/V) = T/V$.

DEMOSTRACIÓN: 1) $T/T = \prod_{i=1}^{n} t_i t_i^{-1} = 1$.

2) Teniendo en cuenta que H es abeliano,

$$U/T = \prod_{i=1}^{n} u_i t_i^{-1} = \prod_{i=1}^{n} (t_i u_i^{-1})^{-1} = \left(\prod_{i=1}^{n} t_i u_i^{-1} \right)^{-1} = (T/U)^{-1}.$$

3) Igualmente:

$$(T/U)(U/V) = \prod_{i=1}^{n} t_i u_i^{-1} \prod_{i=1}^{n} u_i v_i^{-1} = \prod_{i=1}^{n} t_i v_i^{-1} = T/V.$$

■

Teorema 5.21 *Si T, U son transversales, $g \in G$ y $h \in H$, entonces*

$$Tg/Ug = T/U = hT/hU.$$

DEMOSTRACIÓN: Sea $T = \{t_1, \ldots, t_n\}$, $U = \{u_1, \ldots, u_n\}$ de modo que $Ht_i = Hu_i$. Entonces $Ht_i g = Hu_i g$ y $Hht_i = Ht_i = Hu_i = Hhu_i$, luego

$$Tg/Ug = \prod_{i=1}^{n} t_i g (u_i g)^{-1} = \prod_{i=1}^{n} t_i u_i^{-1} = T/U,$$

$$hT/hU = \prod_{i=1}^{n} ht_i (hu_i)^{-1} = \prod_{i=1}^{n} ht_i u_i^{-1} h^{-1} = \prod_{i=1}^{n} t_i u_i^{-1} = T/U.$$

■

Con esto ya podemos definir la aplicación de transferencia:

Definición 5.22 Sea G un grupo y $H \leq G$ un subgrupo abeliano de índice finito $|G : H| = n$. Definimos la *transferencia* de G a H como la aplicación $\tau : G \longrightarrow H$ dada por $\tau(g) = Tg/T$, donde T es una transversal derecha de H en G.

Teorema 5.23 *En las condiciones de la definición anterior, la transferencia τ no depende de la elección de la transversal T y es un homomorfismo de grupos.*

DEMOSTRACIÓN: Si T y U son dos transversales y $g \in G$, entonces

$$Tg/T = (Tg/Ug)(Ug/U)(U/T) = (T/U)(Ug/U)(T/U)^{-1} = Ug/U,$$

donde usamos que H es abeliano. Así pues, la transferencia no depende de la transversal. Por otra parte,

$$\tau(xy) = Txy/T = (Txy/Ty)(Ty/T) = (Tx/T)(Ty/T) = \tau(x)\tau(y).$$

■

Veremos que si H cumple las hipótesis del teorema 5.19, entonces el núcleo de la transferencia será el π'-subgrupo de Hall normal buscado.

Definición 5.24 Sea $\mathcal{T}$ el conjunto de todas las transversales derechas de H en G. Podemos definir dos acciones $\rho : \mathcal{T} \times G \longrightarrow \mathcal{T}$, $\rho^* : H \times \mathcal{T} \longrightarrow \mathcal{T}$ (la primera por la derecha y la segunda por la izquierda) mediante $(T, g) \mapsto Tg$, $(h, T) \mapsto hT$.

El teorema 5.20 implica que la relación en $\mathcal{T}$ dada por

$$T \sim U \qquad \text{si y sólo si} \qquad T/U = 1$$

es una relación de equivalencia y 5.21 implica que es compatible con ambas acciones, es decir, que, si llamamos Ω al conjunto de las clases de equivalencia, también tenemos acciones bien definidas

$$\rho : \Omega \times G \longrightarrow \Omega, \qquad \rho^* : H \times \Omega \longrightarrow \Omega$$

dadas por $([T], g) \mapsto [Tg]$, $(h, [T]) \mapsto [hT]$.

Observemos que si $T = \{t_1, \ldots, t_n\}$ y $h \in H$, entonces

$$hT/T = \prod_{i=1}^{n} ht_i t_i^{-1} = h^n.$$

Nota A partir de aquí supondremos que H es un π-subgrupo de Hall de G, es decir, que $|G : H| = n$ y $|H| = m$ son primos entre sí.

Teorema 5.25 *La acción de H sobre Ω es transitiva (es decir, determina una única órbita) y para cada $\omega \in \Omega$ su estabilizador es $H_\omega = 1$.*

DEMOSTRACIÓN: Tomemos $a, b \in \mathbb{Z}$ tales que $an + bm = 1$. Si $[T], [U] \in \Omega$, tenemos que $T/U \in H$ y $|H/J| = m$, luego $(T/U)^m = 1$, luego $(T/U)^{bm} = 1$, luego $(T/U)^{1-an} = 1$. Sea $h = (T/U)^{-a} \in H$. Entonces, según la observación previa al teorema,

$$hT/U = (hT/T)(T/U) = h^n(T/U) = (T/U)^{-an}(T/U) = 1,$$

luego $hT \sim U$, lo cual equivale a que $h[T] = [U]$, y así $[T]$ y $[U]$ están en la misma órbita.

Si $\omega = [T] \in \Omega$ y$h \in H_\omega$, entonces $h[T] = [T]$, luego $hT \sim T$, luego $hT/T = 1$, luego $h^n = 1$. Entonces $h = h^{an+bm} = (h^n)^a(h^m)^b = 1$, luego $H_\omega = 1$. ∎

Ahora vamos a necesitar un hecho general sobre grupos de permutaciones:

Teorema 5.26 *Si X es un conjunto no vacío $A \leq \Sigma_X$ es un subgrupo abeliano que actúa transitivamente sobre Ω, entonces $C_{\Sigma_X}(A) = A$.*

Demostración: Sea $C = C_{\Sigma_X}(A)$. Como A es abeliano, es claro que $A \leq C$. Sea $\sigma \in C$ y $x \in X$. Sea $y = x\sigma \in X$. Como A actúa transitivamente, existe un $\alpha \in A$ tal que $y = x\alpha$. Así, para todo $\beta \in A$ tenemos que

$$(x\beta)\sigma = (x\sigma)\beta = (x\alpha)\beta = x\beta\alpha,$$

donde hemos usado que $\sigma \in C$ y que A es abeliano. Como la acción es transitiva, $x\beta$ recorre todos los elementos de X al variar β, luego hemos probado que $z\sigma = z\alpha$ para todo $z \in X$, es decir, que $\sigma = \alpha \in A$, luego $C \leq A$ y así $C = A$. ∎

Teorema 5.27 *Para cada $g \in G$ existe un único $g^* \in H$ tal que, para todo $\omega \in \Omega$, $\omega g = g^*\omega$. La aplicación $\theta : G \longrightarrow H$ dada por $\theta(g) = g^*$ es un homomorfismo de grupos y la transferencia $\tau : G \longrightarrow H$ cumple $\tau(g) = \theta(g)^n$.*

Demostración: Podemos ver la acción de G sobre Ω como un homomorfismo $\rho : G \longrightarrow \Sigma_\Omega$. Con la acción de H hay que tener una precaución debido a que es una acción por la izquierda (mientras que Σ_Ω actúa sobre Ω por la derecha[1]). En general, es fácil ver que una acción por la izquierda de un grupo G sobre un conjunto Ω determina una acción por la derecha mediante $\omega g = g^{-1}\omega$. En nuestro caso, la acción por la derecha de H sobre Ω así definida determina un homomorfismo $\rho^* : H \longrightarrow \Sigma_\omega$ dado por

$$\rho^*(h)(\omega) = h^{-1}\omega.$$

De hecho se trata de un monomorfismo, pues si $\rho^*(h) = 1$, entonces h estabiliza a todo $\omega \in \Omega$, pero los estabilizadores son triviales.

Sea $A = \operatorname{Im}\rho^* \leq \Sigma_\Omega$, que es un subgrupo abeliano, porque H es abeliano. Como H actúa transitivamente sobre Ω, es claro que lo mismo le sucede a A con su acción como grupo de permutaciones.

Si T es una transversal y $g \in G$, es claro que $(h^{-1}T)g = h^{-1}(Tg)$, luego si $\omega = [T]$, tenemos que $(h^{-1}\omega)g = h^{-1}(\omega g)$ o, equivalentemente,

$$\rho(g)(\rho^*(h)(\omega)) = \rho^*(h)(\rho(g)(\omega)),$$

para todo $\omega \in \Omega$, luego $\rho^*(h)\rho(g) = \rho(g)\rho^*(h)$, para todo $h \in H$, luego el teorema anterior nos da que $\rho(g) \in C_{\Sigma_\Omega}(A) = A$.

[1]Esto se traduce en que si llamamos $\rho^*(h)(\omega) = h\omega$ no obtenemos un homomorfismo $\rho^* : H \longrightarrow \Sigma_\Omega$, sino que

$$\rho^*(h_1h_2)(\omega) = h_1h_2\omega = h_1\rho^*(h_2)(\omega) = \rho^*(h1)(\rho^*(h_2)(\omega)) = \rho^*(h_2)\rho^*(h_1)(\omega),$$

y así $\rho^*(h_1h_2) = \rho^*(h_2)\rho^*(h_1)$, por lo que ρ^* es lo que se llama un antiautomorfismo.

Así pues, existe un único $g^* \in H$ tal que $\rho(g) = \rho^*((g^*)^{-1})$, es decir, tal que, para todo $\omega \in \Omega$, se cumple $\omega g = g^*\omega$. Con esto tenemos definida la aplicación θ. Ahora:

$$\theta(g_1g_2)\omega = \omega(g_1g_2) = (\omega g_1)g_2 = (\theta(g_1)\omega)g_2 = \theta(g_2)\theta(g_1)\omega = (\theta(g_1)\theta(g_2))\omega,$$

donde usamos que H es abeliano. Como la acción de H tiene estabilizadores triviales, de aquí se sigue que $\theta(g_1g_2) = \theta(g_1)\theta(g_2)$, luego θ es un homomorfismo.

Finalmente, si $g \in G$, sea $h = \theta(g)$. Fijamos una transversal T y observamos que $[T]g = \theta(g)[T]$, luego $[T]g = h[T]$, luego $Tg \sim hT$, luego

$$\tau(g) = Tg/T = (Tg/hT)(hT/T) = 1 \cdot h^n = h^n\theta(g)^n.$$

■

Ahora ya podemos estudiar el núcleo de la transferencia:

Teorema 5.28 *Si $\omega \in \Omega$, el estabilizador G_ω es el núcleo K de la transferencia τ, que coincide con el núcleo del homomorfismo θ. Si G actúa transitivamente sobre Ω, entonces $G/K \cong H$.*

Demostración: Como $\tau = \theta^n$, es claro que $\mathrm{N}(\theta) \leq \mathrm{N}(\tau)$. Si $g \in \mathrm{N}(\tau)$, entonces $\theta^n(g) = 1$, luego $o(\theta(g)) \mid n$. Pero $\theta(g) \in H$, luego $o(\theta(g)) \mid m$ y, como m y n son primos entre sí, $o(\theta(g)) = 1$, es decir, $\theta(g) = 1$ y así $g \in \mathrm{N}(\theta)$. Por lo tanto, podemos llamar $K = \mathrm{N}(\tau) = \mathrm{N}(\theta)$.

Se cumple $g \in G_\omega$ si y sólo si $\omega g = \omega$, si y sólo si $\theta(g)\omega = \omega$, si y sólo si $\theta(g) = 1$ (pues los estabilizadores de la acción de H/J son triviales) si y sólo si $g \in K$. Así pues, $G_\omega = K$.

Supongamos ahora que G actúa transitivamente sobre Ω. Basta probar que $\theta : G \longrightarrow H$ es suprayectiva, pues entonces el teorema de isomorfía nos da que $G/K \cong H$.

Si $h \in H$, tomamos $\omega \in \Omega$. La transitividad de G implica que existe un $g \in G$ tal que $h\omega = \omega g = \theta(g)\omega$. Como los estabilizadores en H son triviales, esto implica que $\theta(g) = h$. ■

Observemos que, dado que H es un π-subgrupo de Hall de G, la conclusión del teorema anterior es que K es un π'-subgrupo de Hall normal. Para expresar las hipótesis en términos de la conjugación en G, tal y como requiere el teorema 5.19, necesitamos un último resultado:

Teorema 5.29 *Para cada $g \in G$ existen números enteros $n_1, \ldots, n_s$ tales que $n_1 + \cdots + n_s = n$ y elementos $x_1, \ldots, x_s \in G$ de modo que $x_i g^{n_i} x_i^{-1} \in H$ y*

$$\tau(g) = \prod_{i=1}^{s} x_i g^{n_i} x_i^{-1},$$

Demostración: Consideremos la acción de $\langle g \rangle$ sobre $(G/H)_d$ por multiplicación a derecha y sean $X_1, \ldots, X_s$ las órbitas que determina. Sea $n_i = |X_i|$, de modo que $n_1 + \cdots + n_s = n$. Elijamos $Hx_i \in X_i$, de modo que

$$X_i = \{Hx_i, Hx_ig, \ldots, Hx_ig^{n_i-1}\}$$

y $Hx_ig^{n_i} = Hx_i$, con lo que $x_ig^{n_i}x_i^{-1} \in H$. Claramente,

$$T = \{x_ig^r \mid r = 0, \dots, n_i - 1,\ i = 1, \dots, s\}$$

es una transversal de H en G y $Tg = \{x_ig^r \mid r = 1, \dots, n_i,\ i = 1, \dots, s\}$. Entonces

$$\tau(g) = Tg/T = \prod_{i=1}^{s} x_ig^{n_i}x_i^{-1},$$

pues el elemento de Tg que corresponde a $x_ig^r \in T$, para $0 < r < n_i$ es él mismo, luego los factores correspondientes a estos términos en $\tau(g)$ se cancelan, y el elemento de Tg correspondiente a $x_i \in T$ es $Hx_ig^{n_i}$. ∎

El teorema siguiente es 5.19 con una condición equivalente adicional:

Teorema 5.30 *Sea H un π-subgrupo de Hall abeliano de un grupo G y sea $n = |G : H|$. Las afirmaciones siguientes son equivalentes:*

1. *G tiene un π'-subgrupo de Hall normal.*
2. *Si $h_1, h_2 \in H$ son conjugados en G, entonces $h_1 = h_2$.*
3. *La transferencia $\tau : G \longrightarrow H$ cumple $\tau(h) = h^n$ para todo $h \in H$.*

Demostración: 1) ⇒ 2). Sea $K \trianglelefteq G$ un π'-subgrupo de Hall. Entonces $H \cap K = 1$ y $G = HK$.

Supongamos que $h_1, h_2 \in H$ cumplen $h_2 = h_1^g$, con $g \in G$. Como $G = HK$, podemos descomponer $g = h'k$, con $h' \in H$ y $k \in K$, con lo que $h_2 = h_1^{h'k} = h_1^k$. Por lo tanto, no perdemos generalidad si suponemos que $g = k \in K$. Como $K \trianglelefteq G$,

$$h_1^{-1}h_2 = h_1^{-1}h_1^k = h_1^{-1}k^{-1}h_1k = (k^{-1})^{h_1}k \in H \cap K = 1,$$

luego $h_1 = h_2$.

2) ⇒ 3) Dado $h \in H$, por el teorema anterior

$$\tau(h) = \prod_{i=1}^{s} x_ih^{n_i}x_i^{-1},$$

donde $x_ih^{n_i}x_i^{-1}$ y h^{n_i} son conjugados en G, luego por hipótesis tenemos que son iguales, luego

$$\tau(h) = \prod_{i=1}^{s} h^{n_i} = h^n.$$

3) ⇒ 1) Observemos que si $h \in H$ y T es una transversal, por hipótesis $\tau(h) = Th/T = h^n = hT/T$ (por las observaciones tras la definición 5.24). Por lo tanto

$$hT/Th = (hT/T)(Th/T)^{-1} = 1,$$

luego $hT \sim Th$ o, equivalentemente, $h\omega = \omega h$ para todo $h \in H$ y todo $\omega \in \Omega$. Esto significa que la restricción a H de la acción de G por la derecha coincide con la acción de H por la izquierda, que es transitiva por 5.25, luego la acción de G por la derecha también es transitiva.

El teorema 5.28 nos da que $K = \mathrm{N}(\tau) \trianglelefteq G$ coincide con G_ω para todo $\omega \in \Omega$, luego $H \cap K = H_\omega = 1$, de nuevo por 5.25, pues el estabilizador de ω en H respecto de la acción por la derecha coincide con el de la acción por la izquierda, ya que hemos visto que ambas acciones coinciden.

Por último, si $g \in G$, como la acción de H es transitiva, dado $\omega \in \Omega$, existe un $h \in H$ tal que $\omega g = \omega h$, luego $gh^{-1} \in G_\omega = K$, luego $g \in HK$, y esto prueba que $G = HK$.

Puesto que $G = HK$ y $H \cap K = 1$, es claro que K es un π'-subgrupo de Hall (normal) de G. ∎

En la sección siguiente extraeremos algunas consecuencias de este teorema.

5.3 Grupos p-nilpotentes

Ahora estamos en condiciones de estudiar más a fondo los grupos p-nilpotentes que hemos definido en 5.15. Para empezar podemos demostrar el recíproco del teorema 5.17:

Teorema 5.31 *Un grupo finito G es p-nilpotente si y sólo si los factores de orden divisible entre p de cualquier serie principal de G prefijada son centrales.*

Demostración: Una implicación es el teorema 5.17. Si el recíproco fuera falso, podríamos tomar un grupo G del menor orden posible que tuviera una serie principal

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

cuyos factores de orden divisible entre p fueran centrales, pero que G no fuera p-nilpotente. Entonces

$$1 = G_1/G_1 \lhd \cdots \lhd G_n/G_1 = G/G_1$$

es claramente una serie principal de G/G_1 y si un factor $G_{i+1}/G_1 \Big/ G_i/G_1$ tiene orden divisible entre p, entonces $p \mid |G_{i+1}/G_i|$, luego $G_{i+1}/G_i \leq Z(G/G_i)$, y esto implica que

$$G_{i+1}/G_1 \Big/ G_i/G_1 \leq Z(G/G_1 \,/\, G_i/G_1).$$

Así pues, G/G_1 tiene una serie central cuyos factores de orden divisible entre p son centrales. Por la minimalidad de G tenemos que G/G_1 es p-nilpotente. Sea N/G_1 un p-complemento normal de G/G_1. Esto significa que

$$|G/G_1 : N/G_1| = |G : N|$$

es potencia de p, y que $p \nmid |N : G_1|$.

Si $p \nmid |G_1|$, entonces $p \nmid |N|$, pues $|N| = |N : G_1||G_1|$, luego N es un p-complemento normal en G y así G es p-nilpotente, en contra de lo supuesto.

Supongamos, pues que $p \mid |G_1|$. Entonces, por la elección de la serie principal, sabemos que $G_1 \leq Z(G)$.

Siendo el penúltimo término de una serie principal, G_1 es un subgrupo normal minimal de G, y es abeliano, luego por el teorema 4.16 es un grupo abeliano elemental, en particular un p-grupo. Como $p \nmid |N : G_1|$, tenemos que G_1 es un p-subgrupo de Sylow de N.

Como $G_1 \leq Z(N)$, no puede suceder que dos elementos distintos de G_1 sean conjugados en N, luego el teorema 5.19 nos asegura que N tiene un p-complemento normal K. Como $G_1 \trianglelefteq N$, se cumple de hecho que $N = G_1 \times K$.

Sea P un p-subgrupo de Sylow de G que contenga a G_1. Como N/G_1 es un p-complemento normal en G/G_1, tenemos que $(P/G_1)(N/G_1) = G/G_1$, luego $G = PN = PG_1K = PK$, luego $|G : K| = |P : P \cap K|$ es potencia de p, y esto implica que K es un p-complemento en G. Si probamos que es normal, resultará que G es p-nilpotente y tendremos una contradicción.

Como $G = KP$, basta ver que si $p \in P$ entonces $K^p = K$. Pero si $k \in K$, tenemos que $k^p \in N^p = N = G_1K$, luego $k^p = gk'$, con $g \in G_1$, $k' \in K$, pero $g = k^p k^{-1} \in K^pK \cap G_1 = 1$, ya que $p \nmid K^pK$ y G_1 es un p-grupo. (Notemos que $K^p \leq N^p = N$ y $K \trianglelefteq N$, por lo que $K^pK \leq N$). Por consiguiente, $k^p = k' \in K$, luego $K \trianglelefteq G$. ∎

Para la siguiente aplicación del teorema 5.19 necesitamos un resultado previo:

Teorema 5.32 (Lema de Burnside) *Sea P un p-subgrupo de Sylow de un grupo finito G. Si dos elementos de $Z(P)$ son conjugados en G, lo son en $N_G(P)$.*

Demostración: Supongamos que $x, y \in Z(G)$ cumplen $y = x^g$, con $g \in G$. Entonces

$$P \leq C_G(x) \cap C_G(y) = C_G(x) \cap C_G(x)^g,$$

luego

$$P^{g^{-1}} \leq C_G(x)^{g^{-1}} \cap C_G(x).$$

Así, P y $P^{g^{-1}}$ son p-subgrupos de Sylow de $C_G(x)$, luego son conjugados en $C_G(x)$. Sea $z \in C_G(x)$ tal que $P^{g^{-1}} = P^z$. Entonces $P = P^{zg}$, luego se cumple que $zg \in N_G(P)$ y $y = x^g = (x^z)^g = x^{zg}$. ∎

Teorema 5.33 (Burnside) *Sea P un p-subgrupo de Sylow de un grupo finito G. Si $P \leq Z(N_G(P))$, entonces G es p-nilpotente.*

Demostración: Sea $H = N_G(P)$. Como $P \leq Z(H)$, se cumple que P es abeliano. Si $x_1, x_2 \in P = Z(P)$ son conjugados en G, por el teorema anterior son conjugados en H, pero coo $P \leq Z(H)$, esto implica que $x_1 = x_2$. El teorema 5.19 implica entonces que G tiene un p'-subgrupo de Hall normal, es decir, un p-complemento normal, luego G es p-nilpotente. ∎

Como aplicación obtenemos lo siguiente:

Teorema 5.34 *Sea G un grupo finito y sea p el menor primo que divide a su orden. Si los p-subgrupos de Sylow de G son cíclicos entonces G es p-nilpotente.*

DEMOSTRACIÓN: Sea P un p-subgrupo de Sylow de G, con $|P| = p^m$. Por hipótesis P es cíclico, luego $P \leq C_G(P) \leq N_G(P)$.

Según las observaciones tras la definición 2.7, sabemos que $N_G(P)/C_G(P)$ es isomorfo a un subgrupo de $\mathrm{Aut}(P) \cong U_{p^m}$ (teorema 1.17). Por lo tanto,

$$|N_G(P) : C_G(P)| \mid |U_{p^m}| = (p-1)p^{m-1},$$

pero, como $P \leq C_G(P)$, se cumple que $p \nmid |N_G(P) : C_G(P)|$, luego de hecho $|N_G(P) : C_G(P)| \mid p-1$.

Sin embargo, $|N_G(P) : C_G(P)| \mid |G|$ y p es el menor primo que divide a $|G|$, luego tiene que ser $||N_G(P) : C_G(P)| = 1$, es decir, que $N_G(P) = C_G(P)$, lo cual implica que $P \leq Z(N_G(P))$, luego G es p-nilpotente por el teorema anterior. ∎

Notemos que este teorema nos da una prueba alternativa del teorema 4.11.

Veamos una variante del teorema de Burnside:

Teorema 5.35 *Sea P un p-subgrupo de Sylow de un grupo finito G. Si P es abeliano y $P \cap Z(N_G(P)) \neq 1$, entonces G no es simple.*

DEMOSTRACIÓN: Consideramos la transferencia $T : G \longrightarrow P$. Tomemos un elemento no trivial $g \in P \cap Z(N_G(P))$. Según el teorema 5.29 existen enteros $n_1, \ldots, n_s$ tales que $n_1 + \cdots + n_s = n = |G : P|$ y elementos $x_1, \ldots, x_s \in G$ de modo que $x_i g^{n_i} x_i^{-1} \in P$ y

$$\tau(g) = \prod_{i=1}^{s} x_i g^{n_i} x_i^{-1}.$$

Como g^{n_i} y $x_i g^{n_i} x_i^{-1}$ son conjugados en G, por 5.32 también son conjugados en $N_G(P)$, es decir, que existe $y_i \in N_G(P)$ de modo que $x_i g^{n_i} x_i^{-1} = y_i^{-1} g^{n_i} y_i$, pero $g^{n_i} \in Z(N_G(P))$, luego $x_i g^{n_i} x_i^{-1} = y_i^{-1} g^{n_i} y_i = g^{h_i}$ y concluimos que $\tau(g) = g^n$.

No puede ser $g^n = 1$, pues entonces $o(g) \mid n = |G_P|$ y $o(g) \mid |P|$, luego $o(g) = 1$, cuando $g \neq 1$. Por lo tanto, $\tau(g) \neq 1$ y el núcleo de la transferencia es un subgrupo $K \lhd G$. No puede ser $K = 1$, pues entonces sería $|G| \leq |P|$. Así pues, G tiene un subgrupo normal propio, luego no es simple. ∎

5.4 Aplicaciones de los teoremas de Burnside

En 1911 Burnside conjeturó que todo grupo de orden impar es resoluble. Actualmente este hecho se conoce como el Teorema de Feit-Thompson, y fue demostrado en 1963. Una demostración revisada ocupa dos libros enteros. Si a la teoría de Sylow añadimos el teorema de Burnside 5.33 y el teorema 6.40 (también de Burnside) que demostraremos en el capítulo siguiente, podemos probar un fragmento del teorema de Feit-Thompson:

Teorema 5.36 *Todo grupo de orden impar menor que* 1000 *es resoluble.*

DEMOSTRACIÓN: En la prueba del teorema 4.5 se ve que todo grupo finito admite una serie con factores simples, y el grupo es resoluble si y sólo si dichos factores son abelianos, luego un grupo no resoluble tiene una serie con un factor simple no abeliano. Por consiguiente, si existiera un grupo no resoluble de orden impar menor que 1 000, tendría una serie con un factor simple no abeliano de orden impar menor que 1 000. Así pues, basta ver que no existen grupos simples no abelianos de orden impar menor que 1 000.

Si G fuera tal grupo y $|G| = p_1p_2$ o $|G| = p_1p_2p_3$, con los p_i primos, no necesariamente distintos, entonces G sería resoluble, bien por ser un p-grupo, bien por ser de orden libre de cuadrados (teorema 4.11) bien por ser de orden p^aq^b.

Así pues, $|G|$ tiene que ser divisible al menos por cuatro primos, no necesariamente distintos. De hecho, no pueden ser distintos, pues el menor producto de cuatro primos impares distintos es $3 \cdot 5 \cdot 7 \cdot 11 = 1\,155$.

Por otro lado, $|G|$ no puede ser divisible entre 6 primos, pues el menor valor posible que no sea potencia de primo es $3^5 \cdot 5 = 1\,215$. Así pues, $|G|$ es divisible entre 4 o 5 primos (no necesariamente distintos).

Si el menor primo que divide a $|G|$ fuera mayor que 3, el menor valor posible sería $5^2 \cdot 7 \cdot 11 = 1\,925$, así que $3 \mid |G|$. Pero el teorema 5.34 nos da que $9 \mid |G|$. Esto nos deja sólo las posibilidades siguientes para $|G|$:

$$3^2 \cdot 5 \cdot 7, \quad 3^2 \cdot 5 \cdot 11, \quad 3^2 \cdot 5 \cdot 13, \quad 3^2 \cdot 5 \cdot 17, \quad 3^2 \cdot 5 \cdot 19,$$

$$3^2 \cdot 7 \cdot 11, \quad 3^2 \cdot 7 \cdot 13, \quad 3^3 \cdot 5 \cdot 7.$$

El tercer teorema de Sylow nos permite descartar algunos casos:

Si $|G| = 3^2 \cdot 5 \cdot 13$, entonces $\nu_{13} = 1$, luego G tiene un 13-subgrupo de Sylow normal. Igualmente, si $|G| = 3^2 \cdot 5 \cdot 17$ resulta que $\nu_{17} = 1$, si $|G| = 3^2 \cdot 5 \cdot 19$ es $\nu_{19} = 1$, si $|G| = 3^2 \cdot 7 \cdot 11$ es $\nu_{11} = 1$ y si $|G| = 3^2 \cdot 7 \cdot 13$ es $\nu_{13} = 1$. Con esto nos quedan únicamente tres posibilidades:

$$3^2 \cdot 5 \cdot 7, \quad 3^2 \cdot 5 \cdot 11, \quad 3^3 \cdot 5 \cdot 7.$$

Si $|G| = 3^2 \cdot 5 \cdot 7$, descartando $\nu_5 = 1$, tiene que ser $\nu_5 = 21$, luego si P es un 5-subgrupo de Sylow, se cumple que $|N_G(P)| = 15$, pero según 3.28 todo grupo de orden 15 es cíclico, luego $P \leq Z(N_G(P))$ y G es 5-nilpotente por el teorema 5.33, luego no es simple.

Igualmente, si $|G| = 3^2 \cdot 5 \cdot 11$, descartando $\nu_3 = 1$, tendría que ser $\nu_3 = 5 \cdot 11$, y entonces, un 3-subgrupo de Sylow cumple $|N_G(P)| = |P|$, luego $P = N_G(P)$ y nuevamente llegamos a que $P \leq Z(N_G(P))$.

Por último, si $|G| = 3^3 \cdot 5 \cdot 7$, tiene que ser $\nu_3 = 7$, luego si P es un 3-subgrupo de Sylow de G, se cumple que $|G : N_G(P)| = 7$, luego el teorema de Cayley 2.25 nos da un homomorfismo $G \longrightarrow \Sigma_7$ que tiene que ser inyectivo si G es simple, pero $|G| = 3^3 \cdot 5 \cdot 7$ no divide a 7!. ∎

Veamos ahora qué podemos decir de los grupos de orden par. Supongamos que G es un grupo simple no abeliano de orden, digamos, n. Sabemos que

1. n tiene que ser divisible al menos entre tres primos distintos (por 6.40).

2. $4 \mid n$ (por el teorema anterior y 2.28).

Los valores de n entre 1 y 500 que cumplen estas condiciones son los que incluye la tabla siguiente:

$60 = 2^2 \cdot 3 \cdot 5$		$312 = 2^3 \cdot 3 \cdot 13$	$\nu_{13} = 1$
$84 = 2^2 \cdot 3 \cdot 7$	$\nu_7 = 1$	$336 = 2^4 \cdot 3 \cdot 7$	$\nu_7 = 8$
$120 = 2^3 \cdot 3 \cdot 5$	$\nu_5 = 6$	$340 = 2^2 \cdot 5 \cdot 17$	$\nu_{17} = 1$
$132 = 2^2 \cdot 3 \cdot 11$	$\nu_{11} = 1$	$348 = 2^2 \cdot 3 \cdot 29$	$\nu_{29} = 1$
$140 = 2^2 \cdot 5 \cdot 7$	$\nu_7 = 1$	$360 = 2^3 \cdot 3^2 \cdot 5$	
$156 = 2^2 \cdot 3 \cdot 13$	$\nu_{13} = 1$	$364 = 2^2 \cdot 7 \cdot 13$	$\nu_7 = 1$
$168 = 2^3 \cdot 3 \cdot 7$		$372 = 2^2 \cdot 3 \cdot 31$	$\nu_{31} = 1$
$180 = 2^2 \cdot 3^2 \cdot 5$	$\nu_5 = 6, 36$	$380 = 2^2 \cdot 5 \cdot 19$	$\nu_{19} = 20$
$204 = 2^2 \cdot 3 \cdot 17$	$\nu_{17} = 1$	$396 = 2^2 \cdot 3^2 \cdot 11$	$\nu_{11} = 12$
$220 = 2^2 \cdot 5 \cdot 11$	$\nu_{11} = 1$	$408 = 2^3 \cdot 3 \cdot 17$	$\nu_{17} = 1$
$228 = 2^2 \cdot 3 \cdot 19$	$\nu_{19} = 1$	$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$	$\nu_7 = 15$
$240 = 2^4 \cdot 3 \cdot 5$	$\nu_5 = 6, 16$	$440 = 2^3 \cdot 5 \cdot 11$	$\nu_{11} = 1$
$252 = 2^2 \cdot 3^2 \cdot 7$	$\nu_7 = 36$	$444 = 2^2 \cdot 3 \cdot 37$	$\nu_{37} = 1$
$260 = 2^2 \cdot 5 \cdot 13$	$\nu_{13} = 1$	$456 = 2^3 \cdot 3 \cdot 19$	$\nu_{19} = 1$
$264 = 2^3 \cdot 3 \cdot 11$	$\nu_{11} = 12$	$460 = 2^2 \cdot 5 \cdot 23$	$\nu_{23} = 1$
$276 = 2^2 \cdot 3 \cdot 23$	$\nu_{23} = 1$	$468 = 2^2 \cdot 3^2 \cdot 13$	$\nu_{13} = 1$
$280 = 2^3 \cdot 5 \cdot 7$	$\nu_5 = 56$	$476 = 2^2 \cdot 7 \cdot 17$	$\nu_{17} = 1$
$300 = 2^2 \cdot 3 \cdot 5^2$	$\nu_5 = 6$	$480 = 2^5 \cdot 3 \cdot 5$	$\nu_2 = 15$
$308 = 2^2 \cdot 7 \cdot 11$	$\nu_{11} = 1$	$492 = 2^2 \cdot 3 \cdot 41$	$\nu_{42} = 1$

En la mayoría de los casos los teoremas de Sylow implican la existencia de un primo p tal que $\nu_p = 1$, es decir, la existencia de un p-subgrupo de Sylow normal, por lo que no hay grupos simples del orden correspondiente.

Descartando el caso $\nu_p = 1$ cuando hay otras alternativas, otro caso sencillo se da cuando $\nu_5 = 6$, pues entonces, si P es un 5-grupo de Sylow, tenemos que $H = N_G(P)$ tiene índice 6, luego el teorema de Cayley 2.25 nos permite sumergir $G \longrightarrow \Sigma_6$ (el homomorfismo es inyectivo porque G es simple), por lo que podemos suponer que $G \leq \Sigma_6$, y entonces $G \cap A_6 \trianglelefteq G$, y no puede ser $G \cap A_6 = 1$, ya que entonces $G \cong G/(G \cap A_6) \cong GA_6/A_6 \leq \Sigma_6/A_6 \cong C_2$ y tendría que ser $|G| \leq 2$. Por lo tanto $G \cap A_6 = G$, que equivale a que $G \leq A_6$, pero en los casos recogidos en la tabla esto implica que el índice $|A_6 : G|$ vale 3 (cuando $n = 120$), 2 (cuando $n = 180$) o ni siquiera es entero (cuando $n = 240, 300$), pero A_6 es un grupo simple, luego no puede tener subgrupos de índice $2, 3, 4$ (teorema 2.29).

Esto nos deja únicamente la posibilidad $\nu_5 = 36$ cuando $n = 180$, que se descarta por el mismo argumento que para $n = 252, 280, 380$, pues en todos ellos $\nu_p = |G : N_G(P)| = |G : P|$, donde P es un p-subgrupo de Sylow del primo indicado en la tabla, luego $N_G(P) = P$, y en todos los casos considerados P es abeliano, luego $P \leq Z(N_G(P))$ y G es p-nilpotente por el teorema 5.33.

Una variante de este argumento se aplica cuando $n = 240$ (descartada la posibilidad $\nu_5 = 6$) y cuando $n = 396$, pues en estos casos $|N_G(P)| = 15, 33$ y, por el teorema 3.28 todo grupo de orden 15 o 33 es abeliano, luego se cumple igualmente que $P \leq Z(N_G(P))$.

Más delicados son los casos $n = 264, 336$. En el primero $\nu_{11} = 12$, luego, si P es un 11-subgrupo de Sylow de G, se cumple que $|N_G(P)| = 22$. Como antes podemos suponer que $G \leq A_{12}$. Entonces G está generado por un ciclo σ de longitud 11, y en A_{12} hay un total de 12!/11 ciclos de longitud 11 y cada 7-subgrupo de Sylow de A_{12} contiene 10 de ellos, luego el número de 7-subgrupos de Sylow de A_{12} es 12!/110, luego $|N_{A_{12}}(P)| = 55$, pero esto es imposible, porque $N_G(P) \leq N_{A_{12}}(P)$ y $22 \nmid 55$.

En el caso $n = 336$ razonamos análogamente. Ahora tenemos que $\nu_7 = 8$, luego $|N_G(P)| = 42$ y, suponiendo $G \leq A_8$, tenemos que P está generado por un ciclo de longitud 7, en total hay 8!/7 tales ciclos, luego en A_8 hay 8!/42 subgrupos de Sylow de orden 7, luego $|N_{A_8}(P)| = 21$, y nuevamente es imposible que $N_G(P) \leq N_{A_8}(P)$.

Si $n = 480$, la teoría de Sylow admite las posibilidades $\nu_2 = 1, 3, 5, 15$, pero G no cabe en A_5, lo que nos da $\nu_2 = 15$, que es el valor que hemos consignado en la tabla anterior. Como $\nu_2 \not\equiv 1 \pmod 4$, el teorema 3.36 nos da la existencia de 2-subgrupos de Sylow P y Q tales que $|P \cap Q| = 2^4$. Entonces $K = P \cap Q$ es normal en P y en Q, pues tiene índice 2, luego $P, Q \leq N_G(K) < G$ (porque K no puede ser normal en G). A su vez, como $N_G(K)$ posee al menos dos 2-subgrupos de Sylow, tiene que ser $P < N_G(K) < G$, pero $|G : P| = 15$, luego $|G : N_G(K)| = 3, 5$, luego G tendría que poder sumergirse en A_5, y no es el caso.

Finalmente, el casos más difícil de descartar es $n = 420$:

Teorema 5.37 *No hay grupos simples de orden* 420.

DEMOSTRACIÓN: Si G es un grupo simple de orden $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, la teoría de Sylow nos da que $\nu_7 = 15$. Sean $P_1, \ldots, P_{15}$ sus subgrupos de Sylow. La acción sobre ellos por conjugación nos permite considerar que $G \leq A_{15}$. Además, $H = N_G(P_{15})$ es el estabilizador de P_{15}, es decir, está formado por las permutaciones que fijan al índice 15. Como tiene índice 15, es $|H| = 28$.

Sea $P_{17} = \langle\sigma\rangle$, donde σ tiene orden 7, luego tiene que ser un ciclo de longitud 7, o bien un producto de dos ciclos disjuntos de longitud 7. Pero el primer caso es imposible, porque entonces existiría otro índice $i \neq 15$ tal que $\sigma \in N_G(P_i)$, luego $P_{15} \leq N_G(P_i)$, y así el normalizador tendría al menos dos 7-subgrupos de Sylow, uno de ellos normal, lo cual es absurdo. Así pues, renumerando los subgrupos de Sylow, podemos suponer que

$$\sigma = (1, 2, 3, 4, 5, 6, 7)(8, 9, 10, 11, 12, 13, 14).$$

Observemos que σ tiene $14!/(2 \cdot 7^2)$ conjugados en Σ_{14}, luego se cumple que $|C_{\Sigma_{14}}(\sigma)| = 2 \cdot 7^2$. Como el centralizador contiene permutaciones impares

(por ejemplo, un producto de 7 trasposiciones que intercambie los dos ciclos), $|C_{A_{14}}(\sigma)| = 7^2$ y, como $|G|$ no es divisible entre 7^2, llegamos a que $|C_G(\sigma)| = 7$, es decir, que $C_G(P_{15}) = P_{15}$.

No puede ser que H tenga elementos de orden 28, pues entonces sería abeliano y $P_{15} \leq Z(N_G(P_{15}))$ y G sería 7-nilpotente, por el teorema 5.33. Veamos que tampoco tiene elementos de orden 14. Una permutación par τ de orden 14 no puede ser un ciclo de orden 14, luego tiene que ser un ciclo de longitud 7 y un número par de trasposiciones, pero entonces τ^2 sería un ciclo de longitud 7, luego $\tau^2 \in P$, pero ya hemos razonado que P no puede estar generado por un ciclo de longitud 7.

Así pues, H tiene 1 elemento de orden 1, otros 6 elementos de orden 7 y los 21 elementos restantes tienen que tener orden 2 o 4, pero según las observaciones tras la definición 2.7, tenemos que H/P_{17} (es decir, $N_G(P_{15})/C_G(P_{15})$) es isomorfo a un subgrupo de $\mathrm{Aut}(P_{15})$, que tiene orden 6, luego H/P no puede tener elementos de orden 4 y H tampoco. En conclusión, H tiene 21 elementos de orden 2.

Si $\tau \in H$ tiene orden 2, no puede ser que $\sigma^\tau = \sigma$, pues entonces $\sigma\tau$ tendría orden 14. Por lo tanto, $\sigma^\tau = \sigma^{-1}$. Explícitamente,

$$(1,2,3,4,5,6,7)^\tau(8,9,10,11,12,13,14)^\tau = (7,6,5,4,3,2,1)(14,13,12,11,10,9,8),$$

pero no puede ser que

$$(1,2,3,4,5,6,7)^\tau = (14,13,12,11,10,9,8),$$

pues τ tiene que ser un producto de trasposiciones, y es fácil ver que para que cumpla esto debe constar exactamente de 7 transposiciones, luego sería impar. Por lo tanto,

$$(1,2,3,4,5,6,7)^\tau = (7,6,5,4,3,2,1),$$

$$(8,9,10,11,12,13,14)^\tau = (14,13,12,11,10,9,8),$$

lo cual puede conseguirse con 6 trasposiciones. En particular,

$$\tau[\{1,2,3,4,5,6,7\}] = \{1,2,3,4,5,6,7\},$$

$$\tau[\{8,9,10,11,12,13,14\}] = \{8,9,10,11,12,13,14\},$$

pero para que un producto de trasposiciones (disjuntas) cumpla esto, debe fijar necesariamente al menos un índice de cada conjunto. Ahora bien, si $\tau(i) = i$, $\tau(j) = j$, con $i \leq 7$, $j \geq 8$, entonces τ está completamente determinada. Por ejemplo, si $\tau(3) = 3$ y $\tau(9) = 9$, necesariamente

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 4 & 3 & 2 & 1 & 7 & 6 & 10 & 9 & 8 & 14 & 13 & 12 & 11 \end{pmatrix}$$

$$= (1,5)(2,4)(6,7)(8,10)(11,14)(12,13).$$

Esto en principio nos daría 49 posibilidades para τ, pero en realidad no puede haber dos permutaciones distintas tales que $\tau(i) = i$ y $\tau'(i) = i$ con $i \leq 7$, ya

que si, por ejemplo, $\tau(j) = j$ y $\tau'(k) = k$ con $j > k \geq 8$, entonces $(\tau\tau')(j) = \tau'(j) \neq j$, luego $\tau\tau' \neq 1$, pero $\tau\tau'$ fija a todos los índices de $\{1, 2, 3, 4, 5, 6, 7\}$, luego $(1, 2, 3, 4, 5, 6, 7)^{\tau\tau'} = (1, 2, 3, 4, 5, 6, 7)$, cuando debería ser el ciclo inverso.

Por lo tanto H sólo puede tener 7 elementos de orden 2, y no 21 como hemos visto que hacen falta. ∎

Con esto hemos probado:

Teorema 5.38 *Todo grupo simple no abeliano de orden* ≤ 500 *tiene orden* $60, 168$ *o* 360.

Recordemos que el teorema 3.40 prueba que todo grupo simple de orden 60 es isomorfo a A_5. Similarmente:

Teorema 5.39 *Todo grupo simple de orden* 360 *es isomorfo a* A_6.

Demostración: Sea G un grupo simple de orden $|G| = 360 = 2^3 \cdot 3^2 \cdot 5$.

En primer lugar, la teoría de Sylow nos dice que el número de 3-subgrupos de Sylow tene que cumplir $\nu_3 \mid 40$ y $\nu_3 \equiv 1$ (mód 3), lo que nos da las posibilidades $\nu_3 = 1, 4, 10, 40$, pero descartamos $\nu_3 = 1$ porque entonces G tendría un único 3-subgrupo de Sylow normal, descartamos $\nu_3 = 4$ porque entonces el teorema de Cayley 2.25 nos daría un monomorfismo $G \longrightarrow \Sigma_4$, lo cual es absurdo, y descartamos $\nu_3 = 40$ porque entonces un 3-subgrupo de Sylow sería abeliano y cumpliría $N_G(P) = P$, y el teorema de Burnside 5.33 nos daría que G es 3-nilpotente.

Así pues, ya sabemos que $\nu_3 = 10$ y si P es un 3-subgrupo de Sylow, entonces $|N_G(P)| = 36$. La teoría de Sylow nos dice también que G actúa transitivamente sobre el conjunto Ω de sus 3-subgrupos de Sylow. Por la simplicidad de G, el homomorfismo $\rho : G \longrightarrow \Sigma_\Omega$ asociado a dicha acción es un monomorfismo, lo que nos permite considerar que $G \leq \Sigma_{10}$ y que los estabilizadores de los elementos de Ω (que son los normalizadores de los 3-subgrupos de Sylow) tienen orden 36.

Si identificamos $P \in \Omega$ con el índice 10 en I_{10}, podemos identificar el estabilizador G_{10} (es decir, el conjunto de las permutaciones de A_{10} que fijan el índice 10), con un subgrupo $P \leq G_{10} \leq A_9$.

En principio tenemos dos posibilidades para P, según si se cumple $P \cong C_9$ o si $P \cong C_3 \times C_3$. Vamos a descartar la primera.

Si P es cíclico, estará generado por un ciclo σ de longitud 9. En Σ_9 hay $9!/9 = 8!$ ciclos de longitud 9, luego $|\mathrm{cl}_{\Sigma_9}(\sigma)| = 8!$, luego $|C_{\Sigma_9}(\sigma)| = 9$. Así,

$$C_{\Sigma_9}(\sigma) \Big/ (C_{\sigma_9}(\sigma) \cap A_9) \cong C_{\Sigma_9}(\sigma)A_9 \Big/ A_9 \leq \Sigma_9/A_9 \cong C_2,$$

pero el primer grupo tiene orden divisor de 9, luego tiene que tener orden 1, luego $C_{\Sigma_9}(\sigma) \leq A_9$, luego $C_{A_9}(\sigma) = C_{\Sigma_9}(\sigma)$ y así $|C_{A_9}(\sigma)| = 9$, es decir, que $C_{A_9}(P) = P$.

Ahora, según hemos visto tras la definición 2.7, el cociente

$$N_{A_9}(P)/C_{A_9}(P)$$

tiene orden 4 y es isomorfo a un subgrupo de $\mathrm{Aut}(P) = \mathrm{Aut}(C_9) \cong U_9$, que tiene orden 6, lo cual es absurdo.

Con esto tenemos demostrado que $P \cong C_3 \times C_3$.

Ahora vamos a probar que si P y Q son dos 3-subgrupos de Sylow distintos en G, necesariamente $P \cap Q = 1$.

En caso contrario $P \cap Q \cong C_3$, luego podemos tomar $\sigma \in P \cap Q$ de orden 3. El centralizador $H = C_G(\sigma)$ contiene al menos dos 3-subgrupos de Sylow (P y Q), y como $\nu_3(H) \mid |H : P| \mid 40$ y $\nu_3(H) \equiv 1 \pmod 3$, las posibilidades son $\nu_3 = 4, 10, 40$, pero H no puede tener más 3-subgrupos de Sylow que G, luego $\nu_3 = 4, 10$.

En el segundo caso $90 \mid |C_G(\sigma)|$, luego $|G : C_G(\sigma)| \mid 4$, luego $G = C_G(\sigma)$ por el teorema 2.29, pero esto implica que $\sigma \in Z(G)$, lo cual es imposible.

Así pues, $\nu_3 = 4$, luego $36 \mid |H|$, luego $|G : H| \mid 10$, pero el índice no puede ser $1, 2, 5$, ya que el teorema de Cayley 2.25 nos daría que $G \leq \Sigma_5$, lo cual es absurdo. Concluimos que $|G : H| = 10$, luego $|H| = 36$.

Por consiguiente, $N_H(P) = P$ y el teorema de Burnside 5.33 nos daría que H es 3-nilpotente, es decir, que tiene un 3-complemento (o un 2-subgrupo de Sylow) normal Q. Entonces $H \leq N_G(Q)$, pero si Q' es un 2-subgrupo de Sylow de G tal que $Q \leq Q'$, entonces $Q' \leq N_G(Q)$ (pues $|G' : Q| = 2$), luego $72 \mid |N_G(Q)|$, luego $|G : N_G(Q)| = 5$ y de nuevo llegamos a que $G \leq \Sigma_5$, contradicción.

Con esto ya tenemos probado que los 3-subgrupos de Sylow tienen intersección trivial. Tomemos ahora $\sigma \in G$ de orden 3. Renumerando los índices, podemos suponer que $\sigma = (1, 2, 3)(4, 5, 6)(7, 8, 9)$, ya que σ no puede ser de tipo $(1, 2, 3)$ ni de tipo $(1, 2, 3)(4, 5, 6)$, pues en ambos casos tendríamos que $\sigma \in N_G(P_8) \cap N_G(P_9)$, pero P_8 y P_9 son los únicos 3-subgrupos de Sylow de sus normalizadores, y σ tiene que estar en un 3-subgrupo de Sylow de cada uno, luego $\sigma \in P_8 \cap P_9 = 1$, contradicción.

Pongamos que $P = \langle \sigma, \tau \rangle$. La permutación τ tiene orden 3 y cumple $\sigma^\tau = \sigma$, con lo que hay dos posibilidades: o bien

$$(1, 2, 3)^\tau = (1, 2, 3), \quad (4, 5, 6)^\tau = (4, 5, 6), \quad (7, 8, 9)^\tau = (7, 8, 9),$$

o bien τ permuta cíclicamente los tres ciclos. Pero, al igual que σ, la permutación τ tiene que ser un producto de tres ciclos disjuntos, luego para fijar los tres ciclos tiene que ser producto de $(1, 2, 3)$ o $(3, 2, 1)$, por $(4, 5, 6)$ o $(6, 5, 4)$ por $(7, 8, 9)$ o $(9, 8, 7)$, luego, o bien $\tau = \sigma$, o bien $\tau = \sigma^{-1}$ (con lo que σ y τ no serían generadores de P), o bien $\sigma\tau \in P$ tiene orden 3 y fija al menos tres índices, cosa que ya sabemos que no puede suceder.

Concluimos que τ permuta cíclicamente los tres ciclos que en los que se descompone σ. Por lo tanto, reordenando los índices podemos suponer (sin

alterar la expresión de σ) que

$$(1,2,3)^\tau = (4,5,6), \quad (4,5,6)^\tau = (7,8,9), \quad (7,8,9)^\tau = (1,2,3),$$

y, reordenando de nuevo, podemos suponer que

$$\tau = (1,4,7)(2,5,8)(3,6,9).$$

Observemos ahora que $C_{\Sigma_9}(P) = P$. Para probarlo basta ver que sólo hay 9 permutaciones ρ que cumplen $\sigma^\rho = \sigma$ y $\tau^\rho = \tau$, para lo cual, a su vez, basta probar que una permutación que cumpla esto está determinada por $\rho(1)$. Por ejemplo, si $\rho(1) = 5$, tiene que ser

$$(1,2,3)^\rho = (5,6,4), \qquad (1,4,7)^\rho = (5,8,2),$$

lo que obliga a que $\rho(2) = 6$, $\rho(3) = 4$, $\rho(4) = 8$, $\rho(7) = 2$ y de las dos últimas igualdades se sigue a su vez que

$$(4,5,6)^\rho = (8,9,7), \qquad (7,8,9)^\rho = (2,3,1),$$

de donde $\rho(5) = 9$, $\rho(6) = 7$, $\rho(8) = 3$, $\rho(9) = 1$, luego $\rho = (1,5,9)(2,6,7)(3,4,8)$, e igualmente se concluye en los otros ocho casos.

En particular, $C_G(P) = P$. Sea $H = N_G(P)$, que es un grupo de orden 36, y sea Q un 2-subgrupo de Sylow de H. Vamos a probar que $Q \cong C_4$. Tenemos que $H = PQ$, luego

$$Q \cong H/P = N_G(P)/C_G(P) \longrightarrow N_{A_9}(P)/C_{A_9}(P) \longrightarrow N_{\Sigma_9}(P)/C_{\Sigma_9}(P),$$

donde las flechas indican los monomorfismos inducidos por la inclusión. Ahora observamos que $N_{A_9}(P) = N_{\Sigma_9}(P) \cap A_9$ tiene índice 2 en $N_{\Sigma_9}(P)$, porque este último subgrupo contiene permutaciones impares, como $\rho = (1,7)(2,8)(3,9)$, y la imagen de $N_{A_9}(P)$ en $N_{\Sigma_9}(P)/C_{\Sigma_9}(P)$ sigue teniendo índice 2, porque

$$|N_{\Sigma_9}(P)/C_{\Sigma_9}(P) : N_{A_9}(P)C_{\Sigma_9}(P)/C_{\Sigma_9}(P)| = |N_{\Sigma_9}(P) : N_{A_9}(P)C_{\Sigma_9}(P)| =$$

$$|N_{\Sigma_9}(P)/N_{A_9}(P) : N_{A_9}(P)C_{\Sigma_9}(P)/N_{A_9}(P)| \,\Big|\, 2$$

y la clase $\rho C_{\Sigma_9}(P)$ no puede estar en dicha imagen, ya que entonces existiría una permutación $\rho' \in N_{A_9}(P)$ tal que $\rho\rho'^{-1} \in C_{\Sigma_9}(P) = P \leq A_9$, contradicción.

Según hemos visto tras la definición 2.7, el cociente $N_{\Sigma_9}(P)/C_{\Sigma_9}(P)$ es isomorfo a un subgrupo de $\mathrm{Aut}(P) \cong \mathrm{LG}(2,3)$. Vamos a ver que es todo $\mathrm{LG}(2,3)$, con lo que $N_{A_9}(P)/C_{A_9}(P)$ será isomorfo al único subgrupo de índice 2 de $\mathrm{LG}(2,3)$, que es $\mathrm{LE}(2,3)$ (véase la sección 3.7), luego Q será isomorfo a un subgrupo de un 2-subgrupo de Sylow de $\mathrm{LE}(2,3)$, pero en la sección 3.7 hemos visto también que dichos subgrupos de Sylow son de tipo Q_8, luego necesariamente $Q \cong C_4$, como queremos probar.

La permutación

$$k = (2,4,3,7)(5,6,9,8)$$

cumple $\sigma^k = \tau$ y $\tau^k = \sigma^{-1}$, luego induce el automorfismo que en la sección 3.7 llamábamos k.

Por otro lado, la permutación

$$g = (2,8,5)(3,6,9)$$

cumple $\sigma^g = \sigma\tau^{-1}$, $\tau^g = \tau$, por lo que el automorfismo que induce es el que en la sección 3.7 llamábamos σ_s^2. Esto significa que la imagen de $N_{\Sigma_9}(P)/C_{\Sigma_9}(P)$ en $\mathrm{Aut}(P)$ contiene un subgrupo de $\mathrm{LE}(2,3)$ de orden ≥ 12, luego dicho subgrupo tiene que ser todo $\mathrm{LE}(2,3)$, pero la imagen no puede ser exactamente $\mathrm{LE}(2,3)$ porque tiene que tener un subgrupo de índice 2 y $\mathrm{LE}(2,3)$ no lo tiene, luego la imagen tiene que ser todo $\mathrm{LG}(2,3)$.

Así pues, $Q = \langle\rho\rangle$, para cierto elemento ρ de orden 4 que induce un automorfismo de orden 4 en $P = \langle\sigma,\tau\rangle$. Esto implica que el polinomio mínimo de ρ (visto como automorfismo de P) tiene que dividir al polinomio

$$x^4 - 1 = (x-1)(x+1)(x^2+1) \in \mathbb{Z}_3[x].$$

Si el polinomio mínimo fuera $x \pm 1$, entonces ρ tendría dos factores invariantes iguales, y su forma canónica sería

$$A = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix},$$

pero entonces ρ tendría orden 2, por lo que el polinomio mínimo tiene que ser x^2+1, luego es el único factor invariante y, según [Al 6.30], la forma canónica es

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Esto significa que podemos tomar una base $P = \langle\sigma,\tau\rangle$ tal que

$$\sigma^\rho = \tau, \qquad \tau^\rho = \sigma^{-1},$$

lo que implica a su vez que

$$\sigma^{\rho^2} = \sigma^{-1}, \qquad \tau^{\rho^2} = \tau^{-1}, \qquad \sigma^{\rho^{-1}} = \tau^{-1}, \qquad \tau^{\rho^{-1}} = \sigma.$$

Es claro entonces que todo elemento de H se expresa de forma única como $\sigma^i\tau^j\rho^k$, con $i,j = 0,1,2$, $k = 0,1,2,3$. Un cálculo rutinario muestra que

$$(\sigma^i\tau^j\rho)^2 = \sigma^{i+j}\tau^{j-i}\rho^2, \qquad (\sigma^i\tau^j\rho)^4 = 1.$$

Por lo tanto, H tiene exactamente:

- 18 elementos de orden 4 (los de la forma $\sigma^i\tau^j\rho$ y $\sigma^i\tau^j\rho^3$),
- 9 elementos de orden 2 (los de la forma $\sigma^i\tau^j\rho^2$),
- 8 elementos de orden 3 (los de $P \setminus \{1\}$),
- 1 elemento de orden 1.

Como estos elementos ya suman 36, no hay más, luego en particular H no tiene elementos de orden 6. Vemos también que H tiene 9 subgrupos de Sylow de orden 4, cuyas intersecciones tienen que ser triviales, para que entre todos contengan los 9 elementos de H de orden 2.

Más aún, las expresiones explícitas que hemos encontrado antes para σ y τ muestran que P actúa transitivamente sobre $P_1, \dots, P_9$, luego lo mismo vale para H, luego el estabilizador de cada P_i tiene índice 9 en H, luego tiene orden 4, es decir, es un 2-subgrupo de Sylow de H. En otras palabras, los nueve 2-subgrupos de Sylow de H coinciden con los estabilizadores de los 3-subgrupos de Sylow $P_1, \dots, P_9$ de G. Como tienen intersección trivial, esto significa que cada elemento de H de orden 4 fija exactamente a dos 3-subgrupos de Sylow (a P_{10} y a otro más). Lo mismo vale para los elementos de orden 2, por lo que los elementos de orden 4 de H tienen que ser permutaciones de la forma

$$(\bullet, \bullet, \bullet, \bullet)(\bullet, \bullet, \bullet, \bullet),$$

pues así fijan sólo dos índices y sus cuadrados también.

Veamos ahora que G no tiene elementos de orden 6 ni de orden 15.

En efecto, si $x \in G$ tuviera orden 6, entonces x^2 tendría orden 3, luego existiría un 3-subgrupo de Sylow P tal que $x^2 \in P$, luego $x^2 \in P \cap P^x \neq 1$, pero hemos visto que dos 3-subgrupos de Sylow distintos tienen intersección trivial, luego $P^x = P$ y así $x \in N_G(P) = H$, cosa que acabamos de ver que es imposible.

Similarmente, si $x \in G$ tuviera orden 15, tendríamos que $x^5 \in P \cap P^x$, de donde $x \in N_G(P)$ y de nuevo tenemos una contradicción.

Ya hemos visto que G cumple $\nu_3 = 10$. La teoría de Sylow nos da que $\nu_5 = 6, 36$. Si fuera $\nu_5 = 6$, entonces, por el teorema de Cayley, G sería isomorfo a un subgrupo de Σ_6, luego sería $G \cong A_6$, como queremos probar (si bien en realidad este caso no puede darse, porque A_6 no cumple $\nu_5 = 6$, como se comprueba fácilmente contando los ciclos de longitud 5).

Así pues, $\nu_5 = 36$ y G tiene exactamente $36 \cdot 4 = 144$ elementos de orden 5. Además, si P_5 es un 5-subgrupo de Sylow de G, se cumple que $|N_G(P_5)| = 10$.

De aquí deducimos que G no tiene elementos de orden 10.

En efecto, si $x \in G$ tiene orden 10, entonces $x^2 \in P_5$, para cierto 5-subgrupo de Sylow, pero entonces $x^2 \in P_5 \cap P_5^x \neq 1$, luego $P_5^x = P_5$, luego $x \in N_G(P_5)$, luego $N_G(P_5)$ es abeliano, luego el teorema de Burnside 5.33 nos da que G es 5-nilpotente y tenemos una contradicción.

Concluimos que todo elemento de G tiene orden $1, 2, 4, 3, 5$ y, concretamente, hay 80 elementos de orden 3 y 144 de orden 5, luego tiene que haber un total de $360 - 1 - 80 - 144 = 135$ elementos de orden $2, 4$.

Por otra parte, $\nu_2 = 9, 15, 45$, donde hemos descartado $\nu_2 = 3, 5$ porque G no puede estar contenido en A_3 o A_5. Ahora bien, si $\nu_2 \leq 15$, habría a lo sumo

$15 \cdot 7 = 105$ elementos de orden $2, 4$, y acabamos de ver que tiene que haber más. Por lo tanto, concluimos que $\nu_2 = 45$ y así, si P_2 es un 2-subgrupo de Sylow, se cumple que $N_G(P_2) = P_2$.

Hemos visto que cada normalizador de un 3-subgrupo de Sylow contiene 18 elementos de orden 4 y cada uno está exactamente en 2 de ellos pues, fija únicamente a dos 3-subgrupos de Sylow. Por lo tanto, hay exactamente $10 \cdot 18/2 = 90$ elementos de orden 4 contenidos en normalizadores de 3-subrupos de Sylow. Análogamente, hay $10 \cdot 9/2 = 45$ elementos de orden 2 contenidos en normalizadores de 3-subgrupos de Sylow. Como $90 + 45 = 135$, son todos los elementos de G de orden $2, 4$, luego ahora podemos afirmar que G tiene exactamente 90 elementos de orden 4 y 45 de orden 2.

Dado un 3-subgrupo de Sylow P, sabemos que su normalizador contiene 9 elementos de orden 2, luego en G hay otros 36 elementos de orden 2 que no normalizan a P. Sea E el conjunto de todos ellos y sea $P^* = P \setminus \{1\}$.

La aplicación $E \times P^* \longrightarrow EP^*$ dada por $(x, y) \mapsto xy$ es inyectiva, pues si $xy = x'y'$, entonces $x = x'y'y^{-1}$ tiene orden 2, luego

$$x'y'y^{-1}x'y'y^{-1} = 1,$$

luego

$$x'y'y^{-1}x' = yy'^{-1} = (y'y^{-1})^{-1}.$$

Si $y \neq y'$, entonces $y'y^{-1}$ es un elemento de orden 3 de P y la igualdad anterior (teniendo en cuenta que $x' = x'^{-1}$) implica que $x' \in N_G(\langle y'y^{-1}\rangle)$, o también que $y'y^{-1} \in P \cap P^{x'}$, pero entonces $P = P^{x'}$, ya que los 3-subgrupos de Sylow tienen intersecciones triviales, luego $x' \in N_G(P)$, contradicción. Por lo tanto, $y = y'$, de donde se sigue que $x = x'$.

Así pues, $|EP^*| = 288$. Esto implica que algún elemento de EP^* tiene orden 5, o de lo contrario tendríamos $288 + 144 = 432$ elementos en G. Por lo tanto, podemos tomar $a, b \in G$ de órdenes 2 y 3 tales que ab tiene orden 5. En la página 101 hemos probado que

$$A_5 = \langle a, b \mid a^5 = b^3 = (ab)^2 = 1\rangle,$$

luego el subgrupo $\langle a, b\rangle$ que acabamos de construir en G es imagen de A_5, pero como A_5 es simple, tiene que ser $\langle a, b\rangle \cong A_5$, luego G tiene un subgrupo de índice 6, luego por el teorema de Cayley G es isomorfo a un subgrupo (de índice 2) de Σ_6, luego tiene que ser $G \cong A_6$. ∎

Estudiamos ahora si existen grupos simples de orden 168, que según el teorema 5.38 es el único orden posible menor que 500 para un grupo simple no abeliano distinto de A_5 y A_6. Vamos a ver que existe un único grupo simple de dicho orden. Para encontrarlo suponemos que G es un grupo simple de orden $|G| = 168 = 2^3 \cdot 3 \cdot 7$ y vamos a ver qué características debe tener.

En primer lugar observamos que G no puede tener subgrupos de índice menor que 7, ya que en tal caso el teorema de Cayley 2.25 nos daría un monomorfismo $G \longrightarrow \Sigma_6$, pero el orden de G no divide a 6!.

7-subgrupos de Sylow La teoría de Sylow nos da que $\nu_7 = 8$, por lo que los normalizadores de los 7-subgrupos de Sylow tienen orden 21. De aquí se sigue a su vez que G no tiene elementos de orden 14, pues si $g \in G$ tuviera orden 14 tendríamos que $\langle g^2 \rangle$ sería un 7-subgrupo de Sylow y g^7 estaría en su normalizador, pero g^7 tiene orden 2 y el normalizador tiene orden 21.

También podemos descartar que G tenga elementos de orden 21. En efecto, si $g \in G$ tuviera orden 21, entonces $\langle g^7 \rangle$ sería un 3-subgrupo de Sylow y g^3 estaría en su normalizador, luego éste tendría orden divisible entre 7, pero entonces la teoría de Sylow nos daría $\nu_3 \mid 8$ y $\nu_3 \equiv 1$ (mód 3), luego tendría que ser $\nu_3 = 4$ y G tendría un subgrupo de índice 4.

Por lo tanto, si $P = \langle g \rangle$ es un 7-subgrupo de Sylow de G, tenemos que $P \leq C_G(g) < N_G(P)$, pues si la última inclusión fuera una igualdad, tendríamos que $P \leq Z(N_G(P))$ y G sería 7-nilpotente por el teorema de Burnside 5.33. Así pues, $|C_G(g)| = 7$, luego g tiene 24 conjugados, pero hay $8 \cdot 6 = 48$ elementos de orden 7, luego concluimos que G tiene dos clases de conjugación de elementos de orden 7, cada una con 24 elementos.

Más aún, el normalizador de P es el grupo no abeliano de orden 21 dado por el teorema 3.30, en el cual existe un elemento h tal que $g^h = g^2$, por lo que g, g^2, g^4 son conjugados en el normalizador, al igual que g^3, g^5, g^6. Esto significa que si g y g^{-1} fueran conjugados en G, todos los elementos de P serían conjugados en G y, como los subgrupos de Sylow son conjugados, habría una única clase de conjugación de elementos de orden 7. En definitiva, si tomamos a g como representante de una clase de conjugación de elementos de orden 7, un representante de la otra clase es g^{-1}.

Todavía podemos decir algo más: si W es cualquier subgrupo de G de orden 21, tiene necesariamente un subgrupo normal de orden 7 (por 3.30), con lo que es el normalizador de un 7-subgrupo de Sylow, y como los subgrupos de Sylow son conjugados, podemos concluir que todos los subgrupos de G de orden 21 son conjugados.

3-subgrupos de Sylow Veamos ahora que $\nu_3 = 28$. Para ello sólo tenemos que descartar la alternativa $\nu_3 = 7$. Sea P un 7-subgrupo de Sylow y sea $H = N_G(P)$, que es un grupo de orden 21 con un único 7-subgrupo de Sylow. Si tuviera un único 3-subgrupo de Sylow, entonces H sería abeliano y por el teorema de Burnside 5.33 tendríamos que G sería 7-nilpotente. Así pues, el número de 3-subgrupos de Sylow de H es necesariamente 7, lo que significa que H contiene todos los 3-subgrupos de Sylow de G. Pero entonces $N = \bigcap_{g \in G} H^g$ contiene también a todos los 3-subgrupos de Sylow de G, luego $1 \neq N \lhd G$, contradicción. Así pues, $\nu_3 = 28$ y los normalizadores de los 3-subgrupos de Sylow tienen orden 6

Esto implica que G no tiene elementos de orden 6, pues si $g \in G$ tuviera orden 6, entonces $\langle g^2 \rangle$ sería un 3-subgrupo de Sylow, y g estaría en su normalizador (de orden 6), luego el normalizador sería cíclico y el teorema de Burnside nos daría que G es 3-nilpotente. En particular, los normalizadores de los 3-subgrupos de Sylow son isomorfos a Σ_3.

Así, si $P = \langle g \rangle$ es un 3-subgrupo de Sylow, tenemos que g y g^{-1} son conjugados en $N_G(P)$ y, como los subgrupos de Sylow son conjugados, ahora concluimos que G tiene una única clase de conjugación de elementos de orden 3, formada por $28 \cdot 2 = 56$ elementos.

2-subgrupos de Sylow Como G no tiene elementos de orden $6, 14, 21$, todo elemento de G tiene orden $1, 2, 4, 8, 3, 7$, luego tiene que haber $168 - 56 - 48 = 64$ elementos de orden $1, 2, 4, 8$. Esto implica que $\nu_2 = 21$, pues la única alternativa es $\nu_2 = 7$, pero entonces habría a lo sumo $7 \cdot 7 = 49$ elementos de orden $2, 4, 8$. Por lo tanto, los normalizadores de los 2-subgrupos de Sylow tienen orden 8, es decir, que son los propios 2-subgrupos de Sylow.

Si cada par de 2-subgrupos de Sylow tuvieran intersección trivial, habría $21 \cdot 7 = 147$ elementos de orden $2, 4, 8$, cuando tiene que haber 63. Por lo tanto, existen dos 2-subgrupos de Sylow T_1 y T_2 de G tales que $U = T_1 \cap T_2$ no es trivial y tiene el mayor orden posible, que en principio será 2 o 4, pero vamos a ver que es 4. Llamemos $N = N_G(U)$.

Veamos que N no tiene un único 2-subgrupo de Sylow (en particular no es un 2-grupo).

En efecto, sea $N_i = N_{T_i}(U) \leq N$. Por 5.6 tenemos que $U < N_i \leq T_i$ y $U \leq N_1 \cap N_2 \leq T_1 \cap T_2 = U$, luego tiene que ser $N_1 \neq N_2$. Basta ver que N_i es un 2-subgrupo de Sylow de N. En caso contrario, $N_i < P_i$, donde P_i es un 2-subgrupo de Sylow de N. No puede ser que $P_i \leq T_i$, porque $U \lhd P_i$, luego sería $P_i \leq N_{T_i}(U) = N_i$. Por lo tanto, $P_i \leq T_i'$, donde T_i' es un 2-subgrupo de Sylow de G distinto de T_i. Pero $U < N_i \leq T_i \cap T_i'$ contradice la maximalidad del orden de U.

Observemos ahora que N, actúa por conjugación sobre los elementos no triviales de U. Si $|U| = 4$, esto nos da un homomorfismo $N \longrightarrow \Sigma_3$ cuyo núcleo tiene índice divisor de 6, luego si N tiene elementos de orden 7, todos ellos están en el núcleo y conmutan con los elementos de U. Esto es trivialmente cierto si $|U| = 2$, luego si $g \in N$ tiene orden 7 podemos encontrar $u \in U$ de orden 2 de modo que $g^u = g$, lo que significa que u está en el normalizador de un 7-subgrupo de Sylow, pero esto es imposible porque hemos visto que éstos tienen orden 21.

Así pues, el orden de N no es divisible entre 7 y, como no es un 2-grupo, tiene que ser de la forma $|N| = 2^i \cdot 3$, con $i = 2, 3$, y podemos tomar un 3-subgrupo de Sylow P de N (que también lo es de G), luego $N_N(P)$ tiene orden 3 o 6 (porque $N_G(P)$ tiene orden 6), luego tiene índice 2 o 4, pero $\nu_3 = 2$ es imposible, así que N tiene exactamente 4 subgrupos de orden 3.

En la prueba del teorema 3.38 se ve que todo grupo de orden 12 tiene un subgrupo normal de orden 4 o bien un subgrupo normal de orden 3, luego N no puede tener orden 12 y así concluimos que $|N| = 24$. Vamos a probar que $N \cong \Sigma_4$. Para ello consideramos la acción de N por conjugación sobre sus cuatro 3-subgrupos de Sylow. Ésta determina un homomorfismo de grupos $N \longrightarrow \Sigma_4$ y basta probar que su núcleo K es trivial.

Claramente, K es la intersección de los normalizadores de los cuatro 3-subgrupos de Sylow de N, que tienen orden 3 o 6, luego $|K| \mid 6$, pero, por el teorema 3.35, un 3-subgrupo de Sylow P no normaliza a ningún otro, luego P no está contenido en K, luego $|K| \mid 2$. Si K tuviera orden 2, entonces $N/K \cong A_4$, luego N tendría un subgrupo normal de orden 8, cuando no es así. Por lo tanto, $K = 1$, con lo que $N \cong \Sigma_4$ y no tiene subgrupos normales de orden 2, pero sí un único subgrupo normal de orden 4, luego tiene que ser $U \cong C_2 \times C_2$. Además, N contiene un 2-subgrupo de Sylow de G, luego concluimos que los 2-subgrupos de Sylow de G son isomorfos a D_8 (pues así son los de Σ_4).

Esto implica que cada 2-subgrupo de Sylow T contiene exactamente 2 elementos de orden 4, que son conjugados en T y, como los distintos 2-subgrupos de Sylow son conjugados en G, es claro que G tiene una única clase de conjugación de elementos de orden 4. Además, si dos 2-subgrupos de Sylow tienen intersección de orden 4, hemos visto que ésta es de tipo $C_2 \times C_2$, luego cada elemento de orden 4 está en un único subgrupo de Sylow, luego en total hay 42 elementos de orden 4.

Observemos a continuación que un elemento de orden 2 de G no puede conmutar con otro de orden 3 o 7, porque entonces su producto tendría orden 6 o 14, y ya hemos visto que no hay elementos de tales órdenes. Por lo tanto, si T es un 2-subgrupo de Sylow de G y $Z(T) = \langle z \rangle$, entonces $T \leq C_G(z)$, pero $C_G(z)$ no puede tener elementos de orden 3 o 7, luego tiene que ser $C_G(z) = T$, luego z tiene 21 conjugados en G, y son todos los elementos de orden 2, pues G tiene $168 - 1 - 42 - 56 - 48 = 21$ elementos posibles de orden 2.

Así pues, G tiene una única clase de conjugación de elementos de orden 2 (con 21 elementos) y una única clase de conjugación de elementos de orden 4 (con 42 elementos).

Veamos ahora que si W es cualquier subgrupo de G de tipo $C_2 \times C_2$, entonces $N_G(W) \cong \Sigma_4$. Para ello basta probar que W es la intersección de dos 2-subgrupos de Sylow, pues en tal caso ya hemos probado que el normalizador tiene que ser Σ_4.

Sea $W \leq T$, donde $T \cong D_8$ es un 2-subgrupo de Sylow de G. Entonces $W = \langle w, z \rangle$, donde $\langle z \rangle = Z(T)$, y hemos visto que $C_G(z) = T$. Como w y z son conjugados en G, digamos $w = z^g$, se cumple que $T^g = C_G(w)$ es un 2-subgrupo de Sylow de G que tiene a w en su centro, luego $T^g \neq T$ y $W \leq T \cap T^g$, luego $W = T \cap T^g$.

Observemos ahora que un 2-subgrupo de Sylow T tiene exactamente dos subgrupos de tipo $C_2 \times C_2$, digamos U y W. Ambos son normales en T, luego no son conjugados en T. Vamos a ver que[2] tampoco lo son en G. Si fuera $W = U^g$, entonces $W = U^g \lhd T^g$, luego $P, P^g \leq N_G(W)$, y por los teoremas de Sylow existiría $x \in N_G(W)$ tal que $P = P^{gx}$, luego $gx \in N_G(P) = P$ y $U^{gx} = W^x = W$, contradicción.

[2]Más en general, dos subgrupos normales de un p-subgrupo de Sylow T de un grupo G son conjugados en G si y sólo si lo son en $N_G(T)$.

Esto implica que $N_G(U)$ y $N_G(W)$ tampoco son conjugados en G, pues cada uno de ellos (isomorfo a Σ_4) tiene un único subgrupo normal de orden 4 (que será U y W, respectivamente), luego si fueran conjugados, también lo serían U y W. Por lo tanto, G tiene dos clases de conjugación de subgrupos isomorfos a Σ_4, cada una con 7 subgrupos, pues cada uno tiene que ser el normalizador de un subgrupo $C_2 \times C_2$ distinto.

Más aún, todo subgrupo de G de orden 24 está en una de estas dos clases de conjugación, pues el teorema 3.45 nos da que el único grupo de orden 24 que sólo contiene elementos de órdenes $1, 2, 3, 4$ es Σ_4, luego un subgrupo de G de orden 24 contiene un subgrupo normal de tipo $C_2 \times C_2$ y es necesariamente su normalizador, es decir, uno de los grupos de las dos clases de conjugación anteriores.

Por el teorema de Cayley, el hecho de que G posea subgrupos de índice 7 implica que es isomorfo a un subgrupo de A_7.

Por último, todo subgrupo maximal M de G es uno de los grupos de orden 21 o 24 que ya hemos considerado. En efecto, si $7 \mid |M|$, como su índice no puede ser menor que 7, tiene que ser $|M| = 7, 14, 21$, pero los 7-subgrupos de Sylow no son maximales, y no hay subgrupos de orden 14, porque tendrían un 7-subgrupo de Sylow normal, luego su normalizador contendría un elemento de orden 2, y esto no es posible, porque tiene orden 21, luego la única posibilidad en este caso es $|M| = 21$.

Si, por el contrario $7 \nmid M$, las únicas posibilidades son $|M| = 6, 12, 24$ (pues los subgrupos de Sylow no son maximales), pero no puede ser $|M| = 6$ porque entonces M es el normalizador de un 3-subgrupo de Sylow y, como los subgrupos de orden 24 contienen 3-subgrupos de Sylow, conjugando, todo 3-subgrupo de Sylow está contenido en un grupo de orden 24, que contiene a su normalizador. Por último, si $|M| = 12$, entonces, al tener sólo elementos de orden $1, 2, 3, 4$, tiene que ser $M \cong A_4$, con lo que tiene un subgrupo normal $C_2 \times C_2$, luego está contenido en su normalizador, que tiene orden 24.

Resumimos en el teorema siguiente lo que hemos obtenido:

Teorema 5.40 *Si G es un grupo simple de orden $168 = 2^3 \cdot 3 \cdot 7$, entonces:*

1. *$\nu_2 = 21$, $\nu_3 = 7$, $\nu_7 = 8$.*
2. *Los 2-subgrupos de Sylow son de tipo D_8.*
3. *G es isomorfo a un subgrupo de A_7 y no tiene subgrupos de índice ≤ 6.*
4. *Las clases de conjugación de G son:*
   (a) *La clase del elemento neutro.*
   (b) *Dos clases de conjugación con 24 elementos de orden 7 cada una (representadas por cualquier elemento de orden 7 y su inverso).*
   (c) *Una clase de conjugación con 56 elementos de orden 3.*
   (d) *Una clase de conjugación con 42 elementos de orden 4.*
   (e) *Una clase de conjugación con 21 elementos de orden 2.*

5. *Si U y W son los dos subgrupos de tipo V_4 de un 2-subgrupo de Sylow de G, entonces U y W no son conjugados en G y $N_G(U) \cong N_G(W) \cong \Sigma_4$.*

6. *Los subgrupos de G de tipo V_4 forman dos clases de conjugación con 7 subgrupos en cada una.*

7. *Los subgrupos maximales de G forman una clase de conjugación con 8 subgrupos no abelianos de orden 21 y dos clases de conjugación con 7 grupos isomorfos a Σ_4 cada una.*

Naturalmente, este teorema no prueba que existan grupos simples de orden 168, pero nos da información valiosa para encontrar uno.

Concretamente, siguiendo bajo la hipótesis de que existe un grupo simple G de orden 168, llamamos X y L a las dos clases de conjugación de subgrupos de tipo V_4.

La acción de G sobre X por conjugación determina un monomorfismo de grupos $\rho : G \longrightarrow \Sigma_X$, de modo que podemos ver a los elementos de G como permutaciones de un conjunto de siete puntos. Observemos ahora que, dados $P \in X$ y $l \in L$, las afirmaciones siguientes son equivalentes:

1. P y l están contenidos en un 2-subgrupo de Sylow de G, que es necesariamente $T = Pl$.
2. $P \leq N_G(l)$.
3. $l \leq N_G(P)$.

En efecto, si $P, l \leq T$, entonces ambos son normales en T, luego $Pl \leq T$ y necesariamente el producto tiene orden 8, luego $Pl = T$, y claramente se cumplen 2) y 3). Recíprocamente, si se cumple 2) o 3), entonces P, l están contenidos en el normalizador de uno de ellos (que será un subgrupo normal de su normalizador) luego $Pl \leq G$, y obviamente tiene orden 8, luego se cumple 1).

Escribiremos $P \sim l$ para indicar que se cumplen las propiedades anteriores, y observamos que se cumplen las propiedades siguientes:

1. *Para cada $l \in L$ existen exactamente tres puntos $P \in X$ tales que $P \sim l$.*

   En efecto, sabemos que $N_G(l) \cong \Sigma_4$, por lo que contiene exactamente tres 2-subgrupos de Sylow, cada uno de los cuales contiene a l (el único subgrupo de Klein normal) y a un $P \in X$ distinto en cada caso, luego hay exactamente 3 elementos en X relacionados con l.

   Por simetría tenemos también:

2. *Para cada $P \in X$ existen exactamente tres $l \in L$ tales que $P \sim l$.*

3. *Para cada par de puntos distintos $P, P' \in X$, existe un único $l \in L$ tal que $P \sim l$, $P' \sim l$.*

   En efecto, veamos en primer lugar que P y P' están relacionados a lo sumo con un $l \in L$. Esto se debe a que si $P \sim l$ y $P' \sim l$, entonces

$P, P' \leq N_G(l)$, pero dos subgrupos de Klein no normales en Σ_4 generan todo Σ_4 (pues el subgrupo generado tiene que tener orden múltiplo de 4, pero no puede ser 4 ni 8, ni tampoco 12, porque entonces sería A_4, pero contiene trasposiciones, luego tiene que tener orden 24), luego ha de ser necesariamente $l = \langle P, P' \rangle$.

Ahora, dado $P \in X$, existen tres elementos $l_1, l_2, l_3 \in L$ tales que $P \sim l_i$. Para cada l_i existen dos puntos $P_{i1}, P_{i2} \in X$ distintos de P y distintos entre sí de modo que

$$P \sim l_i, \qquad P_{i1} \sim l_i, \qquad P_{i2} \sim l_i.$$

Pero los seis puntos P_{ij} son distintos entre sí dos a dos, ya que si fuera $P_{ij} = P_{i'j'}$, entonces $i \neq i'$ y tendríamos dos elementos $l_i, l_{i'} \in L$ tales que

$$P \sim l, l_i, \qquad P_{ij} \sim l, l_{i'},$$

en contra de la unicidad que hemos probado.

Por lo tanto, los P_{ij} son todos los puntos de X distintos de P, y uno de ellos es P', luego existe un $l \in L$ tal que $P \sim l$, $P' \sim l$.

Por simetría tenemos también:

4. *Para cada par de elementos $l, l' \in L$ existe un único $P \in X$ tal que $P \sim l$, $P \sim l'$.*

Estos hechos se enuncian más naturalmente si llamamos "puntos" a los elementos de X y "rectas" a los elementos de L, y leemos $P \sim l$ como que el punto P está en la recta l o que la recta l pasa por el punto P. Así, tenemos 7 puntos y 7 rectas, y en estos términos tenemos:

P1 *Por cada par de puntos distintos pasa una única recta.*

P2 *Cada par de rectas distintas se cortan en un único punto.*

P3 *Existen tres puntos que no están sobre la misma recta.*

P4 *Cada recta contiene exactamente tres puntos.*

Así pues, los puntos y las rectas que hemos definido (o que G define) cumplen los axiomas que definen un plano proyectivo, enunciados al principio de la sección [G 9.1]. Más precisamente, forman un plano proyectivo de orden 2 en el sentido de la definición [G 9.80], por lo que se trata concretamente del plano de Fano descrito a continuación (el único plano proyectivo de orden 2).

Más aún, las permutaciones de X definidas por la acción $\rho : G \longrightarrow \Sigma_X$ por conjugación no son meras permutaciones, sino que son colineaciones (transforman puntos colineales en puntos colineales). En efecto, que tres puntos P_1, P_2, P_3 sean colineales significa que existe una recta l tal que $P_i \leq N_G(l)$, y entonces, si $g \in G$, tenemos que $P_i^g \leq N_G(l^g)$, luego las imágenes de los tres puntos son también colineales.

Teniendo en cuenta que el cuerpo k de dos elementos no tiene automorfismos distintos de la identidad, el teorema fundamental de la geometría proyectiva [G 9.27] afirma que las colineaciones del plano de Fano coinciden con sus homografías, es decir, que el grupo de las colineaciones es el grupo

$$\mathrm{LGP}(3,2) \cong \mathrm{LG}(3,2)/Z(\mathrm{LG}(3,2)),$$

pero, según [Al 4.39], el centro del grupo $\mathrm{LG}(3,2)$ de las matrices regulares 3×3 sobre el cuerpo k de 2 elementos está formado por las matrices de la forma uI, donde $u \in k$ es no nulo (luego es $u = 1$) e I es la matriz identidad. Así pues, $Z(\mathrm{LG}(3,2)) = 1$ y tenemos que el grupo de homografías $\mathrm{LGP}(3,2)$ del plano de Fano no es sino $\mathrm{LG}(3,2)$, que es isomorfo al grupo de los automorfismos de un espacio vectorial V de dimensión 3 sobre k.

Como cada automorfismo está determinado por la imagen de una base (ordenada), vemos que hay tantos automorfismos como bases, y para calcular el número de bases observamos que la imagen del primer vector de una base prefijada puede ser cualquiera de los $8-1$ vectores no nulos de V, y la imagen del segundo vector puede ser cualquiera de los $8-2$ vectores que no están en el subespacio generado por la imagen del primero, mientras que la imagen del tercero puede ser cualquiera de los $8-4$ vectores que no están en el subespacio generado por las imágenes de los dos primeros. Así:

$$|\mathrm{LG}(3,2)| = 7\cdot 6\cdot 4 = 168.$$

Concluimos que $\rho : G \longrightarrow \mathrm{LG}(3,2)$ es un isomorfismo de grupos. Con eso casi hemos demostrado el teorema siguiente:

Teorema 5.41 *El grupo* $\mathrm{LG}(3,2)$ *es, salvo isomorfismo, el único simple de orden* 168*.*

Demostración: Hemos demostrado que si existe un grupo simple de orden 168 tiene que ser isomorfo a $G = \mathrm{LG}(3,2)$, pero falta probar que realmente este grupo es simple.

Supongamos que $N \lhd G$ es un subgrupo normal propio. Consideramos la acción de G sobre el plano de Fano P y llamamos H al estabilizador de un punto. Como la acción es claramente transitiva, tenemos que $|G : H| = 7$. Los conjugados de H son los estabilizadores de los distintos puntos de P, luego la intersección de todos ellos es trivial (el único elemento de G que fija a todos los puntos es la identidad). Por lo tanto $N \not\leq H$ (o de lo contrario N estaría en dicha intersección). Por consiguiente, $G = NH$. Como $|N : N\cap H| = |NH : H| = 7$, tenemos que $7 \mid |N|$.

Podemos considerar que $G \leq \Sigma_7$, y los 7-subgrupos de Sylow de Σ_7 son los subgrupos generados por los 7-ciclos, de los que hay un total de 6! que forman 5! subgrupos de Sylow, luego sus normalizadores tienen orden $7!/5! = 42$. Así, si P es un 7-subgrupo de Sylow de G, también lo es de Σ_7 y $N_G(P) \leq N_{\Sigma_7}(P)$, luego $|N_G(P)| \mid 42$, luego los 7-subgrupos de Sylow de G no son normales. La teoría de Sylow nos da entonces que $\nu_7 = 8$.

Si N tuviera un 7-subgrupo de Sylow normal, sería característico en N, luego normal en G. Así pues, N tampoco tiene 7-subgrupos de Sylow normales. Pero el número de 7-subgrupos de Sylow de N tiene que ser menor o igual que 8, y también congruente con 1 módulo 7, luego N contiene a todos los 7-subgrupos de Sylow de G. Esto implica que $8 \mid |N|$, luego $56 \mid |N|$. Como N es un subgrupo propio, tiene que ser $|N| = 56$.

Como N tiene 8 subgrupos de Sylow de orden 7, tiene 48 elementos de orden 7, luego tiene 8 elementos de otros órdenes, luego sólo puede tener un 2-subgrupo de Sylow, que será característico en N, luego normal en G, y será de hecho un 2-subgrupo de Sylow normal en G. Pero esto es imposible, porque hemos probado que todo subgrupo normal propio de G tiene que tener orden 56. ∎

Así pues, ya conocemos los tres grupos simples no abelianos de menor orden: $A_5, \mathrm{LG}(3,2)$ y A_6, de órdenes $60, 168, 360$, respectivamente.

5.5 El subgrupo de Frattini

Introducimos ahora un concepto útil para estudiar los grupos nilpotentes y, especialmente, los p-grupos, para los cuales la teoría de Sylow se vuelve trivial.

Definición 5.42 Un subgrupo M de un grupo G es *maximal* si $M < G$ y no existen grupos intermedios $M < H < G$.

Obviamente, todo grupo finito no trivial tiene subgrupos maximales.

El *subgrupo de Frattini* de un grupo G es la intersección de todos los subgrupos maximales de G. Se representa por $\Phi(G)$ y claramente es un subgrupo característico en G.

Si un grupo G no tiene subgrupos maximales, el convenio usual es tomar $\Phi(G) = G$, aunque vamos a considerar únicamente grupos finitos, así que el único caso en el que esta observación será relevante para nosotros es el convenio de que $\Phi(1) = 1$.

Observemos que si $N \lhd G$, se cumple que N es maximal en G si y sólo si $|G : N|$ es primo, pues la maximalidad equivale a que el grupo G/N no tenga subgrupos, y esto sólo puede suceder si G/N es cíclico de orden primo.

Esto ya no es cierto para subgrupos que no son normales. Por ejemplo, los 3-subgrupos de Sylow de A_4 son maximales, ya que A_4 no tiene subgrupos de orden 6, pero su índice es 4.

Ahora podemos dar más caracterizaciones de los grupos nilpotentes:

Teorema 5.43 *Si G es un grupo finito no trivial, las afirmaciones siguientes son equivalentes:*

1. *G es nilpotente.*

2. *Si $H < G$, entonces $H < N_G(H)$.*

3. *Todos los subgrupos maximales de G son normales.*

4. $G' \leq \Phi(G)$.

DEMOSTRACIÓN: 1) $\Rightarrow$ 2) es el teorema 5.6.

2) $\Rightarrow$ 3) es evidente: si $H < G$ es maximal, entonces $H < N_G(H) \leq G$ implica que $N_G(H) = G$, luego $H \lhd G$.

3) $\Rightarrow$ 4) Si $M < G$ es un subgrupo maximal, entonces $M \lhd G$, luego G/M es cíclico de orden primo, luego $G' \leq M$, y si G' está contenido en todos los subgrupos maximales, lo está en su intersección $\Phi(G)$.

4) $\Rightarrow$ 3) Si M es un subgrupo maximal de G, entonces $G' \leq \Phi(G) \leq M$, luego $M/G' \lhd G/G'$, luego $M \lhd G$.

3) $\Rightarrow$ 1) Si P es un p-subgrupo de Sylow de G y se cumple $N_G(P) < G$, entonces existe un subgrupo maximal $N_G(P) \leq M \lhd G$, y por el argumento de Frattini 3.37, concluimos que $G = MN_G(P) = M$, contradicción. Por lo tanto, los subgrupos de Sylow de G son normales, y eso implica que G es nilpotente, por 5.7. ∎

Veamos algunas propiedades del subgrupo de Frattini:

Teorema 5.44 *Si G es un grupo finito y $K \trianglelefteq G$, entonces $K \leq \Phi(G)$ si y sólo si no existe $H < G$ tal que $HK = G$.*

DEMOSTRACIÓN: Si $K \leq \Phi(G)$ y $H < G$, existe un subgrupo maximal $H \leq M < G$, luego $K \leq \Phi(G) \leq M$, luego $HK \leq M < G$.

Recíprocamente, si $K \not\leq \Phi(G)$, entonces $G \neq 1$ y existe un subgrupo maximal $M < G$ tal que $K \not\leq M$, luego $M < MK \leq G$, pero la maximalidad de M implica que $MK = G$. ∎

Teorema 5.45 (Frattini) *Si G es un grupo finito, entonces $\Phi(G)$ es un grupo nilpotente.*

DEMOSTRACIÓN: Sea P un p-subgrupo de Sylow de $\Phi(G)$. El argumento de Frattini 3.37 nos da que $G = N_G(P)\Phi(G)$, luego el teorema anterior implica que $G = N_G(P)$, luego $P \trianglelefteq G$ y en particular $P \trianglelefteq \Phi(G)$. Así, todos los subgrupos de Sylow de $\Phi(G)$ son normales, luego 5.7 nos da que $\Phi(G)$ es nilpotente. ∎

Teorema 5.46 *Si $K \lhd G$, entonces $\Phi(G)K/K \leq \Phi(G/K)$ y si $K \leq \Phi(G)$ entonces $\Phi(G/K) = \Phi(G)/K$.*

DEMOSTRACIÓN: Es claro que todo subgrupo maximal de G/K es de la forma M/K, donde M es un subgrupo maximal de M que contiene a K. Como $\Phi(G) \leq M$, tenemos que $\Phi(G)K \leq M$, luego $\Phi(G)K/K \leq M/K$, luego $\Phi(G)K/K \leq \Phi(G/K)$.

Si suponemos además que $K \leq \Phi(G)$ y $\Phi(G/K) = F/K$, para cada subgrupo maximal $M < G$, tenemos que $K \leq \Phi(K) \leq M$, luego M/K es un subgrupo maximal de G/K, luego $\Phi(G/K) = F/K \leq M/K$, luego $F \leq M$ y, como esto vale para todo M, tiene que ser $F \leq \Phi(M)$, luego $\Phi(G/K) = F/K \leq \Phi(G)/K$. ∎

Ejemplo No es necesariamente cierto que $\Phi(G/K) = \Phi(G)K/K$. Consideremos por ejemplo $K = C_5$ y $M = \mathrm{Aut}(K) \cong C_4$, con lo que podemos formar el producto semidirecto $G = M[K]$, de orden 20. Pongamos que $K = \langle a\rangle$, $M = \langle b\rangle$, donde b es el automorfismo dado por $b(a) = a^2$. Equivalentemente, tenemos que $a^b = a^2$, o también, conjugando con b^{-1}, se cumple que $ba = a^3b$. Esto nos permite expresar cada elemento de G de forma única como a^ib^j, para $i = 0, 1, 2, 3, 4$, $j = 0, 1, 2, 3$.

Entonces $M = \{1, b, b^2, b^3\}$, pero otro subgrupo de orden 4 (luego también maximal) es $M^* = \{1, ab, a^4b^2, a^3b^3\}$, y vemos que $\Phi(G) \leq M \cap M^* = 1$, luego $\Phi(G) = 1$.

Sin embargo, $G/K \cong C_4$ y tiene un único subgrupo maximal C_2, luego $\Phi(G/K) \cong C_2$ y no coincide con $\Phi(G)K/K = 1$. ∎

El teorema siguiente permite reconocer con facilidad el subgrupo de Frattini de un p-grupo:

Teorema 5.47 *Si G es un p-grupo, entonces $\Phi(G)$ es el menor subgrupo normal K de G cuyo cociente G/K es abeliano elemental.*

Demostración: Basta probar que $\Phi(G) = 1$ si y sólo si G es abeliano elemental. En efecto, admitiendo esto, $\Phi(G/\Phi(G)) = 1$ por el teorema anterior, luego $G/\Phi(G)$ es abeliano elemental y, si $K \trianglelefteq G$ tiene cociente G/K abeliano elemental, entonces $\Phi(G)K/K \leq \Phi(G/K) = 1$, luego $\Phi(G) \leq K$.

Podemos suponer que $G \neq 1$. Si G es abeliano elemental, entonces es característicamente simple por 4.15, pero $\Phi(G) < G$ es un subgrupo característico, así que tiene que ser $\Phi(G) = 1$.

Recíprocamente, si $\Phi(G) = 1$, como G es nilpotente, el teorema 5.43 nos da que $G' \leq \Phi(G) = 1$, luego G es abeliano. Si $M < G$ es un subgrupo maximal, por el mismo teorema sabemos que $M \lhd G$, y $G/M \cong C_p$, luego todo $g \in G$ cumple que $g^p \in M$, y como esto vale para todo subgrupo maximal M, tenemos que $g^p \in \Phi(G) = 1$, luego todos los elementos no triviales de G tienen orden p. Esto implica que G es abeliano elemental. ∎

Por ejemplo, ahora es inmediato que $\Phi(Q_8)$ es su único subgrupo de orden 2, pues tiene cociente $C_2 \times C_2$ y no puede ser $\Phi(Q_8) = 1$. Similarmente concluimos que $\Phi(D_8) = D_8' = Z(D_8)$.

Para subgrupos tenemos el teorema siguiente:

Teorema 5.48 *Si $K \trianglelefteq G$, entonces $\Phi(K) \leq \Phi(G)$. Más en general, si $H \leq G$ y $K \leq \Phi(H)$, entonces $K \leq \Phi(G)$.*

DEMOSTRACIÓN: La primera afirmación se obtiene de aplicar la segunda con $\Phi(K)$ en lugar de K y K en lugar de H. (Notemos que $\Phi(K)$ es característico en K, luego normal en G).

Para la segunda, supongamos que $K \not\leq \Phi(G)$. Entonces, por 5.44, existe $J < G$ tal que $G = JK$. Tenemos que $K \leq H \leq JK = G$, luego la identidad de Dedekind 4.22 nos da que $H = H \cap KJ = K(H \cap J)$. Pero $K \leq \Phi(H)$, luego el teorema 5.44 implica que $H = H \cap J$, con lo que $K \leq H \leq J$, luego $G = JK = J$, contradicción. Así pues, $K \leq \Phi(G)$. ∎

Con esto podemos probar:

Teorema 5.49 *Si G y H son dos grupos finitos, entonces*

$$\Phi(G \times H) = \Phi(G) \times \Phi(H).$$

DEMOSTRACIÓN: Podemos suponer que G y H no son triviales. Consideremos un subgrupo maximal $G \leq M < G \times H$. Entonces, por la identidad de Dedekind 4.22, se cumple

$$M = M \cap GH = G(M \cap H)$$

y $M^* = M \cap H$ es un subgrupo maximal de H, pues si existiera un subgrupo $M^* < N < H$, entonces $M = G \times M^* < G \times N < G \times H$ y M no sería maximal. Por lo tanto, $\Phi(H) \leq M^*$ y $G \times \Phi(H) \leq G \times M^* = M$. Más aún, tenemos que $G \times \Phi(H)$ es la intersección de todos los subgrupos maximales de $G \times H$ que contienen a G. Similarmente, $\Phi(G) \times H$ es la intersección de los subgrupos maximales de $G \times H$ que contienen a H, luego

$$\Phi(G) \times \Phi(H) = (\Phi(G) \times H) \cap (G \times \Phi(H))$$

es la intersección de todos los subgrupos maximales de $G \times H$ que contienen a G o a H. Esto implica que $\Phi(G \times H) \leq \Phi(G) \times \Phi(H)$.

Por otra parte, por el teorema anterior, $\Phi(G), \Phi(H) \leq \Phi(G \times H)$, luego también $\Phi(G) \times \Phi(H) \leq \Phi(G \times H)$. ∎

El teorema 5.44 puede expresarse de una forma más clara:

Teorema 5.50 *Si $G = \langle X \rangle$ es un grupo finito y $x \in X \cap \Phi(G)$, entonces el conjunto $X \setminus \{x\}$ es también un sistema generador de G.*

DEMOSTRACIÓN: Sea $X^* = X \setminus \{x\}$ y sean $K = \langle x \rangle \leq \Phi(G)$, $H = \langle X' \rangle \leq G$. Entonces $X \subset HK$, luego $G = HK$, luego 5.44 nos da que $G = H$. ∎

En otros términos, los elementos de $\Phi(G)$ son los elementos que se pueden eliminar de cualquier sistema generador de G sin que deje de serlo. El en caso de los p-grupos podemos precisar mucho más esta idea.

Definición 5.51 Si G es un grupo finito, un *generador minimal* de G es un sistema generador X tal que ningún subconjunto propio de X es sistema generador.

Podemos pensar en los generadores minimales como el concepto análogo al de base de un espacio vectorial, pero hay que tener en cuenta que incluso un grupo abeliano puede tener generadores minimales con diferente número de elementos. Por ejemplo, si $G = \langle g \rangle \cong C_6$, tenemos que $\{x\}$ y $\{x^2, x^3\}$ son ambos generadores minimales de G. Sin embargo, vamos a ver que esto no sucede en los p-grupos:

Teorema 5.52 (Teorema de la base de Burnside) *Sea G un p-grupo no trivial, sea $\bar{G} = G/\Phi(G)$ y pongamos que $|\bar{G}| = p^d$. Si $\{x_1\Phi(G), \dots, x_d\Phi(G)\}$ es una base de $\bar{G}$ como espacio vectorial sobre $k = \mathbb{Z}/p\mathbb{Z}$, entonces $\{x_1, \dots, x_d\}$ es un generador minimal de G y, recíprocamente, si X es un generador minimal de G, entonces $|X| = d$ y las clases de sus elementos forman una base de $\bar{G}$.*

Demostración: Notemos que $\bar{G}$ es abeliano elemental, por lo que tiene sentido considerarlo como espacio vectorial sobre k. Como $|\bar{G}| = p^d$, su dimensión es obviamente d.

Observemos ahora que un conjunto $X \subset G$ genera G si y sólo si las clases de sus elementos módulo $\Phi(G)$ generan $\bar{G}$. Una implicación es obvia y, si las clases de X generan $\bar{G}$, sea $H = \langle X \rangle$, de modo que $\bar{G} = H\Phi(G)/\Phi(G)$, luego $G = H\Phi(G)$, luego $G = H$ por 5.44.

Por consiguiente, si $X = \{x_1, \dots, x_m\}$ es un generador minimal de G, ninguno de sus subconjuntos propios es un generador, luego $\{x_1\Phi(G), \dots, x_m\Phi(G)\}$ es un sistema generador de $\bar{G}$ cuyos subconjuntos propios no lo son, luego es una base y en particular $m = d$. Recíprocamente, si $\{x_1\Phi(G), \dots, x_d\Phi(G)\}$ es una base de $\bar{G}$, sabemos que $\{x_1, \dots, x_d\}$ es un generador de G y ningún subconjunto suyo puede serlo, luego es un generador minimal. ∎

Como aplicación vamos a dar una cota inferior al número de grupos de orden p^n. Necesitamos algunas propiedades elementales de los conmutadores:

Teorema 5.53 *En todo grupo se cumplen las relaciones siguientes, donde definimos $[x, y, z] = [[x, y], z]$:*

1. $[xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z]$.
2. $[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z]$.
3. *Si $[x, y]$ conmuta con x y con y, entonces $[x, y^n] = [x^n, y] = [x, y]^n$.*

Demostración: 1) y 2) se demuestran sin más que desarrollar cada término y comprobar que todos llevan a la misma expresión. Por ejemplo:

$$[xy, z] = y^{-1}x^{-1}z^{-1}xyz,$$

y las otras dos expresiones de 1) llevan al mismo resultado. Las igualdades de 3) se prueban por inducción sobre n. Se cumplen claramente para $n = 0, 1$ y, si valen para n, por 2) tenemos

$$[x, y^{n+1}] = [x, y^n][x, y][x, y, y^n] = [x, y]^n[x, y] = [x, y]^{n+1},$$

donde hemos usado que $[x, y]$ conmuta con y, luego con y^n, luego $[x, y, y^n] = 1$. ∎

Ahora vamos a definir una familia de p-grupos. Partimos de un grupo libre $L_r = \langle y_1, \dots, y_r \rangle$ de rango r y de un primo p, y consideramos en él el subgrupo N generado por todos los elementos de cualquiera de las formas

$$x^{p^2}, \qquad [x,y]^p, \qquad [x,yz].$$

Como la imagen de cualquiera de estos generadores por un automorfismo es otro elemento de la misma forma, concluimos que N es un subgrupo característico de L_r, en particular normal, por lo que podemos definir el cociente $G_r = L_r/N$. Llamando $x_i = y_i N$, tenemos que $G_r = \langle x_1, \dots, x_r \rangle$ y es un grupo con la propiedad de que, para cualesquiera de sus elementos x, y, z, se cumle que

$$x^{p^2} = 1, \qquad [x,y]^p = 1, \qquad [x,y,z] = 1.$$

La última relación equivale a que todo conmutador $[x,y]$ conmuta con todo elemento de G_r o, equivalentemente, a que $G_r' \leq Z(G_r)$. En particular, como $[x,y]$ conmuta con x y con y, el teorema anterior nos da que $[x^p, y] = [x,y]^p = 1$, luego $x^p \in Z(G_r)$.

En otros términos, si llamamos G_r^p al subgrupo de G_r generado por todas las potencias p-ésimas, tenemos que $G_r^p \leq Z(G_r)$, luego $G_r' G_r^p \leq Z(G_r)$.

En principio, el subgrupo $G_r' G_r^p$ está generado por todos los elementos de la forma $[x,y]$, x^p, con $x, y \in G_r$, pero vamos a ver que admite el generador finito formado por los elementos $[x_i, x_j]$, x_i^p.

En efecto, como todo elemento de G_r tiene orden finito (divisor de p^2), se puede expresar como producto de generadores $x_1, \dots, x_r$ (sin necesidad de considerar sus inversos). Entonces, las relaciones 1) y 2) del teorema anterior (teniendo en cuenta que $[x,y,z] = 1$), permiten descomponer cualquier conmutador $[x,y]$ en producto de conmutadores $[x_i, x_j]$, mientras que la relación

$$(xy)^n = x^n y^n [y,x]^{n(n-1)/2}$$

(que consideramos ya en la prueba del teorema 3.22), aplicada al exponente p, nos permite expresar cualquier potencia p-ésima de un elemento de G en producto de potencias x_i^p y de conmutadores, que a su vez se expresan como producto de conmutadores $[x_i, x_j]$.

Así pues, $G_r' G_r^p$ es un grupo abeliano generado por un número finito de elementos de orden finito, luego es un grupo finito. Más aún, todos sus generadores tienen orden p, pues $(x^p)^p = 1$ y $[x,y]^p = 1$, luego se trata de un p-grupo abeliano elemental.

Igualmente, el cociente $G_r/G_r' G_r^p$ es abeliano (porque $G_r' \leq G_r' G_r^p$) y finitamente generado, luego también es finito, y todos sus elementos no triviales tienen orden p, luego también es un p-grupo abeliano elemental.

Concluimos que G_r también es finito y es un p-grupo. Como $G_r/G_r' G_r^p$ es abeliano elemental, tiene que ser $\Phi(G_r) \leq G_r' G_r^p$ (por 5.47) y, como $G_r/\Phi(G_r)$ es abeliano elemental también se cumple que $G_r' \leq \Phi(G_r)$ y que $G_r^p \leq \Phi(G_r)$, luego de hecho $\Phi(G_r) = G_r' G_r^p$.

Definición 5.54 Si p es un número primo, llamaremos $\mathfrak{X}_p$ a la clase de todos los p-grupos G que tienen un subgrupo $H \leq Z(G)$ de modo que H y G/H son abelianos elementales.

Hemos demostrado que los grupos finitos G_r están en la clase $\mathfrak{X}_p$, y el teorema siguiente muestra que son "los más generales":

Teorema 5.55 *Si $G \in \mathfrak{X}_p$ y $g_1, \ldots, g_r \in G$, existe un único homomorfismo de grupos $\phi : G_r \longrightarrow G$ tal que $\phi(x_i) = g_i$.*

Demostración: Sea $L_r = \langle y_1, \ldots, y_r \rangle$ un grupo libre de rango r. Por definición de grupo libre existe un homomorfismo de grupos $\phi_0 : L_r \longrightarrow G$ tal que $\phi(y_i) = g_i$. Sea $H \leq Z(G)$ tal que H y G/H sean abelianos elementales. Entonces, como G/H es abeliano elemental, todo $x \in G$ cumple $x^p \in H$ y si $x, y \in G$ se cumple que $[x, y] \in H$. A su vez, como H es abeliano elemental, $x^{p^2} = 1$ y $[x, y]^p = 1$. Por último, como $H \leq Z(G)$ y $[x, y] \in H$, se cumple también que $[x, y, z] = 1$. Por lo tanto, si $x, y, z \in L_r$, tenemos que

$$\phi_0(x^{p^2}) = \phi_0(x)^{p^2} = 1, \quad \phi_0([x, y]^p) = [\phi_0(x), \phi_0(y)]^p = 1,$$

$$\phi_0([x, y, z]) = [\phi_0(x), \phi_0(y), \phi_0(z)] = 1$$

En otras palabras, $x^{p^2}, [x, y]^p, [x, y, z] \in \mathrm{N}(\phi_0)$, luego, si $N \leq L_r$ es el subgrupo generado por los elementos de estas tres formas, se cumple que $N \leq \mathrm{N}(\phi_0)$, luego ϕ_0 define un homomorfismo $\phi : X_r \longrightarrow G$ que cumple $\phi(x_i) = g_i$. Como los elementos $x_1, \ldots, x_r$ son un sistema generador de G_r, es obvio que ϕ es único. ∎

Así pues, todo grupo $G \in \mathfrak{X}_p$ puede expresarse como cociente de G_r, donde r es el número de elementos de un generador de G. De aquí vamos a deducir más propiedades de los grupos G_r.

Para empezar, vamos a probar que los elementos x_i^p, $[x_i, x_j]$ (para $i < j$) forman un generador minimal de $\Phi(G_r)$. Esto equivale a que sean una base de $\Phi(G_r)$ como espacio vectorial sobre $k = \mathbb{Z}/p\mathbb{Z}$. Ya sabemos que son un sistema generador, por lo que sólo tenemos que probar que son linealmente independientes. Teniendo en cuenta que estamos empleando notación multiplicativa, esto equivale a que si

$$\prod_{i=1}^{r} x_i^{pa_i} \prod_{i<j} [x_i, x_j]^{b_{ij}} = 1,$$

donde $0 \leq a_i, b_{ij} < p$, entonces $a_i, b_{ij} = 0$.

En efecto, consideremos un grupo cíclico $G = \langle g \rangle \cong C_{p^2}$. Claramente está en $\mathfrak{X}_p$, pues tiene un subgrupo C_p que es abeliano elemental y da lugar a un cociente abeliano elemental. Por lo tanto, para cada índice $1 \leq k \leq r$, existe un homomorfismo $\phi_k : G_r \longrightarrow G$ que cumple $\phi_k(x_k) = g$ y $\phi_k(x_i) = 1$ si $i \neq k$. Al aplicar este homomorfismo a la combinación lineal anterior, obtenemos que $g^{pa_k} = 1$ y como $o(g) = p^2$, tiene que ser $a_k = 0$.

Ahora consideramos el segundo grupo no abeliano de orden p^3 descrito en el teorema 3.22. Según se ve en la demostración, es de la forma $G = \langle x, y\rangle$, donde ambos generadores tienen orden p y $z = [x, y]$ también tiene orden p y genera $Z(G)$. Como $Z(G) \cong C_p$ es abeliano elemental y $G/Z(G) \cong C_p \times C_p$ también lo es, vemos que $G \in \mathfrak{X}_p$, luego, para $i < j$, el teorema anterior nos da un homomorfismo $\phi_{ij} : G_r \longrightarrow G$ tal que $\phi(x_i) = x$, $\phi(x_j) = y$ y $\phi(x_k) = 1$ para todo $k \neq i, j$. Al aplicar este homomorfismo a la combinación lineal obtenemos $[x, y]^{b_{ij}} = 1$, de donde se sigue que $b_{ij} = 0$.

Con esto tenemos que $|\Phi(G_r)| = p^{r+r(r-1)/2} = p^{r(r+1)/2}$ (el exponente es el cardinal de la base que hemos encontrado).

Por otro lado, si G es un p-grupo elemental abeliano de dimensión r, claramente $G \in \mathfrak{X}_p$ (tomando, por ejemplo, $H = G$), luego existe un homomorfismo $\phi : G_r \longrightarrow G$ que transforma el generador de G_r en una base de G. Esto implica que $x_1, \ldots x_r$ es un generador minimal de G_r, pues si un subconjunto propio fuera generador, su imagen en G sería un generador de G con menos de r elementos, pero eso es imposible, pues G es un espacio vectorial de dimensión r.

Como consecuencia, el teorema 5.52 nos da que $|G_r : \Phi/G_r)| = p^r$. Resumimos en un teorema lo que hemos probado hasta ahora:

Teorema 5.56 *Para cada número natural $r > 0$ y cada primo p, el grupo G_r cumple lo siguiente:*

1. $|G| = p^{r+r(r+1)/2}$.
2. $\Phi(G_r)$ *es abeliano elemental y* $|\phi(G_r)| = p^{r(r+1)/2}$.
3. $|G_r/\Phi(G_r)| = p^r$.
4. $\Phi(G_r) \leq Z(G_r)$.

Necesitamos una última propiedad de estos grupos. Como $\phi(G_r)$ es un subgrupo característico, todo $\alpha \in \mathrm{Aut}(G_r)$ cumple $\alpha[\Phi(G_r)] = \Phi(G_r)$, luego induce un automorfismo $\bar{\alpha} : G_r/\Phi(G_r) \longrightarrow G_r/\Phi(G_r)$.

Teorema 5.57 *Si $\alpha \in \mathrm{Aut}(G_r)$ induce la identidad en $G_r/\Phi(G_r)$, entonces α fija a todos los elementos de $\Phi(G_r)$.*

Demostración: Tenemos que $\alpha(x_i)\Phi(G_r) = x_i\Phi(G_r)$, lo que significa que existe un $h_i \in \Phi(G_r)$ tal que $\alpha(x_i) = x_i h_i$. Notemos que $h_i \in \Phi(G_r) \leq Z(G_r)$. Por lo tanto $\alpha(x_i^p) = x_i^p h_i^p = x_i^p$, pues todos los elementos no triviales de $\Phi(G_r)$ tienen orden p. Por otro lado, $\alpha([x_i, x_j]) = [x_i h_i, x_j h_j] = [x_i, x_j]$ y así α fija a todos los generadores de $\Phi(G_r)$, luego fija a cada elemento de $\Phi(G_r)$. ∎

Hemos visto que los grupos G_r cumplen la definición de grupo libre restringida a grupos de la clase $\mathfrak{X}_r$, de modo que un cociente G_r/N puede verse como una presentación de un grupo mediante generadores y relaciones. Lo que vamos a hacer es dar una cota inferior del número de grupos de orden p^n que pueden expresarse de esta forma, para lo cual necesitamos saber cuándo dos subgrupos N dan lugar a cocientes isomorfos:

Teorema 5.58 *Si $N_1, N_2 \leq \Phi(G_r)$, entonces $G_r/N_1 \cong G_r/N_2$ si y sólo si existe $\alpha \in \mathrm{Aut}(G_r)$ tal que $\alpha[N_1] = N_2$.*

Demostración: Una implicación es inmediata. Supongamos que existe un isomorfismo $\alpha' : G_r/N_1 \longrightarrow G_r/N_2$. Pongamos que $\alpha'(x_iN_1) = y_iN_2$. Entonces las clases y_iN_2 generan G_r/N_2, luego $G_r = \langle y_1, \ldots, y_r, N_2\rangle$, pero, teniendo en cuenta que $N_2 \leq \Phi(G_r)$, el teorema 5.50 nos da que, en realidad, se cumple $G_r = \langle y_1, \ldots, y_r\rangle$.

Por otra parte, el teorema 5.55 nos da un homomorfismo $\alpha : G_r \longrightarrow G_r$ tal que $\alpha(x_i) = y_i$, que es suprayectivo (porque los y_i generan G_r) luego, tratándose de un grupo finito, de hecho α es biyectivo, es decir, $\alpha \in \mathrm{Aut}(G_r)$.

Tenemos, pues la situación siguiente:

$$\begin{array}{ccc} G_r & \xrightarrow{\alpha} & G_r \\ \downarrow & & \downarrow \\ G_r/N_1 & \xrightarrow[\alpha']{} & G_r/N_2 \end{array}$$

de modo que la imagen de cada generador $x_i \in G_r$ por α seguida de la proyección en el cociente es la misma que la imagen por α' de la proyección en el cociente. Como esto vale para todos los generadores de G_r, de hecho vale para todos los elementos de G_r, es decir, tenemos que

$$\alpha(x)N_2 = \alpha'(xN_1).$$

En particular, si $x \in N_1$, esto implica que $\alpha(x) \in N_2$, luego $\alpha[N_1] \subset N_2$, e igualmente, si $\alpha(x) \in N_2$, tiene que ser $\alpha'(xN_1) = 1$, luego $xN_1 = 1$, luego $x \in N_1$, lo que significa que $\alpha[N_1] = N_2$. ∎

Ahora ya podemos contar grupos. El resultado central es el siguiente:

Teorema 5.59 *Si $1 \leq s \leq r(r+1)/2$, hay al menos $p^{sr(r+1)/2-r^2-s^2}$ grupos de orden p^{r+s} no isomorfos dos a dos.*

Demostración: Sea Ω el conjunto de todos los subgrupos $N \leq \Phi(G_r)$ tales que $|\Phi(G_r) : N| = p^s$ y $|G_r/N| = p^{r+s}$. Por el teorema anterior, las clases de equivalencia de grupos isomorfos de la forma G/N se corresponden biunívocamente con las órbitas que $\mathrm{Aut}(G_r)$ determina en Ω. Así pues, el número de órbitas es igual al número de grupos de la forma G/N no isomorfos entre sí, y es una cota inferior del número de grupos de orden p^{r+s}.

Observemos que, como $\Phi(G_r)$ es un subgrupo característico, cada automorfismo de G_r fija a $\Phi(G_r)$, luego tenemos un homomorfismo de grupos

$$\theta : \mathrm{Aut}(G_r) \longrightarrow \mathrm{Aut}(G_r/\Phi(G_r)),$$

y el teorema 5.57 prueba que si $\alpha \in \mathrm{N}(\theta)$, entonces α fija a cada elemento de $\Phi(G_r)$, luego si $N \in \Omega$, se cumple que $\alpha[N] = N$. En otras palabras, tenemos

que $\mathrm{N}(\theta)$ está contenido en el estabilizador $(\mathrm{Aut}(G_r))_N$ de cualquier $N \in \Omega$. Así, el cardinal de la órbita es

$$|\Omega_N| = |\operatorname{Aut}(G_r) : (\operatorname{Aut}(G_r))_N| \leq |\operatorname{Aut}(G_r) : \mathrm{N}(\theta)| \leq |\operatorname{Aut}(G_r/\Phi(G_r))|.$$

El cociente $\mathrm{Aut}(G_r/\Phi(G_r))$ es un p-grupo abeliano elemental, por lo que podemos verlo como un espacio vectorial sobre $k = \mathbb{Z}/p\mathbb{Z}$ de dimensión r. Sus automorfismos como grupo coinciden con sus automorfismos como espacio vectorial, luego el grupo de automorfismos es isomorfo al grupo $\mathrm{LG}(r,p)$ de las matrices regulares $r \times r$ sobre el cuerpo k de p elementos. Una estimación burda de su orden es

$$|\Omega_N| \leq |\operatorname{Aut}(G_r/\Phi(G_r))| = |\mathrm{LG}(r,p)| \leq p^{r^2},$$

pues p^{r^2} es el número total de matrices $r \times r$ con coeficientes en k (regulares o no).

Por otra parte, $\Phi(G_r)$ es también abeliano elemental, luego es un k-espacio vectorial de dimensión $r(r+1)/2$, y cada $N \in \Omega$ es un subespacio vectorial de dimensión s.

En general, podemos estimar como sigue el número de subespacios vectoriales de dimensión s de un k-espacio vectorial V de dimensión d:

El número de conjuntos linealmente independientes de cardinal s es

$$(p^d - 1)(p^d - p)\cdots(p^d - p^{s-1}),$$

pues V tiene p^d elementos, y podemos elegir cualquiera menos el vector nulo, con lo que tenemos $p^d - 1$ posibilidades para elegir el primer vector, el segundo tiene que ser distinto de los p vectores generados por el primero, luego tenemos $p^d - p$ posibilidades, el tercero tiene que ser distinto de los p^2 vectores del subespacio generado por los dos primeros, etc. Tenemos así el número de bases posibles para un subespacio de dimensión s, pero hay que dividirlo entre el número de bases que generan el mismo subespacio. Por el mismo argumento (pero con $d = s$), dicho número es

$$(p^s - 1)(p^s - p)\cdots(p^s - p^{s-1}).$$

Por lo tanto, el número de subespacios es exactamente

$$\frac{p^d - 1}{p^s - 1} \cdot \frac{p^d - p}{p^s - p} \cdots \frac{p^d - p^{s-1}}{p^s - p^{s-1}}.$$

Ahora observamos que, para $0 \leq i < s$,

$$\frac{p^d - p^i}{p^s - p^i} \geq p^{d-s},$$

pues esto equivale a que $p^d - p^i \geq p^d - p^{d-s+i}$, o también a que $p^i \leq p^{d-s+i}$, o a que $p^{d-s} \geq 1$. Por consiguiente, el número N de subespacios es $N \geq p^{s(d-s)}$.

En nuestro caso, tenemos que $|\Omega|$ es el número de subespacios de dimensión s de un k-espacio vectorial de dimensión $r(r+1)/2$, luego

$$|\Omega| \geq p^{s(r(r+1)/2-s)}.$$

Como cada órbita tiene a lo sumo p^{r^2} elementos, el número de órbitas tiene que ser al menos

$$\frac{p^{s(r(r+1)/2-s)}}{p^{r^2}} = p^{sr(r+1)/2-r^2-s^2},$$

que es la cota del enunciado. ∎

Al fijar el exponente de p obtenemos lo siguiente:

Teorema 5.60 *Para cada número natural $n > 6$, hay al menos $p^{\frac{2}{27}n^3-\frac{4}{9}n^2}$ grupos de orden p^n no isomorfos entre sí.*

Demostración: Sea $n = 3k + i$, con $i = 0, 1, 2$ (y $k \geq 2$), y definamos

$$s = \begin{cases} k & \text{si } i = 0, \\ k+1 & \text{si } i = 1, 2. \end{cases}$$

En otros términos, s es el menor número natural que cumple $s \geq n/3$. Llamamos $r = n-s$. Así tenemos una descomposición $n = r+s$ que está en las condiciones del teorema anterior. En efecto, tenemos que comprobar que

$$s \leq \frac{1}{2}r(r+1) = \frac{1}{2}(n-s)(n-s+1) = 1+2+3+\cdots+n-s,$$

para lo cual basta con que se cumpla $s \leq n-s$, o también $2s \leq n$, pero

$$2s \leq 2k+2 \leq 3k \leq n.$$

El teorema anterior nos da entonces que el número N de grupos de orden p^n es

$$N \geq p^{sr(r+1)/2-r^2-s^2}$$

Finalmente observamos que $s = (n+j)/3$, donde $j = 2-i = 0, 1, 2$. Si sustituimos $r = n-s$ en el exponente y $s = (n+j)/3$, operando llegamos a

$$\frac{2}{27}n^3 - \frac{4}{9}n^2 + j\left(\frac{5n}{18} + \frac{j^2}{54} - \frac{jn}{18} - \frac{5j}{18}\right)$$

y la expresión entre paréntesis, evaluada en $j = 1, 2$ da

$$\frac{2n}{9} - \frac{7}{27}, \qquad \frac{n}{6} - \frac{13}{27},$$

y ambas expresiones son positivas si $n > 6$, luego concluimos que

$$N \geq p^{\frac{2}{27}n^3-\frac{4}{9}n^2} = p^{\frac{2}{27}n^2(n-6)}.$$

∎

Capítulo VI

Caracteres de grupos

Gauss se dio cuenta de que cuando se consideran los valores que toma una forma cuadrática $ax^2 + bxy + cy^2$ módulo un primo p que no divida a su discriminante puede suceder que sean restos cuadráticos módulo p o bien restos no cuadráticos módulo p, y ello le llevó a hablar de formas cuadráticas con carácter positivo o negativo módulo p, según fuera el caso (véase [ITAl 14.4], aunque el caso $p = 2$ es un poco más complejo). Por otra parte, Gauss demostró que las formas cuadráticas se dividen en un número finito de clases de equivalencia que forman un grupo abeliano G, y que todas las formas de una misma clase tienen el mismo carácter módulo p, por lo que podemos ver a los caracteres como aplicaciones $\chi_p : G \longrightarrow \{\pm 1\}$ que, de hecho, resultan ser homomorfismos de grupos.

Posteriormente, para demostrar su teorema sobre primos en progresiones aritméticas [ITAn 7.24] Dirichlet extendió la noción de "carácter" para referirse a los homomorfismos de grupos $\chi : U_m \longrightarrow \mathbb{C}^*$, donde U_m es el grupo de las unidades módulo m (véase [ITAn 7.19]). Un poco más en general, los caracteres de un grupo abeliano G pueden definirse como los homomorfismos de grupos $\chi : G \longrightarrow \mathbb{C}^*$. Aquí vamos a exponer una teoría mucho más general, iniciada por Frobenius, sobre caracteres de un grupo finito G, no necesariamente abeliano (si bien podríamos presentarla en un contexto aún más general que el que vamos a considerar).

Los caracteres de un grupo finito no pueden definirse como homomorfismos de grupos, sino que para definirlos tenemos que introducir y estudiar primero lo que se conoce como representaciones lineales de grupos.

6.1 Representaciones lineales de grupos

Un grupo finito es en esencia un concepto abstracto. Por ejemplo, el grupo diédrico D_8 no es ni más ni menos que

$$D_8 = \langle a, b \mid a^4 = b^2 = 1,\, a^b = a^{-1} \rangle\,,$$

donde conviene "olvidar" que el miembro derecho lo hemos definido como un cierto cociente de un grupo libre. Lo que pretende captar la igualdad anterior es que cualquier grupo de orden 8 generado por dos elementos que cumplan las relaciones indicadas tiene pleno derecho a ser considerado como "el" grupo D_8. Ahora bien, a la hora de estudiar un grupo finito, a menudo es útil no considerarlo como grupo abstracto, sino trabajar con una "representación" concreta del mismo, es decir, con un grupo concreto que tenga su estructura. Por ejemplo, podemos representar a D_8 como grupo de permutaciones, lo que técnicamente significa determinar un monomorfismo de grupos $D_8 \longrightarrow \Sigma_4$ que permite identificar cada elemento del grupo con una permutación. Por ejemplo, identificando

$$D_8 = \langle (1,2,3,4), (2,4) \rangle .$$

Sin embargo, es más ilustrativo representar D_8 como el grupo de las simetrías de un cuadrado, lo que técnicamente puede verse como un monomorfismo $D_8 \longrightarrow \mathrm{Is}(E)$, donde E es un plano euclídeo e $\mathrm{Is}(E)$ es su grupo de isometrías. Si fijamos un sistema de referencia con origen en el centro O del cuadrado, cada isometría de E que fija a O se identifica con una matriz del grupo ortogonal $O(2,\mathbb{R}) \leq \mathrm{LG}(2,\mathbb{R})$. Concretamente, podemos representar $D_8 = \langle \sigma, \tau \rangle$ donde

$$\sigma = \begin{pmatrix} \cos\frac{2\pi}{4} & \operatorname{sen}\frac{2\pi}{4} \\ -\operatorname{sen}\frac{2\pi}{4} & \cos\frac{2\pi}{4} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

La primera matriz corresponde a un giro de 90° y la segunda a la simetría respecto al eje vertical.

Esta idea se plasma en la definición siguiente:

Definición 6.1 Una *representación matricial* de *grado* $n \geq 1$ de un grupo finito G sobre un anillo conmutativo A es un homomorfismo de grupos

$$\rho : G \longrightarrow \mathrm{LG}(n, A),$$

donde el grupo *lineal general* $\mathrm{LG}(n, A)$ es el grupo de las matrices inversibles de orden $n \times n$ con coeficientes en A. Diremos que A es el *anillo de coeficientes* de la representación.

Notemos que la definición no exige que ρ sea inyectivo. (En tal caso se dice que la representación es *fiel*.) En general, si N es el núcleo de ρ, tenemos que ρ induce una representación fiel del grupo cociente G/N.

El ejemplo anterior determina una representación matricial del grupo D_8 sobre el anillo de coeficientes $A = \mathbb{Z}$ (luego también sobre cualquier otro anillo que lo contenga). Tomar $A = \mathbb{Z}$ es muy restrictivo, pues, por ejemplo, si queremos una representación análoga del grupo D_6 como grupo de simetrías de un triángulo, tenemos que considerar la matriz de un giro de 120°, y entonces llegamos a la representación $D_6 = \langle \sigma, \tau \rangle$, donde ahora

$$\sigma = \begin{pmatrix} \cos\frac{2\pi}{3} & \operatorname{sen}\frac{2\pi}{3} \\ -\operatorname{sen}\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix} = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}, \quad \tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Esta asignación determina un monomorfismo $D_6 \longrightarrow \mathrm{LG}(2,\mathbb{R})$.

A la hora de estudiar las representaciones matriciales, es útil tener en cuenta que las matrices regulares pueden identificarse con automorfismos de módulos libres. Esto nos lleva a la definición siguiente:

Definición 6.2 Una *representación lineal* de *grado* $n \geq 1$ de un grupo finito G sobre un *anillo de coeficientes* (conmutativo) A es un homomorfismo de grupos $\rho : G \longrightarrow \mathrm{Aut}_A(V)$, donde V es un A-módulo libre de rango n.

Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación lineal de un grupo G, escribiremos a menudo $v\sigma = \rho(\sigma)(v)$. En estos términos, el hecho de que $\rho(\sigma)$ sea un automorfismo de V y que ρ sea un homomorfismo de grupos equivale a las relaciones

$$(v+w)\sigma = v\sigma + w\sigma, \qquad (\alpha v)\sigma = \alpha(v\sigma), \qquad (v\sigma)\tau = v(\sigma\tau),$$

donde v, $w \in V$, σ, $\tau \in G$, $\alpha \in A$.

La relación entre las representaciones matriciales y las representaciones lineales es evidente: toda representación matricial ρ de grado n sobre un anillo A determina una representación lineal sobre cualquier A-módulo libre V de rango n respecto a una base B de V prefijada, sin más que asignar a cada $\sigma \in G$ el automorfismo de V que tiene matriz $\rho(\sigma)$ en la base B.

Recíprocamente, toda representación lineal ρ en un A-módulo libre V de rango n determina una representación matricial de grado n para cada base B de V, sin más que asignar a cada $\sigma \in G$ la matriz de $\rho(\sigma)$ en la base B.

Ahora damos una definición de isomorfismo de representaciones que vuelve irrelevante la arbitrariedad en la elección de las bases:

Definición 6.3 Diremos que dos representaciones lineales $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$ (sobre un mismo anillo de coeficientes A) son *isomorfas* si existe un isomorfismo de A-módulos $\phi : V_1 \longrightarrow V_2$ que cumpla $\rho_2 = \rho_1 \circ \bar{\phi}$, donde $\bar{\phi} : \mathrm{Aut}(V_1) \longrightarrow \mathrm{Aut}(V_2)$ es el isomorfismo de grupos dado por $\bar{\phi}(f) = \phi^{-1} f \phi$. Observemos que la condición $\rho_2 = \rho_1 \circ \bar{\phi}$ es equivalente a que

$$\phi(v\sigma) = \phi(v)\sigma$$

para todo $v \in V_1$ y todo $\sigma \in G$.

Dos representaciones matriciales $\rho_i : G \longrightarrow \mathrm{LG}(n, A)$ son *isomorfas* si existe una matriz $M \in \mathrm{LG}(n, A)$ tal que, para todo $\sigma \in G$, se cumple la relación $\rho_2(\sigma) = M^{-1}\rho_1(\sigma)M$.

Es inmediato que dos representaciones matriciales isomorfas dan lugar a representaciones lineales isomorfas independientemente de los módulos y las bases elegidas, así como que dos representaciones lineales isomorfas dan lugar a representaciones matriciales isomorfas independientemente de las bases elegidas.

A continuación vamos a mostrar una tercera estructura equivalente a la de representación matricial y a la de representación lineal. Se basa en la definición siguiente:

Definición 6.4 Si G es un grupo finito y A es un anillo conmutativo, llamaremos $A[G]$ al A-módulo libre de base G, en el que consideraremos la estructura de A-álgebra[1] determinada por el producto siguiente:

$$(\sum_{\sigma\in G}\alpha_\sigma\sigma)(\sum_{\tau\in G}\beta_\tau\tau)=\sum_{\sigma,\tau\in G}\alpha_\sigma\beta_\tau\sigma\tau.$$

Es evidente que el producto así definido es bilineal y que extiende al producto de G. Teniendo esto en cuenta, se comprueba sin dificultad que cumple todas las propiedades necesarias para que $A[G]$ sea ciertamente una A-álgebra, cuya unidad es el elemento neutro de G.

Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación lineal, podemos dotar a V de estructura de $A[G]$-módulo (por la derecha) mediante el producto dado por

$$v(\sum_{\sigma\in G}\alpha_\sigma\sigma)=\sum_{\sigma\in G}\alpha_\sigma\rho(\sigma)(v).$$

Notemos que el producto $v\sigma$ según esta definición coincide con el producto $v\sigma=\rho(\sigma)(v)$ que habíamos definido. Recíprocamente, si V es un $A[G]$-módulo que como A-módulo es libre de rango finito n, podemos definir una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$ mediante $\rho(\sigma)(v) = v\sigma$.

De este modo, tenemos una correspondencia entre las representaciones lineales de grado n de G y los $A[G]$-módulos (por la derecha) que son A-módulos libres de rango n. Es inmediato que dos representaciones son isomorfas si y sólo si los $A[G]$-módulos correspondientes son isomorfos. Más concretamente, un isomorfismo $f : V_1 \longrightarrow V_2$ entre dos A-módulos libres es un isomorfismo entre dos representaciones lineales de G si y sólo si es un isomorfismo entre los $A[G]$-módulos asociados.

En particular, el producto en $A[G]$ extiende al producto en G, por lo que si el grupo G no es abeliano, el álgebra $A[G]$ no es conmutativa, un hecho que deberemos tener presente en todo momento. Conviene determinar cuál es el centro de $A[G]$. En general el *centro* de un anillo A se define como el subanillo

$$Z(A)=\{a\in A \mid ab=ba \text{ para todo } b\in A\}.$$

Si A es un anillo conmutativo, es obvio que un elemento

$$x=\sum_{\sigma\in G}\alpha_\sigma\sigma\in A[G]$$

está en el centro de $A[G]$ si y sólo si conmuta con todos los elementos $\tau\in G$, es decir, si cumple que $\tau x = x\tau$ o, equivalentemente, $\tau x\tau^{-1} = x$. Explícitamente:

$$\sum_{\sigma\in G}\alpha_\sigma\tau\sigma\tau^{-1}=\sum_{\sigma\in G}\alpha_\sigma\sigma.$$

[1]En álgebra conmutativa, una A-álgebra B se define como un anillo (conmutativo) B con una estructura de A-módulo compatible, en el sentido de que $a(b_1b_2) = (ab_1)b_2$. Si no exigimos que B sea conmutativo, hemos de pedir que $a(b_1b_2) = (ab_1)b_2 = b_1(ab_2)$. En particular, si $A \subset B$, tenemos que los elementos de A conmutan con todos los de B.

Teniendo en cuenta que $\sigma \mapsto \tau\sigma\tau^{-1}$ es biyectiva con inversa $\sigma \mapsto \tau^{-1}\sigma\tau$, esto equivale a que

$$\sum_{\sigma\in G} \alpha_{\tau^{-1}\sigma\tau}\sigma = \sum_{\sigma\in G} \alpha_\sigma\sigma,$$

lo cual equivale a que la función $\sigma \mapsto \alpha_\sigma$ sea constante sobre las clases de conjugación de G. Por consiguiente:

Teorema 6.5 *Si G es un grupo finito y A un anillo conmutativo, el centro de $A[G]$ está formado por los elementos de la forma*

$$\sum_{c\in \mathrm{cl}(G)} \alpha_c e_c, \qquad \alpha_c \in A,$$

donde, para cada clase de conjugación $c \in \mathrm{cl}(G)$, llamamos

$$e_c = \sum_{\sigma\in c} \sigma.$$

Equivalentemente, $Z(A[G])$ es el submódulo de $A[G]$ que tiene por base los elementos e_c.

Veamos un par de ejemplos generales de representaciones:

Definición 6.6 Si G es un grupo finito, la *representación trivial* de grado n de G sobre el anillo conmutativo A es la representación matricial $\rho : G \longrightarrow \mathrm{LG}(n, A)$ dada por $\rho(\sigma) = I_n$ (la matriz identidad) para todo $\sigma \in G$. Sus representaciones lineales asociadas son las representaciones en A-módulos libres V de rango n que cumplen $v\sigma = v$ para todo $v \in V$ y todo $\sigma \in G$.

Definición 6.7 Si G es un grupo finito, llamaremos *representación regular* de G a la representación asociada a la estructura de $A[G]$-módulo de $A[G]$. Claramente es fiel y su grado es el orden de G.

Ejemplo Consideremos un grupo cíclico de orden 3, digamos $G = \{1, \sigma, \sigma^2\}$. Entonces el álgebra $\mathbb{C}[G]$ está formada por los elementos de la forma $a+b\sigma+c\sigma^2$, donde a, b, c son números complejos. El producto se calcula de forma obvia. Por ejemplo:

$$(3 + 2\sigma + i\sigma^2)(2i - \sigma) = 6i + 4i\sigma - 2\sigma^2 - 3\sigma - 2\sigma^2 - i = 5i + (-3 + 4i)\sigma - 4\sigma^2.$$

Las imágenes de los vectores de la base $(1, \sigma, \sigma^2)$ por la multiplicación por σ son, respectivamente $(\sigma, \sigma^2, 1)$, luego la matriz asociada a la multiplicación por sigma es

$$\sigma \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

La representación regular de G es la representación $G \longrightarrow \mathrm{Aut}(\mathbb{C}[G])$ que asigna a σ el automorfismo cuya matriz en la base G es la que acabamos de determinar. ∎

Ahora veamos cómo podemos construir nuevas representaciones a partir de unas dadas:

Definición 6.8 Si $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, son dos representaciones lineales de G, definimos su *suma directa* como la representación

$$\rho_1 \oplus \rho_2 : G \longrightarrow \mathrm{Aut}(V_1 \oplus V_2)$$

asociada a la suma directa de los $A[G]$-módulos $V_1 \oplus V_2$. Obviamente, se trata de la representación dada por $(v_1 + v_2)\sigma = v_1\sigma + v_2\sigma$, donde $v_1\sigma$ se calcula con ρ_1 y $v_2\sigma$ con ρ_2.

Es claro que podemos definir igualmente la suma directa de cualquier número finito de representaciones de G. El grado de la suma directa es la suma de los grados.

Ejemplo Consideremos de nuevo el grupo $G = \langle 1, \sigma, \sigma^2 \rangle$. Si $\omega \in \mathbb{C}$ es una raíz cúbica de la unidad (distinta de 1), una representación $\rho : G \longrightarrow \mathrm{Aut}(\mathbb{C})$ es la dada por $z\sigma = \omega z$, que se corresponde con la representación matricial (considerando la base canónica 1 de $\mathbb{C}$) dada por $\sigma \mapsto (\omega)$.

Otra representación distinta es representación ρ' la dada por $z\sigma = \omega^2 z$, que se corresponde con la representación matricial $\sigma \mapsto (\omega^2)$.

Notemos que no son isomorfas, pues el grupo $\mathrm{LG}(1, \mathbb{C})$ es abeliano, y no existe ninguna matriz regular M que cumpla $(\omega^2) = M^{-1}(\omega)M$.

Sumando ambas representaciones obtenemos otra $\rho \oplus \rho' : G \longrightarrow \mathrm{Aut}(\mathbb{C}^2)$ dada por $(z_1, z_2)\sigma = (z_1\omega, z_2\omega^2)$, que, tomando la base canónica, se corresponde con la representación matricial determinada por

$$\sigma \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}.$$

■

A partir de aquí nos centraremos en las representaciones lineales sobre cuerpos. Observemos que, si K es un cuerpo, todo $K[G]$-módulo V es libre sobre K, aunque, para que determine una representación de G sobre K, hemos de exigir que su dimensión sobre K sea finita.

A la hora de estudiar las representaciones lineales de un grupo finito, es fundamental estudiar la posibilidad de expresar una representación dada como suma de otras más sencillas. Tales sumandos han de ser subrepresentaciones, en el sentido siguiente:

Definición 6.9 Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación de G con coeficientes en un cuerpo K, llamaremos *subrepresentaciones* de ρ a las representaciones $G \longrightarrow \mathrm{Aut}(W)$ asociadas a los $K[G]$-submódulos W de V.

Notemos que, para que un subespacio vectorial $W \subset V$ sea un $K[G]$-submódulo, es suficiente con que $W\sigma \subset W$, para todo $\sigma \in G$.

Según decíamos, si $\rho = \rho_1 \oplus \rho_2 : G \longrightarrow \mathrm{Aut}(V_1 \oplus V_2)$ es la suma de dos representaciones ρ_1 y ρ_2, entonces éstas son subrepresentaciones de ρ, pues están asociadas a V_1 y V_2, que son $K[G]$-submódulos de $V_1 \oplus V_2$.

Ejemplo Consideremos de nuevo la representación regular del grupo cíclico de orden 3. Un submódulo de $\mathbb{C}[G]$ es $W = \langle 1 + \sigma + \sigma^2 \rangle$, pues, ciertamente,

$$(1 + \sigma + \sigma^2)\sigma = \sigma + \sigma^2 + 1 = 1 + \sigma + \sigma^2.$$

De hecho, se cumple que $w\sigma = w$ para todo $w \in W$, por lo que la subrepresentación asociada a W es la representación trivial de grado 1. ∎

Veamos ahora el primer resultado no trivial sobre representaciones lineales:

Teorema 6.10 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de un grupo finito G sobre un cuerpo K cuya característica no divida al orden de G, y sea W un $K[G]$-submódulo de V. Entonces existe un $K[G]$-submódulo W^0 tal que $V = W \oplus W^0$.*

Demostración: Sea W' cualquier subespacio vectorial de V que cumpla $V = W \oplus W'$, sea $p : V \longrightarrow W$ la proyección y sea $p^0 : V \longrightarrow W$ la aplicación lineal dada por[2]

$$p^0(v) = \frac{1}{|G|} \sum_{\sigma \in G} p(v\sigma^{-1})\sigma.$$

Si $w \in W$, entonces $p(w\sigma^{-1})\sigma = (w\sigma^{-1})\sigma = w$, luego $p^0(w) = w$. Si llamamos W^0 al núcleo de p^0, es claro que $V = W \oplus W^0$. Por otra parte,

$$p^0(v\tau^{-1})\tau = \frac{1}{|G|} \sum_{\sigma \in G} p(v\tau^{-1}\sigma^{-1})\sigma\tau = p^0(v).$$

Esto implica que W^0 es un $K[G]$-submódulo, pues si $p^0(v) = 0$, entonces

$$p^0(v\tau)\tau^{-1} = p^0(v) = 0,$$

luego $p^0(v\tau) = 0$ y, por lo tanto, $v\tau \in W^0$. ∎

Ejemplo Continuando con el ejemplo anterior, si $\omega \neq 1$ es una raíz cúbica de la unidad y llamamos

$$\alpha_0 = 1 + \sigma + \sigma^2, \quad \alpha_1 = 1 + \omega^2\sigma + \omega\sigma^2, \quad \alpha_2 = 1 + \omega\sigma + \omega^2\sigma^2,$$

se cumple que

$$\alpha_0\sigma = \alpha_0, \quad \alpha_1\sigma = \omega\alpha_1, \quad \alpha_2\sigma = \omega^2\alpha_2,$$

por lo que $W = \langle \alpha_0 \rangle$, $W_1 = \langle \alpha_1 \rangle$ y $W_2 = \langle \alpha_2 \rangle$ son $\mathbb{C}[G]$ submódulos de $\mathbb{C}[G]$, y α_0, α_1, α_2 son linealmente independientes sobre $\mathbb{C}$, pues

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{vmatrix} \neq 0,$$

luego $\mathbb{C}[G] = W \oplus W_1 \oplus W_2$, y así $W_1 \oplus W_2$ es un $\mathbb{C}[G]$-submódulo de $\mathbb{C}[G]$ que complementa a W en las condiciones del teorema anterior. ∎

[2]Al dividir entre $|G|$ estamos usando la hipótesis sobre la característica de K.

Definición 6.11 Diremos que una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$ es *irreducible* si V no tiene más $K[G]$-submódulos que los triviales: 0 y V.

Por el teorema anterior, si una representación no es irreducible, se descompone en suma directa de dos subrepresentaciones no triviales. Es claro entonces que toda representación puede descomponerse en suma directa de representaciones irreducibles $V = W_1 \oplus \cdots \oplus W_n$. La descomposición no es única, en el sentido de que podemos elegir los submódulos W_i de formas distintas, pero más adelante veremos (teorema 6.24) que la descomposición es única salvo isomorfismo, en el sentido de que dos descomposiciones cualesquiera de un mismo $K[G]$-módulo V han de tener el mismo número de sumandos y que, debidamente ordenados, cada sumando de una descomposición es isomorfo al sumando correspondiente de la otra.

El teorema 6.10 hace que las representaciones de grupos sobre cuerpos de característica cero tengan un comportamiento mucho más simple que sobre cuerpos de característica prima. Por ello se distingue entre la *teoría de representaciones ordinarias* (sobre cuerpos de característica 0) y la teoría de *representaciones modulares* (sobre cuerpos de característica prima, que es esencialmente análoga a la primera cuando la característica no divide al orden del grupo).

6.2 Caracteres

Finalmente estamos en condiciones de introducir el concepto general de carácter de un grupo finito.

Recordemos que la traza [Al 6.38] de una matriz cuadrada $A = (a_{ij})$ se define como

$$\mathrm{Tr}(A) = \sum_i a_{ii}.$$

La traza es invariante por semejanza, es decir, que, si M es una matriz regular, se cumple que $\mathrm{Tr}(M^{-1}AM) = \mathrm{Tr}(A)$. En particular, si V es un espacio vectorial y $f \in \mathrm{Aut}(V)$, podemos definir la traza $\mathrm{Tr}(f)$ como la traza de la matriz de f en cualquier base.

Definición 6.12 Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de un grupo finito G en un K-espacio vectorial V. Llamaremos *carácter* asociado a ρ a la función $\chi_\rho : G \longrightarrow K$ dada por $\chi_\rho(\sigma) = \mathrm{Tr}(\rho(\sigma))$. Los caracteres de las representaciones de G se llaman también caracteres de G. Un carácter es *irreducible* si está asociado a una representación irreducible.

Claramente, dos representaciones isomorfas determinan el mismo carácter. Observemos que, si ρ tiene grado n, entonces $\rho(1)$ es la identidad en V y su matriz asociada en cualquier base es I_n, luego $\chi_\rho(1) = n$.

Otro hecho obvio es que

$$\chi_\rho(\sigma^{-1}\tau\sigma) = \mathrm{Tr}(\rho(\sigma)^{-1}\rho(\tau)\rho(\sigma)) = \mathrm{Tr}(\rho(\tau)) = \chi_\rho(\tau).$$

En otras palabras: los caracteres son constantes sobre las clases de conjugación de G.

Ejemplo Sea r_G el carácter de la representación regular de un grupo G. Entonces

$$r_G(\sigma) = \begin{cases} |G| & \text{si } \sigma = 1, \\ 0 & \text{si } \sigma \neq 1. \end{cases}$$

En efecto, fijemos $\tau \in G$. Si $\tau \neq 1$ la matriz de $\rho(\tau)$ respecto de la base G tiene en la fila correspondiente a σ un único 1 situado en la columna correspondiente a $\sigma\tau \neq \sigma$, y ceros en los demás lugares, luego la diagonal es nula y, por consiguiente $r_G(\tau) = 0$. ∎

Ejemplo El grupo D_8 tiene 5 clases de conjugación:

$$\mathrm{cl}(D_4) = \{\{1\}, \{\sigma, \sigma^3\}, \{\sigma^2\}, \{\tau, \sigma^2\tau\}, \{\sigma\tau, \sigma^3\tau\}\},$$

y se comprueba sin dificultad que el carácter χ asociado a la representación matricial determinada por

$$\sigma = \begin{pmatrix} \cos\frac{2\pi}{4} & \operatorname{sen}\frac{2\pi}{4} \\ -\operatorname{sen}\frac{2\pi}{4} & \cos\frac{2\pi}{4} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

es el determinado por la tabla:

	1	σ	σ^2	τ	$\sigma\tau$
χ	2	0	−2	0	0

(sólo hay que calcular las matrices correspondientes a cada elemento y calcular su traza). ∎

Ejercicio: Calcular el carácter asociado a la representación de D_6 construida tras la definición 6.1.

Observemos que $\mathrm{LG}(1, K) \cong K^*$ y el isomorfismo puede verse como el que a cada matriz le asigna su traza, luego una representación matricial de grado 1 de un grupo G puede verse como un homomorfismo de grupos $G \longrightarrow K^*$, que se identifica a su vez con su carácter. Así pues:

Teorema 6.13 *Los caracteres de grado* 1 *de un grupo finito G son simplemente los homomorfismos de grupos $\chi : G \longrightarrow K^*$.*

Veremos más adelante que los caracteres irreducibles de los grupos abelianos tienen necesariamente grado 1, de modo que lo que se conoce habitualmente como "caracteres de un grupo abeliano" son en este contexto sus caracteres irreducibles sobre $\mathbb{C}$, es decir, los homomorfismos $G \longrightarrow \mathbb{C}^*$.

El teorema siguiente muestra que la suma de caracteres es de nuevo un carácter:

Teorema 6.14 *Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, dos representaciones de un grupo G y sean $\chi_i : G \longrightarrow K$ sus caracteres correspondientes. Entonces el carácter de $\rho_1 \oplus \rho_2$ es $\chi_1 + \chi_2$.*

DEMOSTRACIÓN: Si fijamos bases B_i de V_i y llamamos $\bar{\rho}_i(\sigma)$ a la matriz de $\rho_i(\sigma)$ en la base B_i, es claro que la matriz de $(\rho_1 \oplus \rho_2)(\sigma)$ en la base $B_1 \cup B_2$ de $V_1 \oplus V_2$ es

$$\begin{pmatrix} \bar{\rho}_1(\sigma) & 0 \\ 0 & \bar{\rho}_2(\sigma) \end{pmatrix},$$

y la traza de esta matriz es $\chi_1(\sigma) + \chi_2(\sigma)$. ∎

Puede probarse que el producto de caracteres es también un carácter, pero no vamos a necesitar este hecho.

NOTA: *A partir de aquí supondremos tácitamente que el cuerpo de coeficientes sobre el que consideramos las representaciones es un cuerpo algebraicamente cerrado $K \subset \mathbb{C}$.*

Probaremos que, en estas condiciones, es irrelevante la elección de K, de modo que es indiferente tomar $K = \mathbb{C}$ o $K = \mathbb{A}$ (el cuerpo de los números algebraicos sobre $\mathbb{Q}$).

Teorema 6.15 *Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación y $\sigma \in G$, entonces V admite una base formada por vectores propios de $\rho(\sigma)$, y los valores propios son raíces $|G|$-ésimas de la unidad.*

DEMOSTRACIÓN: Restringiendo ρ al subgrupo generado por σ, podemos suponer que G está generado por σ. Como K es algebraicamente cerrado, el automorfismo $\rho(\sigma)$ tiene al menos un valor propio $\alpha_1 \in K$ (una raíz de su polinomio característico). Sea $v_1 \in V$ un vector propio asociado a α_1, de modo que $v_1\sigma = \alpha_1 v_1$ y, en general, $v_1\sigma^n = \alpha_1^n v_1$. Así pues, $W_1 = \langle v_1 \rangle$ es un $K[G]$-submódulo. Por 6.10 podemos descomponer $V = W_1 \oplus V_1$, donde V_1 es también un $K[G]$-submódulo.

Repitiendo el mismo razonamiento con V_1 podemos encontrar un $K[G]$-submódulo $W_2 = \langle v_2 \rangle$ y una descomposición $V = W_1 \oplus W_2 \oplus V_2$. Tras un número finito de pasos llegamos a una descomposición $V = W_1 \oplus \cdots \oplus W_n$ en $K[G]$-submódulos de la forma $W_i = \langle v_i \rangle$, donde cada v_i es obviamente un vector propio de $\rho(\sigma)$.

La matriz de $\rho(\sigma)$ en esta base es diagonal, y los elementos de la diagonal son sus valores propios α_i. Si $n = |G|$, se cumple que $\sigma^n = 1$, luego $\alpha_i^n = 1$, luego los valores propios α_i son raíces n-simas de la unidad. ∎

En general no es posible elegir una base de V tal que la matriz de $\rho(\sigma)$ sea diagonal simultáneamente para todo $\sigma \in G$, pero, como la traza $\chi(\sigma)$ se puede calcular a partir de la matriz de $\rho(\sigma)$ en cualquier base, concluimos que

$$\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n,$$

donde los números $\epsilon_i \in K$ son raíces $|G|$-ésimas de la unidad y, en particular, son enteros algebraicos (es decir, que son raíces de polinomios mónicos con coeficientes enteros). Pero la suma de enteros algebraicos es un entero algebraico [Al 8.9]), luego tenemos probado el teorema siguiente:

Teorema 6.16 *Los valores que toman los caracteres de los grupos finitos son enteros algebraicos.*

En particular podemos ver los caracteres como aplicaciones $\chi : G \longrightarrow \mathbb{A}$, aunque no hemos probado que las representaciones matriciales que los definen tengan necesariamente sus coeficientes en $\mathbb{A}$. Como es habitual, representamos con una barra la conjugación compleja.

Teorema 6.17 *Si $\chi : G \longrightarrow \mathbb{A}$ es un carácter de un grupo finito G, entonces, para todo $\sigma \in G$, se cumple que $\chi(\sigma^{-1}) = \overline{\chi(\sigma)}$.*

Demostración: Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación que genere el carácter dado. Según 6.15, podemos elegir una base de V en la que $\rho(\sigma)$ admite una matriz diagonal (α_{ij}) cuya diagonal está formada por raíces de la unidad, que son elementos de $\mathbb{A}$ de módulo 1. Entonces

$$\chi(\sigma^{-1}) = \sum_i \alpha_{ii}^{-1} = \sum_i \bar{\alpha}_{ii} = \overline{\chi(\sigma)}.$$

■

Como tercera aplicación de 6.15 mostramos que un carácter determina el núcleo de la representación que lo genera:

Definición 6.18 Si $\chi : G \longrightarrow \mathbb{A}$ es un carácter de un grupo finito G, llamaremos *núcleo* de χ al conjunto

$$\mathrm{N}(\chi) = \{\sigma \in G \mid \chi(\sigma) = \chi(1)\}.$$

Teorema 6.19 *Si $\rho : G \longrightarrow \mathrm{Aut}(G)$ es una representación de un grupo finito G y χ es el carácter que determina, entonces el núcleo de χ es el núcleo de ρ.*

Demostración: Obviamente, $\sigma \in G$ está en el núcleo de ρ si y sólo si $\rho(\sigma) = I_n$, donde n es el grado de la representación, luego, en tal caso, se cumple que $\chi(\sigma) = n = \chi(1)$. Recíprocamente, si $\chi(\sigma) = n$, sabemos que, en una base adecuada, $\rho(\sigma)$ se corresponde con una matriz diagonal y $\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n$ es la suma de dicha diagonal. Los ϵ_i son números complejos de módulo 1, luego la parte real de cada uno de ellos es ≤ 1. Para que la suma dé n es necesario que todas las partes reales sean 1, lo cual implica que $\epsilon_i = 1$ y, por consiguiente, que $\rho(\sigma) = I_n$, de modo que σ está en el núcleo de ρ. ■

Definición 6.20 Si G es un grupo finito, N es un subgrupo normal, para cada carácter $\chi : G/N \longrightarrow \mathbb{A}$ de G/N definimos el carácter $\hat{\chi} : G \longrightarrow \mathbb{A}$ dado por $\hat{\chi}(\sigma) = \chi(\sigma N)$.

Se trata ciertamente de un carácter porque si $\rho : G/N \longrightarrow \mathrm{Aut}(V)$ es la representación que determina χ, entonces la composición $G \longrightarrow G/N \longrightarrow \mathrm{Aut}(V)$ es una representación de G que genera $\hat{\chi}$.

Es claro que χ es irreducible si y sólo si lo es $\hat{\chi}$. Además, tenemos que $N \leq \mathrm{N}(\hat{\chi})$. Recíprocamente, es claro que todo carácter ψ de G que cumpla $N \leq \mathrm{N}(\psi)$ es de la forma $\psi = \hat{\chi}$, para cierto carácter $\chi : G/N \longrightarrow \mathbb{A}$.

En vista de esto, en lo sucesivo identificaremos los caracteres de un grupo cociente G/N con los caracteres de G cuyo núcleo contiene a N.

Las propiedades fundamentales de los caracteres se deducen del teorema siguiente:

Teorema 6.21 (Lema de Schur) *Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$ dos representaciones irreducibles de un grupo finito G y sea $f : V_1 \longrightarrow V_2$ un homomorfismo de $K[G]$-módulos. Si las representaciones no son isomorfas, se cumple que $f = 0$ y, si $V_1 = V_2$ y $\rho_1 = \rho_2$, entonces existe un $\alpha \in K$ tal que $f(v) = \alpha v$, para todo $v \in V_1$.*

DEMOSTRACIÓN: Si $f \neq 0$, el núcleo de V_1 ha de ser un $K[G]$-submódulo distinto de V_1, luego ha de ser trivial, y la imagen ha de ser un $K[G]$-submódulo no trivial de V_2, luego ha de ser todo V_2. Esto prueba que f es un isomorfismo y las representaciones son isomorfas.

Si suponemos que ambas representaciones son la misma, sea $\alpha \in K$ un valor propio de f (aquí usamos que K es algebraicamente cerrado). Sea $f' : V_1 \longrightarrow V_1$ la aplicación lineal dada por $f'(v) = f(v) - \alpha v$. Es claro que es un homomorfismo de $K[G]$-módulos que y su núcleo no es trivial (porque contiene a los vectores propios asociados a α) luego, por la parte ya probada, $f' = 0$, luego $f(v) = \alpha v$ para todo $v \in V_1$. ∎

Para extraer consecuencias del lema de Schur conviene introducir la notación siguiente:

Definición 6.22 Si G es un grupo finito, representamos por K^G al conjunto de funciones $\phi : G \longrightarrow K$. Definimos en K^G la forma bilineal simétrica

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \phi(\sigma)\psi(\sigma^{-1}).$$

El teorema siguiente generaliza a [ITAn 7.22]:

Teorema 6.23 (Relaciones de ortogonalidad) *Si χ_1 y χ_2 son dos caracteres irreducibles de un grupo finito G, entonces*

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & \text{si } \chi_1 = \chi_2, \\ 0 & \text{si } \chi_1 \neq \chi_2. \end{cases}$$

DEMOSTRACIÓN: Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$ representaciones que generen los caracteres χ_i. Sea $h : V_1 \longrightarrow V_2$ una aplicación lineal arbitraria y sea $h^0 : V_1 \longrightarrow V_2$ la aplicación lineal dada por

$$h^0(v) = \frac{1}{|G|} \sum_{\sigma \in G} h(v\sigma)\sigma^{-1}.$$

Se cumple que h^0 es un homomorfismo de $K[G]$-módulos, pues

$$h^0(v\tau) = \frac{1}{|G|} \sum_{\sigma \in G} h(v\tau\sigma)\sigma^{-1} = \left(\frac{1}{|G|} \sum_{\sigma \in G} h(v\tau\sigma)(\tau\sigma)^{-1} \right) \tau = h^0(v)\tau.$$

Fijemos bases de ambos espacios vectoriales, sean $(r^1_{ij}(\sigma))$, $(r^2_{ij}(\sigma))$ las matrices de $\rho_i(\sigma)$ en las bases respectivas y sean (x_{ij}), (x^0_{ij}) las matrices de h y h^0, respectivamente. Entonces,

$$x^0_{ij} = \frac{1}{|G|}\sum_{\sigma,k,l} r^1_{ik}(\sigma)x_{kl}r^2_{lj}(\sigma^{-1}).$$

Si $\chi_1 \neq \chi_2$, las representaciones no son isomorfas, luego, según el lema de Schur, ha de ser $h^0 = 0$, cualquiera que sea la aplicación h de partida. Así pues, el miembro derecho de la igualdad anterior ha de ser nulo cualesquiera que sean los valores de x_{kl}. Si hacemos $x_{ij} = 1$ y $x_{kl} = 0$ cuando $(k,l) \neq (i,j)$, nos queda que

$$\frac{1}{|G|}\sum_{\sigma\in G} r^1_{ii}(\sigma)r^2_{jj}(\sigma^{-1}) = 0$$

y, sumando para todo i, j, queda que

$$\langle\chi_1,\chi_2\rangle = \frac{1}{|G|}\sum_{\sigma\in G}\chi_1(\sigma)\chi_2(\sigma^{-1}) = 0.$$

Tomemos ahora $\rho_1 = \rho_2$. Entonces el lema de Schur nos da que $h^0(v) = \alpha v$ para todo $v \in V_1$. El valor de α depende de h, y podemos calcularlo. Para ello observamos que

$$n\alpha = \operatorname{Tr}(h^0) = \frac{1}{|G|}\sum_{\sigma\in G}\operatorname{Tr}(\rho_1(\sigma)\circ h\circ\rho_2(\sigma^{-1})) = \frac{1}{|G|}\sum_{\sigma\in G}\operatorname{Tr}(h) = \operatorname{Tr}(h),$$

luego $\alpha = (1/n)\operatorname{Tr}(h)$. En el caso $i \neq j$, tomando igualmente $x_{ij} = 1$ y $x_{kl} = 0$ cuando $(k,l) \neq (i,j)$, obtenemos igualmente que

$$\frac{1}{|G|}\sum_{\sigma\in G} r^1_{ii}(\sigma)r^1_{jj}(\sigma^{-1}) = 0.$$

En cambio, para $i = j$, la misma elección de x_{kl} hace que $\operatorname{Tr}(h) = 1$, luego

$$\frac{1}{n} = \frac{1}{|G|}\sum_{\sigma\in G} r^1_{ii}(\sigma)r^1_{jj}(\sigma^{-1}).$$

Al sumar para todo i y todo j, la igualdad $i = j$ se da n veces, luego sumamos n veces la última ecuación y llegamos a que

$$\langle\chi_1,\chi_1\rangle = \frac{1}{|G|}\sum_{\sigma\in G}\chi_1(\sigma)\chi_1(\sigma^{-1}) = 1.$$

■

En realidad, la prueba del teorema anterior contiene más información que la que indica su enunciado, puesto que hemos probado que $\langle\chi_1,\chi_2\rangle = 0$, no bajo la hipótesis de que $\chi_1 \neq \chi_2$, sino bajo la hipótesis de que las representaciones ρ_1 y ρ_2 no eran isomorfas. Por consiguiente, si dos representaciones irreducibles no son isomorfas, sus caracteres χ_1 y χ_2 han de ser distintos o, de lo contrario, cumplirían que $\langle\chi_1,\chi_2\rangle = 1$, mientras que hemos visto que $\langle\chi_1,\chi_2\rangle = 0$.

En otras palabras, tenemos que dos representaciones irreducibles de un grupo G son isomorfas si y sólo si determinan el mismo carácter. Vamos a ver que esto es cierto aunque las representaciones no sean irreducibles. Esto es una consecuencia inmediata del teorema siguiente:

Teorema 6.24 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de G, sea ϕ su carácter y sea $V = W_1 \oplus \cdots \oplus W_m$ una descomposición de V en subespacios invariantes irreducibles. Para cada carácter irreducible χ de G, el número de subespacios W_i que determinan una representación con carácter χ es $\langle \phi, \chi \rangle$.*

Demostración: Sea χ_i el carácter de la subrepresentación asociada a W_i. Entonces $\phi = \chi_1 + \cdots + \chi_m$, luego $\langle \phi, \chi \rangle = \langle \chi_1, \chi \rangle + \cdots + \langle \chi_m, \chi \rangle$, y las relaciones de ortogonalidad implican que este valor es el número de índices i tales que $\chi_i = \chi$. ∎

Dicho de otro modo, si una representación tiene carácter ϕ, es necesariamente la suma directa de tantas representaciones irreducibles de carácter χ como indica el producto $\langle \phi, \chi \rangle$. Así pues:

Teorema 6.25 *Dos representaciones de un grupo finito G son isomorfas si y sólo si determinan el mismo carácter.*

Concluimos también que todo carácter ϕ se descompone de forma única como combinación lineal

$$\phi = n_1\chi_1 + \cdots + n_m\chi_m$$

de caracteres irreducibles con coeficientes enteros $n_i \geq 0$. Además,

$$\langle \phi, \phi \rangle = n_1^2 + \cdots + n_m^2,$$

luego ϕ es irreducible si y sólo si $\langle \phi, \phi \rangle = 1$.

El teorema 6.25 es un hecho sorprendente, y es la clave por la que los caracteres tienen interés en el estudio de los grupos: aunque la traza de una matriz no determina ni mucho menos la matriz de la que se obtiene, las trazas de las matrices de una representación matricial de G determinan la representación salvo isomorfismo. Resulta así que los caracteres de un grupo G contienen mucha más información sobre G de lo que se podría pensar en un principio.

Ejemplo El carácter χ que hemos calculado para el grupo D_8 en la página 215 es irreducible, pues

$$\langle \chi, \chi \rangle = \frac{1}{8} \sum_{\sigma \in G} \chi(\sigma)^2 = \frac{1}{8}(4 + 4) = 1.$$

∎

Vamos a probar que el número de caracteres irreducibles es finito. Para ello consideramos la representación regular $\rho : G \longrightarrow \mathrm{Aut}(K[G])$. En el ejemplo de la página 215 hemos visto que

$$r_G(\tau) = \begin{cases} g & \text{si } \tau = 1, \\ 0 & \text{si } \tau \neq 1, \end{cases}$$

donde g es el orden de G.

Ahora, si χ es cualquier carácter irreducible de G, tenemos que

$$\langle r_G, \chi \rangle = \chi(1).$$

Por lo tanto, si $r_G = n_1\chi_1 + \cdots + n_h\chi_h$ es la descomposición de r_G en suma de caracteres irreducibles, los caracteres χ_i resultan ser todos los caracteres irreducibles de G, y $n_i = \chi_i(1)$ es el grado de χ_i. Teniendo en cuenta que $\langle r_G, r_G \rangle = g$, tenemos probado el teorema siguiente:

Teorema 6.26 *Un grupo finito G tiene un número finito de caracteres irreducibles $\chi_1, \ldots, \chi_h$, cuyos grados n_i verifican la relación*

$$n_1^2 + \cdots + n_h^2 = |G|.$$

Ejemplo Conocemos dos caracteres irreducibles del grupo D_8, a saber, el carácter trivial $\chi_1 = 1$ y el carácter de grado 2 calculado en la página 215. Como $8 - 1^2 - 2^2 = 3$ y la única forma de expresar 3 como suma de cuadrados es $3 = 1^1 + 1^2 + 1^2$, concluimos que D_8 tiene un total de 5 caracteres, los dos que conocemos, que llamaremos χ_1 y χ_5, y otros tres caracteres χ_2, χ_3, χ_4 de los que sabemos que tienen grado 1. ∎

Si aplicamos el teorema 6.26 al caso $K = \mathbb{A}$, vemos que G tiene h representaciones irreducibles sobre $\mathbb{A}$, con caracteres χ_i, cuyos grados al cuadrado suman $|G|$. Si ahora $K \subset \mathbb{C}$ es un cuerpo arbitrario (algebraicamente cerrado), tenemos que $\mathbb{A} \subset K$, y las mismas representaciones matriciales con coeficientes en $\mathbb{A}$ pueden verse como representaciones matriciales sobre K que determinan los mismos caracteres. Como la relación $\langle \chi_i, \chi_i \rangle = 1$ no depende del cuerpo considerado, vemos que al considerarlas como representaciones sobre K siguen siendo irreducibles y, como sus grados al cuadrado siguen sumando $|G|$, no puede haber más representaciones irreducibles de G sobre K. Si, por último, tenemos en cuenta que toda representación es suma directa de representaciones irreducibles, tenemos que toda representación de un grupo finito G sobre un cuerpo $K \subset \mathbb{C}$ algebraicamente cerrado es isomorfa a una determinada por una representación sobre $\mathbb{A}$, la cual es irreducible sobre $\mathbb{A}$ si y sólo si lo es sobre K.

O, dicho de otro modo, que al considerar una representación que genera un carácter dado, siempre podemos exigir que esté definida por una representación matricial con coeficientes en $\mathbb{A}$. De hecho, es fácil ver que todo lo dicho hasta aquí vale para representaciones sobre cualquier cuerpo algebraicamente cerrado de característica 0 (sin que importe si es o no un subcuerpo de $\mathbb{C}$), por lo que en la teoría de representaciones ordinarias (sobre cuerpos de característica 0), cualquier cuerpo algebraicamente cerrado da lugar a las mismas representaciones y a los mismos caracteres.

Por consiguiente, a partir de aquí podríamos trabajar exclusivamente en el caso $K = \mathbb{A}$ sin pérdida de generalidad, pero nos será más cómodo aún trabajar en el caso $K = \mathbb{C}$.

6.3 Caracteres complejos

Para trabajar con caracteres complejos es más natural sustituir la forma bilineal $\langle\ ,\ \rangle$ por el siguiente producto escalar:

Definición 6.27 Si G es un grupo finito, definimos en el espacio vectorial $\mathbb{C}^G$ el producto escalar dado por

$$(\phi,\psi)=\frac{1}{|G|}\sum_{\sigma\in G}\phi(\sigma)\overline{\psi(\sigma)}.$$

Observemos que es ciertamente un producto escalar, es decir, que cumple las propiedades de la definición [An 3.36]:

1. $(\phi,\psi)=\overline{(\psi,\phi)}$,
2. $(\phi+\psi,\chi)=(\phi,\chi)+(\psi,\chi)$, $\quad(\phi,\psi+\chi)=(\phi,\psi)+(\phi,\chi)$,
3. $(\alpha\phi,\psi)=\alpha(\phi,\psi)$, $\quad(\phi,\alpha\psi)=\bar{\alpha}(\phi,\psi)$,
4. $(\phi,\phi)\geq 0$ y $(\phi,\phi)=0$ si y sólo si $\phi=0$,

para todo ϕ, ψ, $\chi\in\mathbb{C}^G$ y todo $\alpha\in\mathbb{C}$.

Por otra parte, el teorema 6.17 prueba que, si $\phi,\psi\in\mathbb{C}^G$ son caracteres de G, entonces $\langle\phi,\psi\rangle=(\phi,\psi)$. Ahora observamos que en la sección anterior sólo hemos usado la forma bilineal $\langle\ ,\ \rangle$ sobre caracteres, por lo que todos los resultados de la sección anterior son válidos igualmente cambiando la forma bilineal $\langle\ ,\ \rangle$ por el producto escalar $(\ ,\ )$. Para trabajar con funciones arbitrarias de $\mathbb{C}^G$ es más práctico el producto escalar.

Definición 6.28 Si G es un grupo finito, una *función de clases* en G es una aplicación $f:G\longrightarrow\mathbb{C}$ tal que $f(\rho^{-1}\tau\rho)=f(\tau)$ para todo par de elementos $\tau,\rho\in G$, es decir, una función que es constante en cada clase de conjugación de G. Llamaremos $F(G)\subset\mathbb{C}^G$ al subespacio vectorial formado por todas las funciones de clases.

Tras la definición 6.12 hemos probado que los caracteres de G son funciones de clases. Tenemos un isomorfismo natural $K^G\cong K[G]$ de espacios vectoriales que identifica cada función $\phi\in K^G$ con el elemento

$$\sum_{\sigma\in G}\phi(\sigma)\sigma\in K[G].$$

De acuerdo con el teorema 6.5, este isomorfismo hace corresponder $F(G)$ con el centro de $\mathbb{C}[G]$.

Probamos ahora una nueva consecuencia del lema de Schur, de la que extraeremos a su vez numerosas consecuencias sobre los caracteres de un grupo finito.

Teorema 6.29 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación irreducible de grado n y carácter χ, y sea $\phi \in F(G)$ una función de clases, que podemos identificar con*

$$x = \sum_{\sigma\in G} \phi(\sigma)\sigma \in Z(\mathbb{C}[G]).$$

Entonces, para todo $v \in V$, se cumple que

$$vx = \frac{|G|}{n}(\phi, \overline{\chi})v.$$

DEMOSTRACIÓN: Como x está en el centro de $\mathbb{C}[G]$, es claro que la aplicación lineal $f : V \longrightarrow V$ dada por $f(v) = vx$ es un homomorfismo de $\mathbb{C}[G]$-módulos, luego el lema de Schur implica que existe un $\alpha \in \mathbb{C}$ tal que $f(v) = \alpha v$, para todo $v \in V$. Sólo hemos de calcular α. Para ello usamos la linealidad de la traza:

$$n\alpha = \mathrm{Tr}(f) = \sum_{\sigma\in G} \phi(\sigma)\,\mathrm{Tr}(\rho(\sigma)) = \sum_{\sigma\in G} \phi(\sigma)\chi(\sigma) = |G|(\phi, \overline{\chi}).$$

■

La primera consecuencia es la siguiente:

Teorema 6.30 *Si G es un grupo finito, sus caracteres irreducibles forman una base (ortonormal) del espacio $F(G)$ de las funciones de clases.*

DEMOSTRACIÓN: Sean $\chi_1, \ldots, \chi_h$ los caracteres irreducibles de G. Las relaciones de ortogonalidad implican que son linealmente independientes, luego sólo hemos de probar que generan $H = F(G)$. Para ello basta probar que la dimensión de H es h y, a su vez, para ello basta probar que los conjugados $\overline{\chi}_1, \ldots, \overline{\chi}_h$ generan H. Notemos que $(\overline{\chi}_i, \overline{\chi}_j) = (\chi_j, \chi_i)$, luego los conjugados también son ortonormales.

Tomamos $\psi \in H$ y consideramos la función de clases

$$\phi = \psi - \sum_{i=1}^{h} (\psi, \overline{\chi}_i)\overline{\chi}_i,$$

que tiene la propiedad de que $(\phi, \overline{\chi}_i) = 0$ para todo i. Sólo hemos de probar que esto implica que $\phi = 0$. Sea $x \in Z(\mathbb{C}[G])$ el elemento correspondiente a ϕ a través del isomorfismo natural.

Consideremos una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$. Si es irreducible, el teorema anterior nos da que $vx = 0$, para todo $v \in V$. Si no es irreducible, llegamos a la misma conclusión descomponiéndolo en suma directa de submódulos irreducibles.

Vamos a aplicar esto al caso en que $V = \mathbb{C}[G]$, es decir, a la representación regular de G, y para $v = 1$. Entonces,

$$0 = 1x = \sum_{\sigma\in G} \phi(\sigma)\sigma,$$

luego $\phi = 0$. ■

Es evidente que la dimensión de $F(G)$ es igual al número de clases de conjugación de G, luego:

Teorema 6.31 *El número de caracteres irreducibles de un grupo G es igual a su número de clases de conjugación.*

Si $\chi_1, \ldots, \chi_h$ son los caracteres irreducibles de un grupo G, tenemos que toda función de clases f se expresa de forma única como

$$f = \sum_{i=1}^{h} (f, \chi_i)\chi_i,$$

luego la condición necesaria y suficiente para que una función de clases $f \neq 0$ sea un carácter es que (f, χ_i) sea un número natural para todo i.

El teorema 6.16 afirma que los valores que toman los caracteres son enteros algebraicos. La siguiente consecuencia de 6.29 es otra propiedad de integridad:

Teorema 6.32 *Sea χ un carácter irreducible de grado n de un grupo G y sea $\psi : G \longrightarrow \mathbb{C}$ una función de clases cuyas imágenes sean enteros algebraicos. Entonces*

$$\frac{1}{n} \sum_{\sigma \in G} \psi(\sigma)\chi(\sigma)$$

es un entero algebraico.

Demostración: Consideremos la aplicación $T : Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}$ dada por

$$T(x) = \frac{|G|}{n}(\phi, \overline{\chi}), \qquad \text{donde } x = \sum_{\sigma \in G} \phi(\sigma)\sigma.$$

Observemos que T es C-lineal, pues si $y = \sum_{\sigma \in G} \psi(\sigma)\sigma$, entonces

$$\alpha x + \beta y = \sum_{\sigma \in G} (\alpha\phi + \beta\psi)(\sigma)\sigma,$$

luego

$$T(\alpha x + \beta y) = \frac{|G|}{n}(\alpha\phi + \beta\psi, \overline{\chi}) = \alpha T(x) + \beta T(y).$$

Por otra parte, el teorema 6.29 afirma que el homomorfismo $V \longrightarrow V$ dado por $v \mapsto vx$ es la homotecia de razón $T(x)$. Como $(vx)y = v(xy)$, concluimos que la homotecia de razón $T(xy)$ es la composición de la homotecia de razón $T(x)$ seguida de la homotecia de razón $T(y)$ o, más simplemente: $T(xy) = T(x)T(y)$.

En definitiva, T es un homomorfismo de $\mathbb{C}$-álgebras.

Según 6.5, si $\mathrm{cl}(G) = \{c_1, \ldots, c_h\}$, el centro de $\mathbb{C}[G]$ tiene por base los elementos de la forma

$$e_i = \sum_{\sigma \in c_i} \sigma.$$

Observemos que las potencias e_i^k son claramente combinaciones lineales de elementos de G con coeficientes enteros, por lo que

$$e_i^k \in \mathbb{Z}[G] \cap Z(\mathbb{C}[G]) = \langle e_1, \ldots, e_h \rangle_{\mathbb{Z}}.$$

Si llamamos $\mathbb{Z}[e_i]$ al anillo formado por los elementos de la forma $p(e_i)$, donde $p(t) \in \mathbb{Z}[t]$, tenemos que $\mathbb{Z}[e_i] \subset \langle e_1, \ldots, e_h \rangle_{\mathbb{Z}}$, luego $\mathbb{Z}[e_i]$ es un $\mathbb{Z}$-módulo finitamente generado [Al 4.42]. Veamos que esto implica que e_i es raíz de un polinomio mónico con coeficientes enteros (el argumento es esencialmente el mismo empleado en [Al 8.8]).

En efecto, sean $p_1(e_i), \ldots, p_r(e_i)$ un generador de $\mathbb{Z}[e_i]$ y sea m un número natural mayor que los grados de todos los polinomios p_i. Entonces e_i^m es combinación lineal de los generadores, luego $e_i^m = p(e_i)$, para cierto polinomio $p(t) \in \mathbb{Z}[t]$ de grado menor que m, luego e_i es raíz del polinomio mónico $f_i(t) = t^m - p(t)$.

Como T es un homomorfismo de anillos, de $f_i(t_i) = 0$, al aplicar T se sigue que $f_i(T(e_i)) = 0$, es decir que $T(e_i) \in \mathbb{C}$ es un entero algebraico.

Eligiendo $\sigma_i \in c_i$, podemos expresar

$$x = \sum_{\sigma \in G} \psi(\sigma)\sigma = \sum_{i=1}^{h} \psi(\sigma_i) e_i$$

y, aplicando T, resulta que

$$T(x) = \sum_{i=1}^{h} \psi(\sigma_i) T(e_i)$$

es también un entero algebraico, pero

$$T(x) = \frac{|G|}{n}(\psi, \overline{\chi}) = \frac{1}{n} \sum_{\sigma \in G} \psi(\sigma)\chi(\sigma). \qquad \blacksquare$$

Veamos una primera aplicación:

Teorema 6.33 *Los grados de las representaciones irreducibles de un grupo G dividen al orden de G.*

DEMOSTRACIÓN: Basta probar que si χ es un carácter irreducible de G, entonces $\chi(1) \mid |G|$. Para ello aplicamos el teorema anterior a la función $\psi = \overline{\chi}$, lo que nos da que

$$\frac{1}{n} \sum_{\sigma \in G} \chi(\sigma)\overline{\chi}(\sigma) = \frac{|G|}{n}(\chi, \chi) = \frac{|G|}{n}$$

es un entero algebraico. Como es un número racional, ha de ser entero, y esto significa que $n \mid |G|$. $\blacksquare$

Los teoremas 6.26 y 6.31 nos dan una caracterización de los grupos abelianos:

Teorema 6.34 *Un grupo finito G es abeliano si y sólo si todos sus caracteres irreducibles tienen grado* 1.

DEMOSTRACIÓN: Sea g el orden de G y h su número de clases. Es claro que G es abeliano si y sólo si $g = h$. Si $n_1, \ldots, n_h$ son los grados de los caracteres irreducibles de G, sabemos que

$$n_1^2 + \cdots + n_h^2 = g,$$

luego $g = h$ si y sólo si $n_i = 1$ para todo i. $\blacksquare$

Así pues, de acuerdo con el teorema 6.13, los caracteres irreducibles de un grupo finito abeliano G son simplemente los homomorfismos $\chi : G \longrightarrow \mathbb{C}^*$.

Relaciones de ortogonalidad duales A la hora de calcular tablas de caracteres, es útil contar con que no sólo las filas de la tabla son ortogonales dos a dos, sino que las columnas también lo son. En efecto:

Teorema 6.35 *Sea G un grupo finito, sean $\chi_1, \dots, \chi_h$ sus caracteres irreducibles y sean $\sigma, \tau \in G$. Entonces*

$$\sum_{r=1}^{h} \chi_r(\sigma)\overline{\chi_r(\tau)} = \begin{cases} |G|/|\mathrm{cl}_G(\sigma)| & si \ \ \mathrm{cl}_G(\sigma) = \mathrm{cl}_G(\tau), \\ 0 & si \ \ \mathrm{cl}_G(\sigma) \neq \mathrm{cl}_G(\tau). \end{cases}$$

Demostración: Sean $\sigma_1, \dots, \sigma_h$ representantes de las clases de conjugación de G y sea $h_i = |\mathrm{cl}_G(\sigma_i)|$. En estos términos, lo que hemos de probar es que

$$\sum_{r=1}^{h} \chi_r(\sigma_i)\overline{\chi_r(\sigma_j)} = \frac{|G|}{h_j}\delta_{ij},$$

donde (δ_{ij}) es la matriz identidad. Consideremos las matrices B y C dadas por

$$b_{ij} = \frac{h_j}{|G|}\overline{\chi_i(\sigma_j)}, \qquad c_{ij} = \chi_j(\sigma_i).$$

Entonces, el elemento (i, j) de BC es

$$\frac{1}{|G|}\sum_{r=1}^{h} h_r\overline{\chi_i(\sigma_r)}\chi_j(\sigma_r) = \frac{1}{|G|}\sum_{\sigma\in G}\overline{\chi_i(\sigma)}\chi_j(\sigma) = \delta_{ij},$$

por las relaciones de ortogonalidad, luego $BC = I$. Esto implica que $CB = I$, lo que se traduce precisamente en la relación que queríamos probar. ∎

Subgrupos normales El teorema 6.19 nos permite reconocer el núcleo de un carácter a partir de la tabla de caracteres de un grupo. Obviamente, los núcleos de caracteres son subgrupos normales. Los demás subgrupos normales de un grupo dado pueden calcularse a partir de la tabla de caracteres sin más que tener en cuenta que son intersecciones de núcleos:

Teorema 6.36 *Todo subgrupo normal de un grupo finito es la intersección de los núcleos de los caracteres irreducibles que lo contienen.*

Demostración: Es trivial: sea G un grupo y N un subgrupo normal. Los caracteres irreducibles que contienen a N en su núcleo son los caracteres irreducibles de G/N, luego todo se reduce a probar que la intersección de los núcleos de todos los caracteres irreducibles de un grupo dado es trivial, pero ello se debe a que dicha intersección es el núcleo de la representación regular, que es fiel. ∎

Teorema 6.37 *El subgrupo derivado de un grupo finito es la intersección de los núcleos de los caracteres irreducibles de grado* 1.

DEMOSTRACIÓN: Si un carácter irreducible $\chi : G \longrightarrow \mathbb{C}$ cumple $G' \leq \mathrm{N}(\chi)$, entonces χ es un carácter irreducible de G/G' y, como el cociente es abeliano, χ tiene grado 1. Recíprocamente, si χ tiene grado 1, entonces es un homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$, luego $G/\mathrm{N}(\chi)$ es abeliano y, por consiguiente, $G' \leq \mathrm{N}(\chi)$. ∎

En particular, el número de caracteres de grado 1 de un grupo finito G es igual al índice $|G : G'|$.

También podemos calcular el centro de un grupo a partir de su tabla de caracteres. Para ello definimos el *centro* de un carácter $\chi : G \longrightarrow \mathbb{C}$ como el conjunto

$$Z(\chi) = \{\sigma \in G \mid |\chi(\sigma)| = \chi(1)\}.$$

Teorema 6.38 *Sea G un grupo finito.*

1. *Si χ es un carácter de G asociado a una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$, entonces*
$$Z(\chi) = \{\sigma \in G \mid \rho(\sigma) \text{ es una homotecia }\}.$$
2. *$Z(\chi)$ es un subgrupo de G y $Z(\chi)/\mathrm{N}(\chi)$ es cíclico.*
3. *$Z(G)$ es la intersección de los centros de todos los caracteres irreducibles de G.*
4. *Si χ es un carácter irreducible y fiel de G, entonces $Z(G) = Z(\chi)$.*

DEMOSTRACIÓN: 1) Dado $\sigma \in G$, según 6.15, eligiendo una base en V, podemos suponer que la matriz asociada al automorfismo $\rho(\sigma)$ es diagonal y $\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n$ es la suma de dicha diagonal. Además, todos los ϵ_i tienen módulo 1.

Tenemos que $\sigma \in Z(\chi)$ si y sólo si $|\epsilon_1 + \cdots + \epsilon_n| = n$, y es fácil ver que esto ocurre sí y sólo si todos los ϵ_i son iguales, es decir, si y sólo si $\rho(\sigma)$ es una homotecia de razón ϵ.

2) Ahora es inmediato que $Z(\chi)$ es un subgrupo de G. Más aún, si llamamos $\lambda(\sigma)$ a la razón de la homotecia $\rho(\sigma)$, tenemos que $\lambda : Z(\chi) \longrightarrow \mathbb{C}^*$ es un homomorfismo de grupos cuyo núcleo es $\mathrm{N}(\chi)$, luego $Z(\chi)/\mathrm{N}(\chi)$ es isomorfo a un subgrupo finito de $\mathbb{C}^*$, luego ha de ser cíclico, por [Al 4.50].

3) Si χ es irreducible, el teorema 6.29 implica que $Z(G) \leq Z(\chi)$. Por otra parte, como $\rho[Z(\chi)]$ está formado por homotecias, $\rho[Z(\chi)] \leq Z(\rho[G])$. Teniendo en cuenta el isomorfismo natural $\rho[G] \cong G/\mathrm{N}(\chi)$, vemos que

$$Z(\chi)/\mathrm{N}(\chi) \leq Z(G/\mathrm{N}(\chi)).$$

Si σ pertenece a los centros de todos los caracteres irreducibles de G y $\tau \in G$, se cumple que $\sigma\tau\sigma^{-1}\tau^{-1} \in \mathrm{N}(\chi)$, y esto vale para todo carácter irreducible χ, luego $\sigma\tau\sigma^{-1}\tau^{-1} = 1$, lo que implica que $\sigma \in Z(G)$.

4) Si χ es un carácter irreducible y fiel de G (es decir, tal que $\mathrm{N}(\chi) = 1$), en 3) hemos probado que $Z(\chi) \leq Z(G)$, y también la inclusión opuesta, luego $Z(G) = Z(\chi)$. ∎

En particular, vemos que una condición necesaria para que un grupo G pueda tener un carácter irreducible y fiel es que $Z(G)$ sea cíclico. Hay ejemplos que muestran que no es suficiente.

6.4 Ejemplos y aplicaciones

Los caracteres de C_6 Por ejemplo, si $G = \langle g \rangle$ es un grupo cíclico de orden 6 y $\zeta \in \mathbb{C}$ es una raíz de la unidad de orden 3, entonces $-\zeta$ es una raíz de la unidad de orden 6, y es claro que cada homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$ cumple $\chi(g)^6 = 1$, luego $\chi(g) = (-\zeta)^i$, para cierto $i = 0, \ldots 5$, y estas 6 posibilidades nos dan los 6 caracteres de G:

$\mathrm{cl}(x)$	1	g	g^2	g^3	g^4	g^5
$\lvert\mathrm{cl}(x)\rvert$	1	1	1	1	1	1
χ_0	1	1	1	1	1	1
χ_1	1	$-\zeta$	ζ^2	-1	ζ	$-\zeta^2$
χ_2	1	ζ^2	ζ	1	ζ^2	ζ
χ_3	1	-1	1	-1	1	-1
χ_4	1	ζ	ζ^2	1	ζ	ζ^2
χ_5	1	$-\zeta^2$	ζ	-1	ζ^2	$-\zeta$

Los caracteres de D_8 Nos faltaba calcular los caracteres de grado 1 del grupo D_8. Observemos que el subgrupo derivado es $D_8' = \langle 1, \sigma^2 \rangle$, de modo que $D_8/D_8' \cong C_2 \times C_2$ tiene cuatro caracteres de grado 1, que son, por tanto, los caracteres que buscamos más el carácter trivial.

Como los elementos de D_8/D_8' tienen orden 2, sus caracteres sólo pueden tomar valores ± 1, lo que nos deja sólo cuatro posibilidades y, como necesitamos cuatro caracteres, todas las posibilidades corresponden realmente a caracteres del cociente. Así, la tabla de caracteres (irreducibles) de D_8 resulta ser:

$\mathrm{cl}(x)$	1	σ	σ^2	τ	$\sigma\tau$
$\lvert\mathrm{cl}(x)\rvert$	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ_5	2	0	-2	0	0

Notemos que podríamos haber calculado χ_5 a partir de los otros caracteres sin necesidad de conocer la representación que lo genera. Basta tener en cuenta que $r_G = \chi_1 + \chi_2 + \chi_3 + \chi_4 + 2\chi_5$ y que r_G toma siempre el valor 0 salvo en 1. ∎

Los caracteres de Q_8 El grupo cuaternio tiene cinco clases de conjugación:

$$\mathrm{cl}(Q_8) = \{\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}\}$$

Su subgrupo derivado es $Q_8' = \langle \pm 1 \rangle$ de modo que $Q_8/Q_8' \cong C_2 \times C_2$, luego este cociente determina exactamente los mismos cuatro caracteres de grado 1 de D_8. Esto implica que el quinto carácter ha de tener grado 2 y, teniendo en cuenta que puede calcularse a partir del carácter regular de Q_8, concluimos que la tabla de caracteres de Q_8 es idéntica a la de D_4:

$\mathrm{cl}(x)$	1	i	-1	j	k
$\lvert\mathrm{cl}(x)\rvert$	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ_5	2	0	-2	0	0

Vemos así que grupos no isomorfos pueden tener la misma tabla de caracteres. Una representación matricial que determina el carácter de grado 2 de Q_8 es la dada en [G 4.6]. ∎

La tabla de caracteres de Σ_3 El grupo Σ_3 tiene tres clases de conjugación, luego tres caracteres. Uno es el carácter trivial χ_1, otro el carácter del cociente $\Sigma_3/A_3 \cong C_2$, que asigna a cada permutación su signatura, y el tercero tiene que tener grado 2, para que $6 = 1^2 + 1^2 + 2^2$, y puede deducirse de las relaciones de ortogonalidad duales:

$\mathrm{cl}(x)$	1	(12)	(123)
$\lvert\mathrm{cl}(x)\rvert$	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

No obstante, es fácil encontrar una representación de Σ_3 que lo induce. En general, una representación de grado n de Σ_n es la que resulta de tomar un espacio vectorial $V = \langle e_1, \ldots, e_n \rangle$ de dimensión n y convertirlo en $\mathbb{C}[\Sigma_n]$-módulo mediante $e_i\sigma = e_{\sigma(i)}$, la matriz asociada a $\rho(\sigma)$ en la base $e_1, \ldots, e_n$ tiene un 1 en cada fila y 0 en las demás posiciones, y el 1 de la fila i-ésima está en la diagonal si y sólo si $\sigma(i) = 1$, por lo que el carácter χ asociado a esta representación viene dado por

$$\chi(\sigma) = |\{i \mid \sigma(i) = i\}|,$$

luego en el caso de Σ_3 viene dado por $\chi(1) = 3$, $\chi(12) = 1$, $\chi(123) = 0$.

En general, esta representación no es irreducible, pues $\langle e_1 + \cdots + e_n \rangle$ es un $\mathbb{C}[\Sigma_n]$-submódulo correspondiente a la representación trivial, pero en el caso de Σ_3 vemos que

$$\chi_3 = \chi - \chi_1$$

sí que es irreducible. ∎

La tabla de caracteres de Σ_4 Sea χ_1 el carácter trivial de Σ_4. Otro carácter χ_2 es el carácter no trivial de $\Sigma_4/A_4 \cong C_2$, que es el homomorfismo que asigna el -1 a las permutaciones impares. Otro carácter χ_3 es el asociado al carácter de grado 2 del cociente $\Sigma_4/V_4 \cong \Sigma_3$. Como tiene que haber 5 caracteres, los dos que faltan tienen que ser de grado 3, para que sea $24 = 1^2 + 1^2 + 2^2 + 3^2 + 3^2$.

Si al carácter asociado a la representación descrita en el ejemplo precedente le restamos el carácter principal, obtenemos un carácter χ_4 (el incluido en la tabla siguiente) que resulta ser irreducible, pues $(\chi_4, \chi_4) = 1$. El último carácter se deduce de las relaciones de ortogonalidad duales:

$\mathrm{cl}(x)$	1	(12)	(123)	(1234)	(12)(34)
$\lvert\mathrm{cl}(x)\rvert$	1	6	8	6	3
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

■

El teorema $p^a q^b$ de Burnside Una aplicación típica de la teoría de caracteres es la demostración del teorema de Burnside, que ya hemos usado en varias ocasiones. Se trata de un teorema muy difícil de probar si no se usan caracteres y con una prueba muy simple en términos de caracteres.

Necesitamos un resultado previo:

Teorema 6.39 *Sea χ un carácter irreducible de un grupo finito G y sea $\sigma \in G$ tal que $|\mathrm{cl}_G(\sigma)|$ sea primo con $\chi(1)$. Entonces $\chi(\sigma) = 0$ o bien $|\chi(\sigma)| = \chi(1)$.*

Demostración: Sean $u, v \in \mathbb{Z}$ tales que $u|\mathrm{cl}_G(\sigma)| + v\chi(1) = 1$. Entonces

$$\frac{u|\mathrm{cl}_G(\sigma)|\chi(\sigma)}{\chi(1)} + v\chi(\sigma) = \frac{\chi(\sigma)}{\chi(1)}.$$

El miembro izquierdo es un entero algebraico por el teorema 6.32, aplicado a la función de clases ψ que vale 1 sobre $\mathrm{cl}_G(\sigma)$ y 0 en las demás clases. Por consiguiente, el número $a = \chi(\sigma)/\chi(1)$ también es un entero algebraico.

Sea K la adjunción a $\mathbb{Q}$ de las raíces del polinomio mínimo de a sobre $\mathbb{Q}$ (de modo que $K/\mathbb{Q}$ es una extensión normal, por [Al 5.21]). Si $a = a_1, \ldots, a_n$ son estas raíces, tenemos [Al 5.23] que a_i es la imagen de a por un $\mathbb{Q}$-automorfismo de K. Como $\chi(\sigma)$ es suma de $\chi(1)$ raíces de la unidad, cada a_i es de la forma

$$\frac{\text{suma de } \chi(1) \text{ raíces de la unidad}}{\chi(1)},$$

luego $|a_i| \leq 1$. Por consiguiente $|\,\mathrm{N}_{\mathbb{Q}}^{K}(a)| \leq 1$ y esta norma es un entero algebraico [Al 8.9], a la vez que un número racional, luego ha de ser un número entero [Al 8.7], más concretamente, 0 o ± 1.

Si $\mathrm{N}_{\mathbb{Q}}^K(a) = 0$, entonces $a = 0$ y $\chi(\sigma) = 0$, mientras que si $\mathrm{N}_{\mathbb{Q}}^K(a) = \pm 1$, ha de ser $|a| = 1$, luego $|\chi(\sigma)| = \chi(1)$. ∎

Teorema 6.40 (Burnside) *Todo grupo de orden $p^a q^b$, con p y q primos, es resoluble.*

Demostración: Sea G un grupo de orden $p^a q^b$. Razonamos por inducción sobre el orden de G, es decir, suponemos que el teorema es cierto para todos los grupos de orden menor que $|G|$. Si G es abeliano, es trivialmente resoluble, luego podemos suponer que $Z(G) < G$.

Sea P un p-subgrupo de Sylow de G. Entonces $Z(P) \neq 1$, por 2.5, luego podemos tomar $\sigma \in Z(P)$ tal que $\sigma \neq 1$. Consideremos la clase de conjugación $C = \mathrm{cl}_G(\sigma)$. Entonces $P \leq C_G(\sigma)$, luego $p \nmid |G : C_G(\sigma)| = |C|$, luego $|C| = q^{b'}$, para cierto $b' \leq b$.

Basta probar que G tiene un subgrupo $1 < N \lhd G$, pues entonces N y G/N son resolubles por hipótesis de inducción, luego G también lo es. Supongamos que no es así, es decir, que G es un grupo simple no abeliano.

Si $b' = 0$, entonces $\sigma \in Z(G) \neq 1$, lo que nos da una contradicción. Supongamos, pues, que $b' > 0$. Sean $\chi_1, \ldots, \chi_h$ los caracteres irreducibles de G, donde $\chi_1 = 1$. El teorema 6.35 nos da que

$$0 = \sum_{i=1}^{h} \chi_i(1)\chi_i(\sigma) = 1 + \sum_{i=2}^{h} \chi_i(1)\chi_i(\sigma).$$

Podemos ordenar los caracteres de modo que $q \nmid \chi_i(1)$ para $1 \leq i \leq h_0$ y $q \mid \chi_i(1)$ para $h_0 < i \leq h$. En el primer caso, tenemos que $\chi_i(1)$ es primo con $|\mathrm{cl}_G(\sigma)|$, luego el teorema anterior nos da que $\chi_i(\sigma) = 0$ o bien $|\chi_i(\sigma)| = \chi_i(1)$. Si se da esta segunda posibilidad, como χ_i es fiel (porque G es simple), 6.38 nos da que $\sigma \in Z(G)$, lo cual es imposible. Por consiguiente, ha de ser $\chi_i(\sigma) = 0$. Esto nos reduce la igualdad anterior a

$$1 + \sum_{i=h_0+1}^{h} \chi_i(1)\chi_i(\sigma) = 0,$$

donde q divide a cada $\chi_i(1)$, pero esto es absurdo, porque nos permite expresar el número racional $1/q$ como combinación lineal entera de enteros algebraicos, lo que implica que $1/q \in \mathbb{Z}$. ∎

Una caracterización de los grupos abelianos Veamos ahora una curiosa caracterización de los grupos abelianos. Primero demostramos lo siguiente:

Teorema 6.41 *Si un grupo finito G tiene h clases de conjugación, entonces*

$$|G| + 3|G : G'| \geq 4h.$$

DEMOSTRACIÓN: Sean $n_1, \dots, n_h$ los grados de los caracteres irreducibles de G. Por la observación tras el teorema 6.37, de todos ellos, habrá $k = |G : G'|$ iguales a 1. Podemos suponer que son los k primeros, de modo que, por 6.26, se cumple que

$$|G| = k + n_{k+1}^2 + \cdots + n_h^2 \geq k + 4(h-k) = 4h - 3k.$$

∎

Ahora podemos probar que si la probabilidad de que dos elementos de un grupo finito conmuten es mayor que $5/8 = 0.625$, es que el grupo es abeliano:

Teorema 6.42 *Si G es un grupo finito y*

$$\frac{|\{(g,h) \in G \times G \mid gh = hg\}|}{|G|^2} > \frac{5}{8},$$

entonces G es abeliano.

DEMOSTRACIÓN: Basta observar que

$$|\{(g,h) \in G \times G \mid gh = hg\}| = \sum_{g \in G} |\{h \in G \mid gh = hg\}| = \sum_{g \in G} |C_G(g)|.$$

Si llamamos $c_1, \dots, c_h$ a las clases de conjugación de G, entonces, para cada $g \in c_i$, tenemos que $|c_i| = |G : C_G(g)|$, luego la suma anterior es

$$\sum_{i=1}^{h} \sum_{g \in c_i} \frac{|G|}{|c_i|} = \sum_{i=1}^{h} |c_i||G|/|c_i| = h|G|,$$

luego el cociente de la izquierda en el enunciado es $h/|G|$, luego la hipótesis es que $h/|G| > 5/8$. Por el teorema anterior,

$$|G| + 3|G : G'| \geq 4h > 5|G|/2,$$

luego $|G : G'| > |G|/2$, luego $|G'| < 2$, luego $G' = 1$, y esto significa que G es abeliano. ∎

El valor $5/8$ no puede reducirse, pues si un grupo cumple $|G : Z(G)| = 4$, la probabilidad de que dos de sus elementos conmuten es exactamente $5/8$. En efecto, si

$$G/Z(G) = \{Z(G), u_1Z(G), u_2Z(G), u_3Z(G)\},$$

los $|Z(G)|^2$ pares de $Z(G) \times Z(G)$ conmutan, al igual que los $3|Z(G)|^2$ pares de $Z(G) \times u_iZ(G)$, para $i = 1, 2, 3$, así como los de $u_iZ(G) \times Z(G)$ y los de $u_iZ(G) \times u_iZ(G)$. Esto hace un total de $10|Z(G)|^2$ pares, luego la probabilidad de conmutar es al menos

$$\frac{10|Z(G)|^2}{16|Z(G)|^2} = \frac{5}{8}.$$

Puesto que G no es abeliano, el teorema anterior implica que se cumple la igualdad.

Capítulo VII

Grupos de permutaciones II

En este capítulo vamos a profundizar en el estudio de los grupos de permutaciones. En principio, un grupo de permutaciones es un subgrupo G de un grupo simétrico Σ_Ω, pero conviene dar una definición ligeramente más general:

Definición 7.1 Un *grupo de permutaciones* sobre un conjunto Ω es un par (G, ρ), donde G es un grupo y $\rho : G \longrightarrow \Sigma_\Omega$ es un monomorfismo de grupos.

Equivalentemente, un grupo de permutaciones G es un grupo dotado de una acción fiel sobre un conjunto Ω, de modo que cada elemento de G puede identificarse con una permutación de Ω.

7.1 Grupos de permutaciones primitivos y múltiplemente transitivos

Recordemos que una acción de un grupo G sobre un conjunto Ω es transitiva si determina una única órbita, es decir, si cualquier elemento de Ω puede transformarse en cualquier otro mediante un elemento adecuado de G. Existen formas más fuertes de transitividad:

Definición 7.2 Una acción de un grupo G sobre un conjunto Ω es *k veces transitiva* si cuando $x_1, \ldots, x_k$ son elementos de Ω distintos dos a dos e $y_1, \ldots, y_k$ también, existe un $g \in G$ tal que $x_i g = y_i$ para $i = 1, \ldots, k$. Si el elemento g es único se dice que la acción es *estrictamente k-veces transitiva.*

Así las acciones "una vez transitivas" son simplemente las acciones transitivas. Las acciones k-veces transitivas, con $k \geq 2$ se llaman también *múltiplemente transitivas.* Las acciones estrictamente 1-transitivas se llaman acciones *regulares.*

Es obvio que si $1 \leq k \leq l$, toda acción l veces transitiva es también k veces transitiva.

Recordemos que si G actúa sobre Ω y $x, x' \in \Omega$, $g \in G$ cumplen $xg = x'$, entonces sus estabilizadores cumplen $G_x^g = G_{x'}$. En particular, si la acción es transitiva todos los estabilizadores son conjugados.

En tal caso, la acción es regular si y sólo si los estabilizadores son triviales (o, equivalentemente, si lo es uno cualquiera de ellos). En efecto, si $G_x = 1$ y $xg = xg' = x'$, entonces $xgg'^{-1} = x$, luego $gg'^{-1} \in G_x$, luego $g = g'$ y la acción es regular. Recíprocamente, si la acción es regular, el único $g \in G$ que cumple $xg = x$ tiene que ser $g = 1$, luego $G_x = 1$.

Ejemplos Un caso trivial de transitividad múltiple es la del grupo simétrico Σ_n, que es claramente n veces transitivo. En cambio, si consideramos la acción natural del grupo diédrico D_8 sobre los vértices de un cuadrado, vemos que se trata de un grupo de permutaciones transitivo no doblemente transitivo, pues ningún elemento de D_8 transforma un par de vértices contiguos en un par de vértices opuestos.

Si Ω es una recta proyectiva, cualquier terna de puntos distintos en Ω es un sistema de referencia proyectivo (definición [G 8.18]), luego el teorema [G 8.20] nos da que el grupo de las homografías de Ω es un grupo de permutaciones estrictamente triplemente transitivo sobre Ω.

Si Ω es una recta afín, el grupo de las afinidades de Ω es estrictamente doblemente transitivo sobre Ω.

Esto se puede probar análogamente al caso proyectivo (existe una única afinidad que transforma dos puntos afínmente independientes en otros dos) y también se deduce del ejemplo anterior teniendo en cuenta que las biyecciones afines de Ω se identifican con las homografías de la extensión de Ω a una recta proyectiva que fijan el punto infinito, con lo que, dados dos pares de puntos finitos distintos (x_1, x_2), (y_1, y_2), existe una única homografía (biyección afín) que transforma (x_1, x_2, ∞) en (y_1, y_2, ∞).

Tenemos así ejemplos de grupos transitivos no doblemente transitivos, de grupos doblemente transitivos no triplemente transitivos y de grupos triplemente transitivos no cuádruplemente transitivos. ∎

Teorema 7.3 *Sea G un grupo de permutaciones k veces transitivo sobre un conjunto Ω de cardinal n. Las afirmaciones siguientes son equivalentes:*

1. *G es estrictamente k veces transitivo.*
2. *Si $g \in G$ fija a k elementos de Ω entonces $g = 1$.*
3. *$|G| = n!/(n-k)!$.*

Si $k \geq 2$, estas afirmaciones equivalen también a

4. *Para cada $x \in \Omega$ el estabilizador G_x es estrictamente $k-1$ veces transitivo sobre $\Omega \setminus \{x\}$.*

DEMOSTRACIÓN: Claramente $1 \Rightarrow 2$, y también se cumple el recíproco, pues si tuviéramos g_1, g_2 en G tales que $x_j g_i = y_j$, para dos k-tuplas $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k)$ de elementos de Ω distintos dos a dos, entonces $x_j g_1 g_2^{-1} = x_j$ para todo j, luego $g_1 g_2^{-1} = 1$, luego $g_1 = g_2$, y la acción es estrictamente k veces transitiva.

Dado cualquier $x \in \Omega$, tenemos que el cardinal de su órbita (que es n) es el índice del estabilizador G_x, es decir, que $|G| = n|G_x|$. Si $k = 1$ la transitividad estricta equivale a que $|G_x| = 1$, luego también a que $|G| = n$, luego $1 \Leftrightarrow 3$.

A partir de aquí suponemos que $k \geq 2$ y observamos que si $x \in \Omega$, entonces G_x es claramente $k-1$ veces transitivo sobre $\Omega \setminus \{x\}$. Por lo tanto, por la equivalencia $1 \leftrightarrow 2$ ya probada, vemos que G_x es estrictamente $k-1$ veces transitivo sobre $\Omega \setminus \{x\}$ si y sólo si el único elemento de G_x que fija a $k-1$ elementos de $\Omega \setminus \{x\}$ es la identidad.

Esto implica a su vez que $2 \Leftrightarrow 4$, pues el hecho de que el único elemento de G que fija a k elementos de Ω sea la identidad equivale a que el único elemento de G_x que fije a todos los elementos de $\Omega \setminus \{x\}$ sea la identidad.

Finalmente observamos que si $x_1 \in \Omega$, entonces $|G| = n|G_{x_1}|$ y, a su vez, si $x_2 \in \Omega$ es distinto de x_1, tenemos que $|G| = n(n-1)|G_{x_1 x_2}|$, donde el último grupo es el estabilizador de x_2 en G_{x_1}, es decir, el subgrupo de los elementos de G que fijan a x_1 y x_2. De este modo llegamos a que

$$|G| = \frac{n!}{(n-k)!} G_{x_1 \cdots x_k},$$

pero, por 2), G es estrictamente k veces transitivo si y sólo si $G_{x_1 \cdots x_k} = 1$, lo que equivale a que $|G| = n!/(n-k)!$ y tenemos que $1 \Leftrightarrow 3$. ∎

Con esto obtenemos un segundo ejemplo elemental de transitividad múltiple:

Teorema 7.4 *Para cada n, el grupo Σ_n es estrictamente n veces transitivo y, si $n \geq 3$, el grupo A_n es estrictamente $n-2$ veces transitivo.*

DEMOSTRACIÓN: Ya hemos señalado que Σ_n es obviamente n veces transitivo.

Si $x_1, \ldots, x_{n-2}, y_1, \ldots, y_{n-2}$ son elementos de $\Omega = \{1, \ldots, n\}$ distintos dos a dos en cada bloque, podemos completarlos hasta $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ y considerar la permutación $g \in \Sigma_n$ dada por $g(x_i) = y_i$. Si g es impar, intercambiando y_{n-1}, y_n si es preciso podemos suponer que $x_n \neq y_n$, con lo que $f = g(x_n, y_n)$ es par y sigue cumpliendo $f(x_i) = y_i$ para $i = 1, \ldots, n-2$, luego A_n es $n-2$ veces transitivo, y la transitividad es estricta por el teorema anterior (apartado 3). ∎

Puede probarse que hay pocos grupos k-transitivos para $k \geq 4$. Para precisar esta afirmación necesitamos la noción obvia de isomorfismo de acciones:

Definición 7.5 Un *isomorfismo* entre dos acciones $\rho_i : \Omega_i \times G_i \longrightarrow \Omega_i$, para $i = 1, 2$ es un par (f, ϕ), donde $f : \Omega_1 \longrightarrow \Omega_2$ es una biyección y $\phi : G_1 \longrightarrow G_2$

es un isomorfismo de grupos de modo que, para todo $x \in \Omega_1$ y todo $g \in G_1$ se cumpla

$$f(xg) = f(x)\phi(g).$$

Puede probarse que todo grupo de permutaciones 6-transitivo es isomorfo (en el sentido de la definición anterior) a Σ_n, para $n \geq 6$ o bien a A_n para $n \geq 8$, mientras que, de grupos cuatro o cinco veces transitivos (además de los Σ_n, para $n \geq 4$ y A_n, para $n \geq 6$), sólo hay cinco ejemplos más, que son los cinco grupos de Mathieu que presentaremos en la sección 7.3.

Ahora vamos a estudiar una propiedad una propiedad intermedia entre la transitividad y la transitividad doble:

Definición 7.6 Sea G un grupo que actúe transitivamente sobre un conjunto Ω. Si $\Delta \subset \Omega$ es un conjunto no vacío, diremos que es un *bloque* si para todo $g \in G$ se cumple que $\Delta g = \Delta$ o $\Delta \cap \Delta g = \varnothing$. Diremos que es un bloque *trivial* si $\Delta = \Omega$ o bien Δ tiene un único elemento. La acción de G sobre Ω es *primitiva* si no tiene bloques no triviales. Es frecuente hablar de *grupos primitivos* en el sentido de grupos dotados de una acción primitiva.

Es obvio que los bloques triviales son bloques. En la acción de D_4 sobre los vértices de un cuadrado, dos vértices opuestos son un ejemplo de bloque no trivial.

Es inmediato que toda acción doblemente transitiva es primitiva, pues si Δ no es un bloque trivial, podemos tomar dos elementos distintos $a, b \in \Delta$ y un $c \in \Omega \setminus \Delta$, y tiene que existir un $g \in G$ tal que $ag = a$, $bg = c$, con lo que $a \in \Delta \cap \Delta g$, pero $\Delta \neq \Delta g$.

Teorema 7.7 *Sea G un grupo que actúe transitivamente sobre un conjunto Ω y sea $a \in \Omega$. Entonces G es primitivo si y sólo si el estabilizador G_a es un subgrupo maximal, es decir, si no hay ningún subgrupo $G_a < H < G$.*

Demostración: Observemos que, como la acción es transitiva, todos los estabilizadores son conjugados, luego que uno sea maximal es equivalente a que lo sean todos.

Si B es un bloque no trivial y $a \in B$, entonces $G_a < G_B < G$, donde G_B es el subgrupo formado por los $f \in G$ tales que $f[B] = B$. En efecto, si $f \in G_a$, entonces $a \in f[B] \cap B$, luego $f[B] = B$, pero si $b \in B$, $b \neq a$, existe $f \in G$ tal que $f(a) = b$, y entonces $b \in f[B] \cap B$, luego $f[B] = B$, y así $f \in G_B \setminus G_a$. También es obvio que $G_B < G$. Por lo tanto, G_a no es un subgrupo maximal.

Recíprocamente, si existe un subgrupo $G_a < H < G$, consideremos el conjunto $B = \{h(a) \mid h \in H\} \subset \Omega$. Se trata de un bloque, pues si $f \in H$, claramente $f[B] = B$, y vamos a ver que si $f \in G \setminus H$, entonces $f[B] \cap B = \varnothing$.

En efecto, si $x \in g[B] \cap B$, existen $h, h' \in H$ tales que $x = h(a) = g(h'(a))$, luego $h'gh^{-1} \in G_a \leq H$, luego $g \in H$. ∎

Ejemplo *El grupo cíclico $C_n = \langle (1, 2, \ldots, n) \rangle \leq \Sigma_n$ es transitivo, pero no doblemente transitivo si $n \geq 4$, y es primitivo si y sólo si n es primo.*

En efecto, C_n transforma puntos consecutivos en puntos consecutivos, luego no es doblemente transitivo si $n \geq 4$. Por otra parte, los estabilizadores son triviales, luego son maximales si y sólo si C_n no tiene subgrupos propios, es decir, si y sólo si n es primo. ∎

Ejercicio: Adaptar el argumento del ejemplo anterior al grupo D_{2n}, visto como grupo de simetrías de un n-ágono regular.

Criterios de simplicidad Hay condiciones sencillas que garantizan que un grupo primitivo o múltiplemente transitivo es simple. Vamos a obtener algunas de ellas. Para ello probamos un par de resultados sobre subgrupos normales de grupos de permutaciones:

Teorema 7.8 *Si un grupo G actúa transitivamente sobre un conjunto Ω y $N \trianglelefteq G$, entonces las órbitas de N en Ω son bloques para la acción de G. En particular, si G es primitivo, la acción de N es trivial o transitiva.*

Demostración: Sea Δ una órbita de N en Ω. Entonces, si $g \in G$, es claro que Δg es una órbita para la acción de $N^g = N$, pero dos órbitas tienen que ser iguales o disjuntas, luego Δ es un bloque para G. Si G es primitivo pero la acción de N no es transitiva, entonces las órbitas de N son distintas de Ω, luego son todas triviales, luego la acción de N es trivial. ∎

Teorema 7.9 *Si G es un grupo de permutaciones primitivo sobre un conjunto Ω y existe $x \in \Omega$ tal que el estabilizador G_x es simple, entonces todo subgrupo normal propio de G actúa regularmente sobre Ω.*

Demostración: Sea $1 < N \lhd G$. El teorema 7.8 nos da que N es transitivo (ya que su acción no puede ser trivial, porque G es un grupo de permutaciones). Observemos que, como los estabilizadores son conjugados, la hipótesis implica que todos son simples, luego si $x \in \Omega$, tenemos que $N \cap G_x \trianglelefteq G_x$, luego, o bien $N \cap G_x = 1$, o bien $G_x \leq N$, pero G_x es maximal, por 7.7, luego $N = G_x$, pero esto es imposible, pues todos los estabilizadores serían iguales a N y entonces $N = 1$. Por consiguiente, es $N_x = N \cap G_x = 1$ para todo $x \in \Omega$, luego la acción de N en Ω es regular. ∎

Ahora necesitamos un último hecho técnico:

Teorema 7.10 *Sea G un grupo que actúa transitivamente sobre un conjunto Ω, sea $H \trianglelefteq G$ un subgrupo que actúe regularmente sobre Ω y sea $x \in \Omega$. Entonces la acción de G_x en $\Omega \setminus \{x\}$ es isomorfa a su acción por conjugación sobre $H \setminus \{1\}$.*

Demostración: Definimos $f : H \setminus \{1\} \longrightarrow \Omega \setminus \{x\}$ mediante $f(h) = xh$. Claramente es una biyección, pues no puede ser $xh = x$, ya que la regularidad implica entonces que $h = 1$, la propia definición de acción implica que f es inyectiva y la transitividad implica que f es suprayectiva. Además, si $g \in G_x$, $h \in H \setminus \{1\}$, tenemos que

$$f(h^g) = xg^{-1}hg = xhg = f(h)g.$$

∎

Veamos ahora las consecuencias de que un grupo de permutaciones tenga un subgrupo normal regular:

Teorema 7.11 *Sea G un grupo que actúa k-transitivamente sobre un conjunto Ω con $|\Omega| = n$ y $k \geq 2$, y sea $H \trianglelefteq G$ un subgrupo que actúe regularmente sobre Ω. Entonces $k \leq 4$ y además:*

1. *Existe un primo p tal que $H \cong C_p^r$ y $n = p^r$.*
2. *Si $k \geq 3$, o bien $H \cong C_3$ y $n = 3$ o bien $H \cong C_2^r$ y $n = 2^r$.*
3. *Si $k = 4$ entonces $H \cong C_2 \times C_2$ y $n = 4$.*

Demostración: 1) Fijado $x \in \Omega$, como G actúa k-transitivamente sobre Ω, es claro que G_x es $k-1$-transitivo sobre $\Omega \setminus \{x\}$, luego, por 7.10 la acción de G_x sobre $H \setminus \{1\}$ por conjugación también es $k-1$-transitiva (en particular, transitiva, pues $k \geq 2$). Esto implica que todos los elementos de $H \setminus \{1\}$ son conjugados, luego todos tienen el mismo orden p, que necesariamente será primo (pues en todo grupo hay elementos de orden primo). Por lo tanto, $|H| = p^r$, para cierto r. Por otro lado, como H es regular sobre Ω, resulta que $n = |\Omega| = |H| = p^r$.

Además, $1 < Z(H) \trianglelefteq G$ y la acción de $Z(H)$ sobre Ω no es trivial (porque H es regular), luego 7.8 nos da que $Z(H)$ actúa transitivamente sobre Ω, y como la acción de H es regular, la de $Z(H)$ también lo es, luego $|Z(H)| = |\Omega| = |H|$, luego H es abeliano, y así $H \cong C_p^r$.

2) Si $h \in H \setminus \{1\}$, es claro que $\{h, h^{-1}\}$ es un bloque para la acción de G_x, pero si $k \geq 3$ la acción de G_x es doblemente transitiva, luego primitiva, luego $\{h, h^{-1}\} = H \setminus \{1\}$ o bien $\{h, h^{-1}\} = \{h\}$. En el primer caso $|H| = 3$ y en el segundo $h^2 = 1$, luego $p = 2$.

3) Si $k \geq 4$ tiene que ser $|H| = |\Omega| \geq 4$, luego el apartado anterior nos da que $H \cong C_2^r$ con $r \geq 2$, luego existe $V \leq H$ tal que $V \cong C_2 \times C_2$. Tomemos $h \in H$, de modo que la acción de $(G_x)_h$ sobre $H \setminus \{1, h\}$ es doblemente transitiva, luego primitiva. Sin embargo, si $V = \{1, h, h', h''\}$, tenemos que $B = \{h', h''\}$ es un bloque, pues si $g \in (G_x)_h$ y $h' \in \{h', h''\} \cap \{h'^g, h''^g\}$, o bien $h' = h'^g$, en cuyo caso $h''^g = (hh')^g = hh' = h''$, con lo que $B = g[B]$, o bien $h' = h''^g$, en cuyo caso $h'^g = h^g h''^g = hh' = h''$, y nuevamente $B = g[B]$. Por lo tanto, $\{h', h''\} = H \setminus \{1, h\}$, luego $H = \{1, h, h', h''\} = V$ y $k \leq n = 4$.

Como hemos probado esta última parte bajo la hipótesis $k \geq 4$, de hecho hemos probado que no puede ser $k > 4$. ∎

De aquí obtenemos inmediatamente un criterio sencillo de simplicidad:

Teorema 7.12 *Sea G un grupo de permutaciones k-transitivo sobre un conjunto Ω, con $|\Omega| = n$ y $k \geq 2$. Supongamos que, para cierto $x \in \Omega$, el estabilizador G_x es simple.*

1. *Si n no es potencia de primo, entonces G es simple.*
2. *Si $k \geq 3$ y n no es potencia de 2, entonces $G = \Sigma_3$ o bien G es simple.*
3. *Si $k \geq 4$, entonces G es simple.*

DEMOSTRACIÓN: Si G no es simple, tiene un subgrupo normal propio N que, por el teorema 7.9, actúa regularmente sobre Ω, luego el teorema anterior nos da que $k \leq 4$ y que n es potencia de primo, de donde se sigue 1).

Si suponemos que $k \geq 3$, el teorema anterior nos da que $n = 3$, en cuyo caso $G \cong \Sigma_3$, pues un subgrupo triplemente transitivo de Σ_3 tiene que ser Σ_3, o bien n es potencia de 2, lo que implica 2).

Finalmente, si $k = 4$ tiene que ser $n = 4$, pero el único subgrupo cuatro veces transitivo de Σ_4 es el propio Σ_4 y sus estabilizadores son isomorfos a Σ_3, que no son simples, luego tenemos una contradicción y concluimos que G es simple. ∎

Por ejemplo, teniendo en cuenta que A_n es cuatro veces transitivo para $n \geq 6$ y que los estabilizadores de A_n son isomorfos a A_{n-1}, el teorema anterior implica que para probar que A_n es simple para todo $n \geq 5$ basta probar que A_5 lo es.

Para grupos primitivos, no necesariamente múltiplemente transitivos, existe también un criterio algo más técnico, pero muy útil:

Teorema 7.13 (Iwasawa) *Sea G un grupo de permutaciones primitivo sobre un conjunto Ω tal que $G = G'$. Sea $H = G_a$, para cierto $a \in \Omega$ y supongamos que existe un subgrupo resoluble $A \trianglelefteq H$ cuya envoltura normal en G es el propio G. Entonces G es simple.*

DEMOSTRACIÓN: Sea $1 < N \trianglelefteq G$. Como G es un grupo de permutaciones, la acción de N en Ω no puede ser trivial, luego por 7.8 tenemos que N actúa transitivamente, luego $NH = G$ (dado $g \in G$, existe un $n \in N$ tal que $ag = an$, luego $agn^{-1} = a$, luego $gn^{-1} \in H$, luego $g \in NH$). Como $N \triangleleft G$ y $A \trianglelefteq H$, tenemos que $H \leq N_G(NA)$ y, como $NH = G$, resulta que $NA \trianglelefteq G$. Como G es la envoltura normal de A, tiene que ser $G = NA$.

Como A es resoluble, también lo es $G/N \cong A/(N \cap A)$. Si fuera $N < G$, es decir, si $G/N \neq 1$, tendría que ser $(G/N)' < G/N$, pero, como $G = G'$, también $G/N = (G/N)'$, luego tiene que ser $G = N$. ∎

En la sección siguiente usaremos este criterio para probar la simplicidad de una familia de grupos.

7.2 Los grupos lineales especiales proyectivos

En toda esta sección V será un espacio vectorial de dimensión finita $n \geq 2$ sobre un cuerpo k. Usaremos la notación $\mathrm{LG}(V)$ para referirnos al grupo de los automorfismos de V, que es isomorfo [Al 4.37] al grupo $\mathrm{LG}(n, k)$ de las matrices regulares $n \times n$ con coeficientes en k. Un isomorfismo es el que a cada automorfismo le asigna su matriz en una base de V prefijada). En lo sucesivo trataremos indistintamente con un grupo u otro, según nos interese ver a sus elementos como automorfismos o como matrices.

Según [Al 4.39], el centro de $\mathrm{LG}(n, k)$ es el subgrupo $Z(n, k) \cong k^*$ formado por las matrices escalares, es decir, las matrices de la forma αI, con $\alpha \in k^*$.

El cociente

$$\mathrm{LGP}(V) = \mathrm{LG}(V)/Z(V)$$

recibe el nombre de *grupo lineal general proyectivo* de V, porque sus elementos pueden identificarse con las homografías del espacio proyectivo $P(V)$ (véase la sección [G 8.2]).

Por otro lado tenemos la aplicación determinante $\det : \mathrm{LG}(n,k) \longrightarrow k^*$, que es un epimorfismo de grupos cuyo núcleo es el *grupo lineal especial*

$$\mathrm{LE}(n,k) \trianglelefteq \mathrm{LG}(n,k),$$

formado por las matrices regulares $n \times n$ con determinante 1.

Llamando $\mathrm{ZE}(V) = \mathrm{LE}(V) \cap Z(V)$, podemos formar el *grupo lineal especial proyectivo*

$$\mathrm{LEP}(V) = \mathrm{LE}(V)/\mathrm{ZE}(V),$$

que podemos identificar con un subgrupo $\mathrm{LEP}(V) \trianglelefteq \mathrm{LGP}(V)$.

Vamos a probar que, salvo unas pocas excepciones, los grupos $\mathrm{LEP}(V)$ son simples.

En particular esto se aplica al caso en que el cuerpo k es finito. Según el teorema [Al 9.2], si q es una potencia de primo, existe un cuerpo k con q elementos y es único salvo isomorfismo. Usaremos la notación $\mathrm{LG}(n,q)$ para referirnos al grupo lineal general $\mathrm{LG}(n,k)$ cuando k es el cuerpo de q elementos, y análogamente escribiremos $\mathrm{LE}(n,q)$, $\mathrm{LEP}(n,q)$, etc. En 5.41 hemos probado que $\mathrm{LG}(3,2)$ es un grupo simple de orden 168.

Es fácil calcular los órdenes de los grupos. En primer lugar:

$$|\mathrm{LG}(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = q^{(n-1)n/2}\prod_{i=1}^{n}(q^i-1).$$

En efecto, fijada una base $e_1,\dots,e_n$ de V, un automorfismo $f : V \longrightarrow V$ puede enviar e_1 a cualquiera de los q^n-1 vectores no nulos de V, mientras que $f(e_2)$ puede ser cualquiera de los q^n-q vectores de $V \setminus \langle f(e_1)\rangle$, y $f(e_3)$ puede ser cualquiera de los q^n-q^2 vectores de $V \setminus \langle f(e_1), f(e_2)\rangle$, etc., luego las posibilidades para f son las que da la fórmula anterior.

Es claro que la aplicación determinante $\det : \mathrm{LG}(n,q) \longrightarrow k^*$ es un epimorfismo de grupos luego el teorema de isomorfía nos da que su núcleo tiene índice $q-1$ en $\mathrm{LG}(n,q)$. Por consiguiente:

$$|\mathrm{LE}(n,q)| = q^{(n-1)n/2}\prod_{i=1}^{n-1}(q^{i+1}-1).$$

Por otro lado, es claro que $|Z(n,q)| = |k^*| = q-1$, por lo que

$$|\mathrm{LGP}(n,q)| = |\mathrm{LE}(n,q)| = q^{(n-1)n/2}\prod_{i=1}^{n-1}(q^{i+1}-1).$$

A su vez, $\mathrm{ZE}(n,q)$ es el grupo formado por las matrices de la forma αI con $\det(\alpha I) = \alpha^n = 1$. Como el grupo $Z(n,q)$ es cíclico de orden $q-1$, también lo es su subgrupo $\mathrm{ZE}(n,q)$, y un generador M tiene que cumplir que $o(M) \mid q-1$ y $o(M) \mid n$, luego $o(M) = (n, q-1)$, ya que ciertamente $Z(n,q)$ tiene que contener elementos de orden $(n, q-1)$. Por lo tanto:

$$|\mathrm{ZE}(n,q)| = (n, q-1),$$

y así

$$|\mathrm{LEP}(n,q)| = \frac{q^{(n-1)n/2}}{(n,q-1)} \prod_{i=1}^{n-1} (q^{i+1} - 1).$$

Observemos que si hemos podido demostrar la simplicidad de $\mathrm{LG}(3,2)$ es porque "casualmente" $\mathrm{LG}(3,2) = \mathrm{LE}(3,2) = \mathrm{LEP}(3,2)$, por lo que, "en realidad", lo que hemos probado en 5.41 es la simplicidad de $\mathrm{LEP}(3,2)$.

La tabla siguiente contiene los órdenes de los primeros grupos $\mathrm{LEP}(2,q)$:

q	2	3	4	5	7	8	9	11
$\lvert\mathrm{LEP}(2,q)\rvert$	6	12	60	60	168	504	360	660
q	13	16	17	19	23	25	27	29
$\lvert\mathrm{LEP}(2,q)\rvert$	1 092	4 080	2 448	3 420	6 072	7 800	9 828	12 180

Para $n \geq 3$ los órdenes crecen mucho más rápidamente:

q	2	3	4	5
$\lvert\mathrm{LEP}(3,q)\rvert$	168	5 616	20 160	372 000
$\lvert\mathrm{LEP}(4,q)\rvert$	20 160	6 065 280	987 033 600	7 254 000 000

Lo primero que observamos es que $\mathrm{LEP}(2,2)$ y $\mathrm{LEP}(2,3)$ no pueden ser simples. De hecho,

$$\mathrm{LEP}(2,2) \cong \Sigma_3, \qquad \mathrm{LEP}(2,3) \cong A_4.$$

Más aún, $\mathrm{LGP}(2,3) \cong \Sigma_4$, pues se trata del grupo de las homografías de la recta proyectiva sobre el cuerpo de 3 elementos, que tiene 4 puntos, luego tenemos un monomorfismo natural $\mathrm{LGP}(2,3) \longrightarrow \Sigma_4$ y, como ambos grupos tienen el mismo orden, tiene que ser un isomorfismo. El mismo argumento prueba que $\mathrm{LEP}(2,2) = \mathrm{LGP}(2,2) \cong \Sigma_3$ o que $\mathrm{LGP}(2,5) \cong \Sigma_5$.

En esta sección demostraremos que todos los demás grupos $\mathrm{LEP}(V)$ son simples. Admitiendo esto, las tablas anteriores nos permiten extraer varias consecuencias. Por una parte

$$\mathrm{LEP}(2,4) \cong \mathrm{LEP}(2,5) \cong A_5,$$

puesto que A_5 es el único grupo simple de orden 60 (aunque el segundo isomorfismo se sigue inmediatamente de $\mathrm{LGP}(2,5) \cong \Sigma_5$). También vemos que

$$\mathrm{LEP}(2,7) \cong \mathrm{LEP}(3,2),$$

pues ambos tienen que ser el único grupo simple de orden 168, e igualmente

$$\mathrm{LEP}(2,9) \cong A_6.$$

Vemos también que $\mathrm{LEP}(3,4)$ y $\mathrm{LEP}(4,2)$ tienen el mismo orden, y no es un orden cualquiera, sino que es precisamente el orden de A_8. En 7.43 probaremos que

$$\mathrm{LEP}(4,2) \cong A_8,$$

pero en cambio:

Teorema 7.14 *Los grupos A_8 y $\mathrm{LEP}(3,4)$ no son isomorfos.*

Demostración: Las permutaciones

$$(1,2)(3,4), \qquad (1,2)(3,4)(5,6)(7,8)$$

son pares, luego están en A_8, y no son conjugadas. Basta probar que en $\mathrm{LEP}(3,4)$ cualquier par de elementos de orden 2 son conjugados.

Sea $k = \{0, 1, \alpha, \alpha^2\}$ el cuerpo de 4 elementos, donde $\alpha^3 = 1$. Entonces $\mathrm{ZE}(3,4) = \{I, \alpha I, \alpha^2 I\}$. Un elemento de $\mathrm{LEP}(3,4)$ de orden 2 es la clase de una matriz $A \in \mathrm{LE}(3,4)$ que no sea escalar, es decir, de la forma aI, pero cuyo cuadrado sí que lo sea. Así pues, tiene que ser $A^2 = I$, $A^2 = \alpha I$ o $A^2 = \alpha^2 I$. En el segundo caso, la matriz αA determina la misma clase en $\mathrm{LEP}(3,4)$ y cumple $(\alpha A)^2 = I$, y en el tercer caso sucede lo mismo con $\alpha^2 A$, luego, cambiando si es preciso el representante de la clase, podemos suponer que $A^2 = I$.

Sea C la forma canónica de A en el sentido del teorema [Al 6.30]. La relación entre A y C es que $C = P^{-1}AP$, para cierta matriz $P \in \mathrm{LG}(3,4)$. Esto hace que C no sea escalar, pero $C^2 = I$.

Si C consta de tres cajas M_i de dimensión 1×1, entonces C es diagonal:

$$C = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}, \qquad C^2 = \begin{pmatrix} a^2 & 0 & 0 \\ 0 & b^2 & 0 \\ 0 & 0 & c^2 \end{pmatrix},$$

luego $a^2 = b^2 = c^2$, pero, como el cuerpo k tiene característica 2, esto implica que $a = b = c$, luego C es escalar y tenemos una contradicción. Si C consta de una única caja, entonces

$$C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & b & c \end{pmatrix},$$

y C^2 tiene el valor 0 en la posición $(1,1)$, con lo que no puede ser escalar. La única opción es que C conste de dos cajas:

$$C = \left(\begin{array}{c|cc} a & 0 & 0 \\ \hline 0 & 0 & 1 \\ 0 & b & c \end{array}\right),$$

y la condición $C^2 = I$ fuerza a que

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Así pues, hemos probado que todo elemento de orden 2 de $\mathrm{LEP}(3,4)$ es la clase de una matriz $A \in \mathrm{LE}(3,4)$ conjugada en $\mathrm{LG}(3,4)$ a esta matriz C. Si probamos que ambas son conjugadas en $\mathrm{LE}(3,4)$, podremos concluir que la clase de A en $\mathrm{LEP}(3,4)$ es conjugada en $\mathrm{LEP}(3,4)$ a la clase de C y el teorema quedará probado.

Ahora bien para ello basta observar que $H = \mathrm{LE}(3,4)$ es un subgrupo normal de $G = \mathrm{LG}(3,4)$, que $|G:H| = 3$ y que $C_H(C) < C_G(C)$, ya que la matriz

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

conmuta con C y no está en H. El teorema siguiente nos da la conclusión. ∎

Teorema 7.15 *Si H es un subgrupo normal de índice primo en un grupo G y $c \in H$ cumple que $C_H(c) < C_G(c)$, entonces todo $a \in H$ conjugado con c en G, es conjugado con c en H.*

Demostración: Tenemos que $C_H(c) = C_G(c) \cap H$, luego

$$1 \neq C_G(c)/C_H(c) \cong C_G(c)H/H \leq G/H,$$

y, como G/H tiene orden primo p, tiene que darse la igualdad, luego se cumple que $|C_G(c)| = p|C_H(c)|$, y esto implica a su vez que

$$|\mathrm{cl}_H(c)| = |H : C_H(c)| = |G : C_G(c)| = |\mathrm{cl}_G(c)|,$$

luego c tiene los mismos conjugados en H y en G. ∎

Para probar la simplicidad de los grupos $\mathrm{LEP}(V)$ llamemos M_{ij} a la matriz $n \times n$ sobre k que tiene todos sus coeficientes nulos excepto un 1 en el lugar (i,j). Entonces, según [Al 6.22] (véase la nota al pie) el grupo $\mathrm{LE}(V)$ de los automorfismos de V de determinante 1 está generado por las transvecciones que, en una base prefijada de V, admiten una matriz de la forma

$$T_{ij}(\alpha) = I + \alpha M_{ij},$$

con $i \neq j$ y $\alpha \in k^*$. Equivalentemente, el grupo $\mathrm{LE}(n,k)$ está generado por estas matrices. Observemos además que

$$M_{ij}M_{kl} = \begin{cases} M_{il} & \text{si } j = k, \\ 0 & \text{en otro caso.} \end{cases}$$

Con esto podemos probar lo siguiente:

Teorema 7.16 *Si $n \geq 3$ o bien $n = 2$ y $|k| > 3$. Entonces $G = \mathrm{LE}(n,k)$ cumple $G = G'$.*

Demostración: Basta probar que todas las matrices $T_{ij}(\alpha)$ son conmutadores. Observemos que si $i \neq j$, entonces $M_{ij}^2 = 0$, luego

$$(I - \alpha M_{ij})(I + \alpha M_{ij}) = I,$$

luego $(I + \alpha M_{ij})^{-1} = I - \alpha M_{ij}$.

Supongamos en primer lugar que $n \geq 3$ y consideremos tres índices distintos $1 \leq i, j, k \leq n$. Entonces

$$M_{ik}^{I+\alpha M_{kj}} = (I - \alpha M_{kj}) M_{ik} (I + \alpha M_{kj}) = M_{ik} + \alpha M_{ij},$$

luego

$$(I + M_{ik})^{I+\alpha M_{kj}} = (I - \alpha M_{kj})(I + M_{ik})(I + \alpha M_{kj}) =$$

$$((1 - \alpha M_{kj}) + (1 - \alpha M_{kj}) M_{ik})(I + \alpha M_{kj}) = I + M_{ik} + \alpha M_{ij},$$

luego

$$[I + M_{ij}, I + \alpha M_{kj}] = (I + M_{ij})^{-1} (I + M_{ik})^{I+\alpha M_{kj}} =$$

$$(I - M_{ij})(I + M_{ik} + \alpha M_{ij}) = I + \alpha M_{ij} = T_{ij}(\alpha).$$

Así pues, todas las transvecciones son conmutadores, como había que probar. Supongamos ahora que $n = 2$, tomemos $\beta, \gamma \in k$ no nulos y consideremos las matrices

$$B = \begin{pmatrix} \beta^{-1} & 0 \\ 0 & \beta \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}.$$

Un cálculo rutinario muestra que

$$[B, C] = \begin{pmatrix} 1 & \gamma(1 - \beta^2) \\ 0 & 1 \end{pmatrix}.$$

Si $|k| > 3$, dado $\alpha \in k$ no nulo, podemos tomar $\beta \in k$ tal que $\beta \neq \pm 1$, con lo que $1 - \beta^2 \neq 0$, y a su vez podemos tomar γ tal que $\alpha = \gamma(1 - \beta^2)$, y entonces $[B, C] = T_{1,2}(\alpha)$. Esto implica a su vez que $[(C^{-1})^t, (B^{-1})^t] = T_{2,1}(\alpha)$, luego concluimos igualmente que todas las transvecciones son conmutadores. ∎

Como $\mathrm{LGP}(V)$ se identifica con el grupo de las homografías del espacio proyectivo $\Omega = P(V)$ de dimensión $n - 1$, podemos ver a $\mathrm{LGP}(V)$ y a $\mathrm{LEP}(V)$ como grupos de permutaciones sobre Ω.

Teorema 7.17 *Si $n \geq 3$ o bien $n = 2$ y $|k| > 3$. Entonces el grupo $\mathrm{LEP}(n,k)$ es simple.*

Demostración: Consideremos $V = k^n$, de modo que podemos identificar $\mathrm{LE}(V)$ con $E = \mathrm{LE}(V)$ y, llamando $Z = \mathrm{ZE}(V)$, $\mathrm{LEP}(V) \cong \bar{E} = E/Z$. Basta probar que $\bar{E}$ cumple las hipótesis del teorema de Iwasawa.

En primer lugar probamos que $\bar{E}$ es doblemente transitivo sobre Ω, con lo que en particular es primitivo. En efecto, si $\langle u_1\rangle, \langle u_2\rangle$ y $\langle v_1\rangle, \langle v_2\rangle$ son dos pares de puntos distintos en Ω (con lo que u_1, u_2 y v_1, v_2 son dos pares de vectores linealmente independientes en V, podemos completar bases $u_1, \ldots, u_n$, $v_1, \ldots, v_n$ y considerar el automorfismo $f \in \mathrm{LG}(V)$ que cumple $f(u_i) = v_i$. Si el determinante de f es α, consideramos el automorfismo $g \in \mathrm{LG}(V)$ dado por $g(v_1) = \alpha^{-1}v_1$ y $g(v_i) = v_i$, cuyo determinante es α^{-1} y así $h = fg \in \mathrm{LE}(V)$ cumple que $h(\langle u_i\rangle) = \langle v_i\rangle$ y la imagen $\bar{h} \in \bar{E}$ cumple lo mismo.

El teorema 7.16 prueba que $E' = E$, de donde se sigue que $\bar{E}' = \bar{E}$.

Consideremos la base canónica $v_1, \ldots, v_n$ de $V = k^n$. Llamemos H_j al estabilizador de $V_j = \langle v_j\rangle$ en E. Entonces H_j actúa sobre el espacio cociente V/V_j, con lo que tenemos un homomorfismo de grupos $H_j \longrightarrow \mathrm{LG}(V/V_j)$. Llamemos $A_j \trianglelefteq H_j$ a su núcleo. Así, A_j está formado por todas las matrices de E que fijan al subespacio V_j y que actúan trivialmente sobre V/V_j. Por lo tanto, todo $a \in A_1$ tiene que ser de la forma

$$a = \left(\begin{array}{c|ccc} \alpha_1 & 0 & \cdots & 0 \\ \hline \alpha_2 & 1 & & 0 \\ \vdots & & \ddots & \\ \alpha_n & & & 1 \end{array}\right).$$

Además, $\det a = 1$, luego $\alpha_1 = 1$ y así

$$a = I + \sum_{i\neq 1} \alpha_i M_{i,1}.$$

El mismo argumento se aplica si $a \in A_j$, y la conclusión es que

$$a = I + \sum_{i\neq j} \alpha_i M_{ij}.$$

Recíprocamente, es claro que toda matriz de esta forma está en A_j. El producto en A_j viene dado por

$$\left(I + \sum_{i\neq j} \alpha_i M_{ij}\right)\left(I + \sum_{i\neq j} \beta_i M_{ij}\right) = \left(I + \sum_{i\neq j} (\alpha_i + \beta_i) M_{ij}\right),$$

de donde se sigue que A_j es un grupo abeliano. Como E actúa transitivamente en Ω, los estabilizadores H_j son conjugados, y es fácil ver que la conjugación que transforma un H_j en $H_{j'}$ también transforma A_j en $A_{j'}$, por lo que los subgrupos A_j también son conjugados. Por lo tanto, la envoltura normal de A_1 contiene a todos los A_j, y cada A_j contiene las transvecciones $T_{ij}(\alpha)$ (para el j correspondiente), luego la envoltura normal de A_1 contiene todos los generadores de E, luego es el propio E.

Todo esto se traduce al cociente $\bar{E}$, es decir, el estabilizador de $\langle v_1\rangle$ es $H = H_1/Z$, que tiene como subgrupo normal a $A = A_1Z/Z$, que es abeliano, luego resoluble, y su clausura normal en $\bar{E}$ es todo $\bar{E}$. El teorema de Iwasawa implica entonces que $\bar{E}$ es simple. ∎

Así pues, ahora conocemos dos familias infinitas de grupos simples finitos, la de los grupos alternados A_n, salvo A_4, y la de los grupos $\mathrm{LEP}(n,q)$, salvo $\mathrm{LEP}(2,2)$ y $\mathrm{LEP}(2,3)$. La tabla siguiente contiene todos los órdenes de grupos simples menores de 25 000. Cada par (n,q) hace referencia al grupo $\mathrm{LEP}(n,q)$:

A_5, $(2,4),(2,5)$	60	$(2,13)$	1 092	$(3,3)$	5 616	$(2,27)$	9 828
$(2,7),(3,2)$	168	$(2,17)$	2 448	?	6 048	$(2,29)$	12 180
A_6, $(2,9)$	360	A_7	2 520	$(2,23)$	6 072	$(2,31)$	14 880
$(2,8)$	504	$(2,19)$	3 420	$(2,25)$	7 800	A_8, $(4,2)$	20 160
$(2,11)$	660	$(2,16)$	4 080	?	7 920	$(3,4)$	20 160

Vemos que hay dos huecos correspondientes a grupos que no conocemos. En la sección siguiente veremos que el segundo de ellos corresponde al grupo de Mathieu M_{11}.

7.3 Los grupos de Mathieu

Tal y como hemos explicado en la introducción, los grupos de Mathieu son los primeros grupos simples esporádicos descubiertos. Son grupos de permutaciones que fueron descritos por Émile Mathieu en 1861 y 1873, si bien sus construcciones eran dudosas (no estaba claro que sus grupos no fueran meros grupos A_n) y fue en 1938 cuando Witt mostró dos construcciones alternativas completamente satisfactorias. Como hemos señalado más arriba, entre los grupos de Mathieu están los únicos ejemplos no triviales de grupos de permutaciones cuatro y cinco veces transitivos. Para construirlos conviene generalizar el concepto de sistema de Steiner que introdujimos en [G 7.41]:

Definición 7.18 Si $1 \leq l \leq m \leq n$, un *sistema de Steiner* generalizado de tipo $S_\lambda(l,m,n)$ es un par $(X,\mathcal{B})$, donde X es un conjunto de n elementos y $\mathcal{B}$ es una familia de subconjuntos de X de m elementos, llamados *bloques,* de modo que cada subconjunto de X con l elementos está contenido exactamente en λ bloques.

Los *sistemas de Steiner* de este tipo $S(l,m,n)$ definidos en [G 7.41] son los sistemas de Steiner en este sentido con $\lambda = 1$.

Así, en [G 7.42] demostramos que los sistemas de Steiner de tipo $S(2,n,n^2)$ son precisamente los planos afines finitos, mientras que en [G 8.81] vimos que los sistemas de Steiner de tipo $S(2,n+1,n^2+n+1)$ son los planos proyectivos finitos.

Recordemos también la noción de isomorfismo entre sistemas de Steiner (que vale igualmente para sistemas generalizados):

Un *isomorfismo* entre dos sistemas de Steiner generalizados $(X,\mathcal{B})$, $(X',\mathcal{B}')$ es una biyección $f : X \longrightarrow X'$ tal que, para todo $A \subset X$, se cumple que $A \in \mathcal{B}$ si y sólo si $f[A] \in \mathcal{B}'$.

La definición de sistema de Steiner no exige nada sobre el número de bloques, pero éste está determinado por sus parámetros. Más en general:

Teorema 7.19 *Si $(X, \mathcal{B})$ es un sistema de Steiner generalizado de tipo $S_\lambda(l, m, n)$, el número de bloques que contienen a un determinado conjunto $S \subset X$ con $|S| = s \leq l$ es*

$$b_s = \lambda \frac{\binom{n-s}{l-s}}{\binom{m-s}{l-s}}.$$

En particular, el número de bloques es

$$b = b_0 = \lambda \frac{\binom{n}{l}}{\binom{m}{l}}.$$

DEMOSTRACIÓN: Vamos a contar todos los pares (A, B) tales que $|A| = m$ y $S \subset A \subset B \in \mathcal{B}$.

Por una parte, hay $\binom{m-s}{l-s}$ conjuntos A y cada uno de ellos está contenido en λ bloques, luego en total hay $\lambda\binom{m-s}{l-s}$ pares.

Por otra parte, hay b_s bloques B que contienen a S, y cada uno de ellos contiene $\binom{n-s}{l-s}$ conjuntos A, luego el número de pares es $b_s\binom{m-s}{l-s}$. Al igualar los dos resultados obtenemos la fórmula del enunciado. ∎

Esencialmente, necesitamos construir dos sistemas de Steiner, que obtenemos con una misma técnica en los dos teoremas siguientes:

Teorema 7.20 *Existe un sistema de Steiner de tipo $S(5, 6, 12)$.*

DEMOSTRACIÓN: Sea k el cuerpo de 11 elementos, y consideremos la recta proyectiva Ω sobre k. Concretamente, podemos tomar $V = k^2$ y $\Omega = P(V)$ es el conjunto de los subespacios vectoriales de V de dimensión 1. Podemos llamar $\infty = \langle(1, 0)\rangle$ e identificar cada $\alpha \in k$ con el punto $\alpha = \langle(\alpha, 1)\rangle$. Así

$$\Omega = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \infty\}.$$

Consideremos el grupo de las homografías de Ω, es decir, el grupo lineal general proyectivo $\mathrm{LGP}(2, 11)$ y su subgrupo $G = \mathrm{LEP}(2, 11)$, el grupo lineal especial proyectivo, que tiene orden $|G| = 1\,320/2 = 660$.

Si una homografía fija a ∞, esto significa que

$$(0, 1)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (0, \alpha),$$

lo cual sucede si y sólo si $c = 0$.

Como podemos cambiar la matriz por $d^{-1}I$, podemos suponer que es de la forma

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

Así pues, las homografías que fijan a ∞ son las inducidas por automorfismos f con matrices de esta forma, que sobre los punto finitos actúan en la forma $f(x) = ax + b$. Ahora bien, para que la homografía esté en $\mathrm{LEP}(2, 11)$ es necesario que exista un $\alpha \in k$ tal que

$$\begin{pmatrix} \alpha a & \alpha b \\ 0 & \alpha \end{pmatrix}.$$

tenga determinante 1, es decir, tal que $\alpha^2 a = 1$, para lo cual es necesario y suficiente que $a = \alpha^{-2}$ sea un cuadrado en k.

En resumen, el estabilizador G_∞ está formado por las homografías que sobre los puntos finitos actúan en la forma $f(x) = ax + b$, donde a es un cuadrado no nulo en k.

Sea $\sigma \in \mathrm{LEP}(2, 11)$ la homografía inducida por el automorfismo de matriz

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Explícitamente:

x	0	1	2	3	4	5	6	7	8	9	10	∞
$\sigma(x)$	∞	0	6	8	9	3	10	4	5	7	2	1

En particular $\sigma(\infty) = 1$, $\sigma(1) = 0$, $\sigma(0) = \infty$ y σ^3 fija los tres puntos, luego $\sigma^3 = 1$.

Llamemos $X = \{\infty, 0, 1\}$ y sea $G_X = \{f \in G \mid f[X] = X\}$. Claramente es un subgrupo de G y hemos probado que $\sigma \in G_X$. Vamos a ver que $G_X = \langle\sigma\rangle$ tiene orden 3. Para ello tomamos $f \in G_X$ tal que $g(\infty) = \infty$ y veamos que, necesariamente, $g = 1$.

O bien $g(0) = 0$ y $g(1) = 1$ (en cuyo caso $g = 1$), o bien $g(0) = 1$ y $g(1) = 0$. Vamos a ver que este segundo caso no puede darse. Hemos visto que $g(x) = ax + b$, donde a es un cuadrado no nulo en k. La condición $g(0) = 1$ implica que $b = 1$, mientras que $g(1) = 0$ se traduce en que $a + 1 = 0$, luego $-1 = a$ es un cuadrado en k, digamos $-1 = \alpha^2$, en cuyo caso $\alpha \in k^*$ tiene orden 4, pero eso es imposible, pues $|k^*| = 10$.

Ahora supongamos que $f \in G_X$ cumple $f(\infty) = 1$. Entonces $f\sigma^{-1} \in G_X$ fija a ∞, luego hemos probado que $f\sigma^{-1} = 1$, luego $f = \sigma$. E igualmente, si $f(\infty) = 0$, concluimos que $f = \sigma^{-1}$, luego en cualquier caso $f \in \langle\sigma\rangle$.

Observemos ahora que G actúa sobre el conjunto de los subconjuntos de Ω con 3 elementos, y G_X es el estabilizador de X respecto de esta acción, luego la órbita de X tiene $660/3 = 220$ elementos. Ahora bien, hay $\binom{12}{3} = 220$ subconjuntos de Ω con 3 elementos, luego hemos probado que G es transitivo: puede transformar cualquier subconjunto de Ω con 3 elementos en cualquier otro.

Consideremos ahora el conjunto

$$B_0 = \{\infty, 1, 3, 4, 5, 9\} \subset X,$$

formado por ∞ y los cuadrados no nulos de k. Definimos $\mathcal{B} = \{g[B_0] \mid g \in G\}$, que es un conjunto de subconjuntos de X con 6 elementos cada uno. Más aún, ahora es claro que $(\Omega, \mathcal{B})$ es un sistema de Steiner generalizado de tipo $S_\lambda(3, 6, 12)$, para cierto λ.

En efecto, hemos probado que cualquier subconjunto $X \subset \Omega$ con 3 elementos estará en algún bloque. Pongamos que está concretamente en λ bloques. Si $Y \subset \Omega$ es otro conjunto con 3 elementos, sabemos que existe $f \in G$ tal que $f[X] = Y$, luego $B \mapsto f[B]$ biyecta los bloques que contienen a X con los bloques que contienen a Y, luego hay también λ bloques que contienen a Y. Concluimos que todo subconjunto de Ω con 3 elementos está exactamente en λ bloques. Vamos a calcular el valor λ.

La homografía dada por $\tau(x) = 3x$ está en G, porque 3 es un cuadrado en k, y por esto mismo cumple $\tau[B_0] = B_0$, como 3 tiene orden 5 en k^*, se cumple que τ tiene orden 5 en G, luego el estabilizador de B_0 respecto de la acción de G sobre los subconjuntos de Ω con 6 elementos contiene a τ y, por lo tanto, cumple $|G_{B_0}| = 5m$, para cierto m.

La órbita de B_0 es precisamente el conjunto de bloques $\mathcal{B}$, por lo que su cardinal es

$$b = |B| = \frac{660}{5m} = \frac{132}{m}.$$

Según el teorema 7.19,

$$b = \frac{132}{m} = \lambda \frac{\binom{12}{3}}{\binom{6}{3}} = \frac{220\lambda}{20},$$

luego $\lambda = 12/m$. La tabla siguiente muestra explícitamente 12 bloques que contienen a $\{0, 1, \infty\}$, con lo que $\lambda = 12$, $m = 1$ (las columnas segunda y tercera se obtienen de aplicar σ y σ^2 a la primera):

	1	σ	σ^2
$B_0 - 3$	$\infty, 0, 1, 2, 6, 9$	$\infty, 0, 1, 6, 7, 10$	$\infty, 0, 1, 2, 4, 10$
$B_0 - 4$	$\infty, 0, 1, 5, 8, 10$	$\infty, 0, 1, 2, 3, 5$	$\infty, 0, 1, 3, 6, 8$
$\sigma[B_0 - 3] + 1$	$\infty, 0, 1, 2, 7, 8$	$\infty, 0, 1, 4, 5, 6$	$\infty, 0, 1, 3, 9, 10$
$\sigma[B_0 - 1] + 3$	$\infty, 0, 1, 4, 8, 9$	$\infty, 0, 1, 5, 7, 9$	$\infty, 0, 1, 3, 4, 7$

En particular, ahora sabemos que el sistema $(\Omega, \mathcal{B})$ tiene 132 bloques. Seguidamente observamos que los 12 bloques que hemos obtenido en la tabla anterior constan de $\{\infty, 0, 1\}$ y las filas, las columnas y las transversales (un elemento de cada fila y cada columna) de la matriz

$$\begin{pmatrix} 2 & 3 & 5 \\ 6 & 7 & 10 \\ 9 & 4 & 8 \end{pmatrix}.$$

Es obvio entonces que estos 12 subconjuntos de $\{2,3,4,5,6,7,8,9,10\}$ forman un sistema de Steiner $\mathcal{B}'$ de tipo $S(2,3,9)$, y con esto ya podemos probar que el sistema $\mathcal{B}$ que hemos construido, no sólo es de tipo $S_{12}(3,6,12)$, sino que también es de tipo $S(5,6,12)$.

En efecto, si $A = \{a_1, a_2, a_3, a_4, a_5\} \subset \Omega$ tiene 5 elementos, podemos tomar $f \in G$ tal que $f[\{\infty, 0, 1\}] = \{a_1, a_2, a_3\}$. Así $f[A] = \{\infty, 0, 1, f(a_4), f(a_5)\}$, y sabemos que $\{f(a_4), f(a_5)\}$ está contenido en uno de los 12 bloques del sistema $\mathcal{B}'$, luego de hecho $f[A] \subset B$, donde B es uno de los 12 bloques que contienen a $\infty, 0, 1$, luego $A \subset f^{-1}[B] \in \mathcal{B}$.

Por otra parte, si $A \subset B_1 \cap B_2$, entonces $f[A] \subset f[B_1] \cap f[B_2]$, pero entonces $\{f(a_4), f(a_5)\}$ está contenido en los dos bloques de tres elementos que resultan de eliminar $\{\infty, 0, 1\}$ de $f[B_1]$ y $f[B_2]$, luego éstos tiene que ser el mismo, luego $f[B_1] = f[B_2]$, luego $B_1 = B_2$. ∎

Teorema 7.21 *Existe un sistema de Steiner de tipo $S(5,8,24)$.*

Demostración: Consideramos el cuerpo k de 23 elementos, el espacio vectorial $V = k^2$, la recta proyectiva $\Omega = P(V)$ sobre k y el grupo $G = \mathrm{LEP}(2, 23)$.

Cálculos análogos a los que hemos hecho en la prueba del teorema anterior nos dan que

$$|\mathrm{LG}(2,23)| = (23^2 - 1)(23^2 - 23) = 267\,168, \qquad |\mathrm{LE}(2,23)| = 12\,144,$$

con lo que $|G| = 6\,072$. Exactamente igual que antes concluimos que G_∞ está formado por las homografías de la forma $f(x) = ax + b$, donde a es un cuadrado no nulo en k. Tomamos de nuevo $\sigma \in \mathrm{LEP}(2,23)$ la homografía inducida por el automorfismo de matriz

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},$$

que en este caso es

x	0	1	2	3	4	5	6	7	8	9	10	11
$\sigma(x)$	∞	0	12	16	18	10	20	14	21	6	17	3
x	12	13	14	15	16	17	18	19	20	21	22	∞
$\sigma(x)$	22	8	19	4	11	5	15	7	9	13	2	1

y exactamente igual que en la prueba del teorema anterior concluimos que, si $X = \{\infty, 0, 1\}$, se cumple que $|G_X| = \langle\sigma\rangle$, donde usamos que $|k^*| = 22$, por lo que k^* no tiene elementos de orden 4, luego -1 no es un cuadrado en k. Esto implica que la órbita de X consta de $6\,072/3 = 2\,024 = \binom{24}{3}$, por lo que G actúa transitivamente sobre los subconjuntos de 3 elementos de Ω.

Ahora consideramos las homografías determinadas por las matrices

$$a = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} 3 & 1 \\ 1 & -3 \end{pmatrix},$$

cuyos determinantes son $2 = 5^2$ y $-10 = 17^2$, luego podemos pasar a automorfismos de determinante 1 que inducen la misma homografía sin más que

multiplicar las matrices por $5^{-1}I$ y $17^{-1}I$, así que son homografías de G. Una comprobación rutinaria muestra que

$$a^4 = b^2 = 1, \qquad a^b = a^{-1},$$

así como que las 8 matrices $a^i b^j$, con $0 \le i < 4$, $0 \le j < 2$ son distintas entre sí, por lo que $D = \langle a, b\rangle \cong D_8$. Tomamos como bloque B_0 la órbita de ∞ respecto de D, que resulta ser

$$B_0 = \{\infty, 0, 1, 3, 12, 15, 21, 22\}.$$

Llamamos $\mathcal{B} = \{g[B_0] \mid g \in G\}$, que, exactamente igual que en la prueba del teorema anterior, se razona que es un sistema de Steiner generalizado de tipo $S_\lambda(3, 8, 24)$. Como D está contenido en el estabilizador de B_0, tenemos que $|G_{B_0}| = 8m$, para cierto m. El número de bloques en B será de la forma

$$b = |B| = \frac{6\,072}{8m} = \frac{759}{m}.$$

El teorema 7.19 nos da que $\lambda = 21/m$. Ahora necesitamos encontrar 21 bloques distintos que contengan a $\infty, 0, 1$. Por brevedad omitimos en cada uno de ellos estos tres elementos comunes:

	1	σ	σ^2
B_0	3, 12, 15, 21, 22	2, 4, 13, 16, 22	2, 8, 11, 12, 18
$B_0 + 2$	2, 3, 5, 14, 17	5, 10, 12, 16, 19	7, 10, 11, 17, 22
$2B_0$	2, 6, 7, 19, 21	17, 12, 13, 14, 20	8, 9, 14, 19, 22
$2B_0 - 1$	5, 6, 18, 20, 22	2, 9, 10, 15, 20	4, 6, 9, 12, 17
$2B_0 - 6$	13, 15, 17, 18, 19	4, 5, 7, 8, 15	4, 10, 14, 18, 21
$8B_0 - 4$	3, 4, 11, 19, 20	3, 7, 9, 16, 18	6, 11, 14, 15, 16
$8B_0 - 7$	8, 16, 17, 20, 21	5, 9, 11, 13, 21	3, 6, 8, 10, 13

Esto prueba que $\lambda = 21$, $m = 1$ y $|\mathcal{B}| = 759$. Una comprobación rutinaria muestra que los 21 conjuntos de la tabla anterior forman un sistema de Steiner de tipo $S(2, 5, 21)$, es decir, que cada par de números entre 2 y 22 está exactamente en uno de los 21 conjuntos. Así, el mismo argumento empleado al final de la prueba del teorema anterior muestra que $\mathcal{B}$ es un sistema de Steiner de tipo $S(5, 8, 24)$. ∎

A partir de un sistema de Steiner es fácil construir como sigue otros más sencillos:

Definición 7.22 A partir de un sistema de Steiner generalizado $(X, \mathcal{B})$ de tipo $S_\lambda(l, m, n)$ con $l \ge 2$ y de un punto $p \in X$, podemos definir el *sistema derivado* $(X_p, \mathcal{B}_p)$ dado por $X_p = X \setminus \{p\}$ y cuyos bloques son los de la forma $B \setminus \{p\}$, donde $B \in \mathcal{B}$ y $p \in B$. Es inmediato que se trata de un sistema de Steiner de tipo $S_\lambda(l - 1, m - 1, n - 1)$.

Hay que tener presente que dos sistemas derivados de un mismo sistema respecto de puntos distintos no tienen por qué ser isomorfos, aunque es fácil ver que si el grupo de automorfismos del sistema es transitivo, entonces todos sus derivados son isomorfos.

Ahora tenemos garantizada la existencia de sistemas de Steiner de tipos

$$S(2,3,9), \quad S(3,4,10), \quad S(4,5,11), \quad S(5,6,12),$$
$$S(2,5,21), \quad S(3,6,22), \quad S(4,7,23), \quad S(5,8,24).$$

Vamos a demostrar que, salvo isomorfismo, sólo hay uno de cada tipo. Las definiciones siguientes presuponen que ya hemos probado dicha unicidad, pero las adelantamos para verlas todas conjuntamente en lugar de ir introduciéndolas gradualmente:

Para cada uno de los valores de n que figuran en la tabla siguiente, llamaremos W_n al único sistema de Steiner de tipo que se indica en ella:

n	W_n	$\lvert\mathrm{Aut}(W_n)\rvert$	$\lvert M_n\rvert$	transitividad
9	$S(2,3,9)$	$2^4\cdot 3^3$	$2^3\cdot 3^2$	2 estricta
10	$S(3,4,10)$	$2^5\cdot 3^2\cdot 5$	$2^4\cdot 3^2\cdot 5$	3 estricta
11	$S(4,5,11)$	$2^4\cdot 3^2\cdot 5\cdot 11$	$2^4\cdot 3^2\cdot 5\cdot 11$	4 estricta
12	$S(5,6,12)$	$2^6\cdot 3^3\cdot 5\cdot 11$	$2^6\cdot 3^3\cdot 5\cdot 11$	5 estricta
21	$S(2,5,21)$	$2^7\cdot 3^3\cdot 5\cdot 7$	$2^6\cdot 3^2\cdot 5\cdot 7$	2
22	$S(3,6,22)$	$2^8\cdot 3^2\cdot 5\cdot 7\cdot 11$	$2^7\cdot 3^2\cdot 5\cdot 7\cdot 11$	3
23	$S(4,7,23)$	$2^7\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 23$	$2^7\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 23$	4
24	$S(5,8,24)$	$2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23$	$2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23$	5

En particular, W_{n-1} es el sistema derivado de W_n, para todos los n de la tabla, salvo $n = 9, 21$. Los *grupos de Mathieu* $M_n \leq \mathrm{Aut}(W_n)$ se definen como sigue:

$$M_{12} = \mathrm{Aut}(W_{12}), \qquad M_{24} = \mathrm{Aut}(W_{24}),$$

mientras que M_9, M_{10}, M_{11} son, cada uno, el estabilizador de un punto en el siguiente, e igualmente con M_{21}, M_{22}, M_{23}.

Así, por ejemplo, M_{11} es el estabilizador de un punto en M_{12}, lo cual permite identificarlo con un subgrupo del grupo de los automorfismos del sistema derivado $W'_{12} = W_{11}$, que en este caso veremos que es el grupo de todos los automorfismos, aunque esto no es así en otros casos. Por ejemplo, vemos en la tabla que M_{10} tiene índice 2 en $\mathrm{Aut}(W_{10})$.

Tenemos que probar que los sistemas W_n (y, por consiguiente, los grupos M_n) están bien definidos (salvo isomorfismo), así como el resto de datos que se incluyen en la tabla, en particular que cada grupo M_n es un grupo de permutaciones multiplemente transitivo sobre W_n, con la multiplicidad k que se indica.

Los cuatro primeros grupos de Mathieu se conocen como los *grupos de Mathieu pequeños,* mientras que los cuatro últimos son los *grupos grandes.* No obstante, cabe señalar que, en muchos contextos, sólo se llama grupos de Mathieu a los grupos M_n correspondientes a los cinco índices marcados en negrita en la tabla.

Nos ocupamos en primer lugar de los grupos de Mathieu pequeños, y el punto de partida es que en [G 7.44] demostramos que existe, salvo isomorfismo, un único sistema de Steiner W_9 de tipo $S(2,3,9)$, que no es sino el plano afín sobre el cuerpo de 3 elementos. Vamos a estudiarlo con algo de detalle.

El plano afín de orden 3 El plano afín P de orden 3 consta de 12 rectas agrupadas en 4 clases $\Pi_1, \Pi_2, \Pi_3\Pi_4$ de 3 rectas paralelas cada una. Numerando sus puntos adecuadamente y disponiéndolos así:

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array}$$

las cuatro clases de rectas paralelas son:

$$\begin{array}{ll} \text{Las “horizontales”} & \Pi_1 = \{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}, \\ \text{Las “verticales”} & \Pi_2 = \{\{1,4,7\},\{2,5,8\},\{3,6,9\}\}, \\ \text{Las “diagonales } \searrow\text{”} & \Pi_3 = \{\{1,5,9\},\{2,6,7\},\{3,4,8\}\}, \\ \text{Las “diagonales } \swarrow\text{”} & \Pi_4 = \{\{3,5,7\},\{2,4,9\},\{1,6,8\}\}. \end{array}$$

El grupo de automorfismos de un plano afín, considerado como sistema de Steiner, no es más que el grupo de todas las colineaciones (es decir, las biyecciones que transforman rectas en rectas) y, por el teorema fundamental de la geometría afín [G 5.17] (teniendo en cuenta que el cuerpo de 3 elementos no tiene más automorfismo que la identidad, por lo que las aplicaciones semilineales coinciden con las afinidades)), éste no es sino el grupo de las biyecciones afines.

Llamaremos $\mathrm{Af}(2,3)$ al grupo de las biyecciones afines de P (es decir, del espacio afín de dimensión 2 sobre el cuerpo de 3 elementos).

Cada biyección afín está determinada por la imagen de un sistema de referencia afín (que en dimensión 2 se reduce a un sistema de tres puntos no colineales), luego hay tantas biyecciones afines como sistemas de referencia afines, y así:

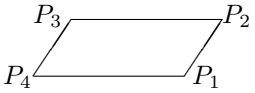
$$|\mathrm{Aut}(W_9)| = |\mathrm{Af}(2,3)| = 432 = 2^4 \cdot 3^3,$$

pues para formar un sistema de referencia afín podemos elegir un punto cualquiera de los 9 del espacio, luego otro punto cualquiera de entre los 8 restantes, y luego otro cualquiera de entre los 6 puntos que no están en la recta formada por los dos anteriores, lo que nos da $9 \cdot 8 \cdot 6 = 432$ posibilidades.

Llamaremos *triángulos* en P a los conjuntos de 3 puntos no alineados y *cuadriláteros* a los conjuntos de 4 puntos que no contienen rectas. Veamos algunos resultados sobre cuadriláteros:

Teorema 7.23 *Sea P el espacio afín de orden 3.*

1. *P contiene exactamente 54 cuadriláteros.*
2. *Dados dos cuadriláteros Q_1 y Q_2, existe una biyección afín $f \in \mathrm{Af}(2,3)$ tal que $f[Q_1] = Q_2$.*
3. *Todos los cuadriláteros son paralelogramos, es decir, que son de la forma $Q = \{P_1, P_2, P_3, P_4\}$, de modo que $P_1P_2 \parallel P_3P_4$ y $P_1P_4 \parallel P_2P_3$.*



4. *Más precisamente: de las seis rectas que unen los cuatro puntos de un cuadrilátero cuatro forman dos pares de rectas paralelas (sus lados), que se cortan en los puntos del cuadrilátero, y las otras dos (sus diagonales) se cortan en un punto exterior al que llamaremos punto diagonal.*

5. *El complementario de un cuadrilátero es una unión de dos rectas que se cortan en su punto diagonal, o, equivalentemente, consta del punto diagonal y de otro cuadrilátero con el mismo punto diagonal.*

6. *Los conjuntos de la forma $Q \cup \{D\}$, donde Q es un cuadrilátero y D su punto diagonal, coinciden con las uniones de dos rectas secantes.*

7. *Todo conjunto de cinco puntos contiene al menos un cuadrilátero.*

8. *Si un conjunto de cinco puntos A contiene un único cuadrilátero Q, entonces $A = Q \cup \{D\}$, donde D es el punto diagonal de Q.*

Demostración: 1) P posee $\binom{9}{4} = 126$ subconjuntos de 4 puntos, de los cuales no serán cuadriláteros los formados por una recta y uno de los 6 puntos no contenidos en ella. Como hay 12 rectas, hay $12 \cdot 6 = 72$ conjuntos así, luego nos quedan $126 - 72 = 54$ cuadriláteros.

2) Si $Q = \{P_1, P_2, P_3, P_4\}$ es un cuadrilátero en las condiciones de 2), los puntos P_1, P_2, P_3 son afínmente independientes, pues las rectas P_1P_2 y P_2P_3 son secantes. Lo mismo podemos decir de otro cuadrilátero $Q' = \{P'_1, P'_2, P'_3, P'_4\}$, y, según se razona tras la definición [G 3.16], existe una única afinidad $f : P \longrightarrow P$ que cumple $f(P_i) = P'_i$, para $i = 1, 2, 3$, que será de hecho una biyección afín, pues su inversa es la afinidad que cumple $g(P'_i) = P_i$. Ahora bien, P_4 es la intersección de la paralela a P_1P_2 por P_3 con la paralela a P_2P_3 por P_1, y P'_4 cumple la propiedad análoga. Como las biyecciones afines conservan el paralelismo, también se cumple $f(P_4) = P'_4$. Por lo tanto, $f[Q] = Q'$.

Teniendo esto en cuenta, para probar que todo cuadrilátero cumple una propiedad que se conserva por biyecciones afines basta probarlo para un cuadrilátero en particular, por ejemplo, $Q = \{1, 3, 7, 9\}$, para el cual 3), 4) y 5) resultan inmediatos, así como la mitad de 6). Para probar el recíproco de 6) observamos que una biyección afín nos permite transformar dos rectas secantes en otras dos cualesquiera (tomando como sistemas de referencia afines el punto de intersección y un punto de cada recta), por lo que basta probarlo para un par de rectas en concreto y entonces es trivial.

7) Si $A = \{P_1, P_2, P_3, P_4, P_5\}$ y los cuatro primeros puntos no son un cuadrilátero, es que contienen una recta. No perdemos generalidad si suponemos que $L_1 = \{P_1, P_2, P_3\}$ forman una recta. Si $\{P_2, P_3, P_4, P_5\}$ tampoco son un cuadrilátero, contienen una recta. Ésta no puede contener a P_2 y P_3, pero tiene que contener a uno de los dos. Podemos suponer que es P_3, con lo que $L_2 = \{P_3, P_4, P_5\}$ es una recta. Pero entonces, $Q = \{P_1, P_2, P_4, P_5\}$ tiene que ser un cuadrilátero.

8) De nuevo no perdemos generalidad si suponemos que, concretamente, $Q = \{1, 3, 7, 9\}$, con lo que $D = 5$. Es claro que $Q \cup \{D\}$ no contiene más cuadriláteros, pues si eliminamos un punto que no sea D, el conjunto resultante contiene a una de las diagonales $\{1, 5, 9\}$ o $\{3, 5, 7\}$, luego no es un cuadrilátero. En cambio, si añadimos a Q cualquiera de los otros cuatro puntos posibles, por ejemplo, el 2, entonces $\{1, 2, 3, 7, 9\}$ contiene el cuadrilátero $Q' = \{1, 2, 7, 9\}$, y es fácil ver que lo mismo vale en los otros tres casos. ∎

Definición 7.24 Si Π y Π' son dos clases distintas de rectas paralelas de P, diremos que un cuadrilátero es *de tipo* $\{\Pi, \Pi'\}$ si sus pares de lados paralelas están uno en Π y otro en Π'.

Es claro que las biyecciones afines transforman todos los cuadriláteros de un mismo tipo en todos los de otro mismo tipo, por lo que tiene que haber el mismo número de cuadriláteros de cada tipo. Por lo tanto, tiene que haber, concretamente, 9 cuadriláteros de cada tipo.

En realidad nos conviene hilar un poco menos fino, y por ello definimos las tres clases siguientes de cuadriláteros:

- Llamamos $\mathcal{Q}_1$ a la clase de los cuadriláteros de tipo $\{\Pi_1, \Pi_2\}$ o $\{\Pi_3, \Pi_4\}$.
- Llamamos $\mathcal{Q}_2$ a la clase de los cuadriláteros de tipo $\{\Pi_1, \Pi_3\}$ o $\{\Pi_2, \Pi_4\}$.
- Llamamos $\mathcal{Q}_3$ a la clase de los cuadriláteros de tipo $\{\Pi_1, \Pi_4\}$ o $\{\Pi_2, \Pi_3\}$.

Tenemos así tres clases disjuntas de 18 cuadriláteros cada una.

Si $f \in \mathrm{Af}(2, 3)$, tenemos que f transforma todos los cuadriláteros de una clase en todos los de otra, por lo que podemos definir una acción del grupo $\mathrm{Af}(2, 3)$ en el conjunto $\Omega = \{\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3\}$ de las tres clases de cuadriláteros. Como cualquier cuadrilátero se puede transformar en cualquier otro, la acción es transitiva. Más aún, vamos a ver que es triplemente transitiva o, más sencillamente, que el homomorfismo $f : \mathrm{Af}(2, 3) \longrightarrow \Sigma_3$ inducido por esta acción es un epimorfismo, es decir, que existen biyecciones afines que permutan las tres clases de cualquiera de las seis formas posibles.

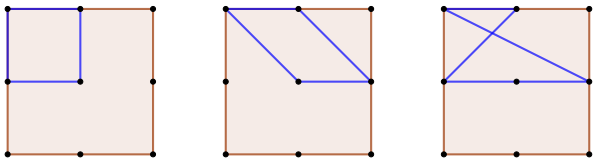
En realidad vamos a demostrar algo aún más fino:

Teorema 7.25 *Sea $G = \mathrm{Af}(2, 3)$, sean, $p, q \in P$ dos puntos distintos y sea $H = G_{p,q}$ el estabilizador de ambos puntos respecto de la acción de G en P. Entonces, el homomorfismo $H \longrightarrow \Sigma_\Omega$ inducido por la acción de G sobre Σ_Ω es un isomorfismo.*

Demostración: Como hay biyecciones afines que transforman cualquier terna de puntos no colineales en cualquier otra, en particular la acción de $G = \mathrm{Af}(2, 3)$ sobre P es doblemente transitiva, luego $|G_p| = 432/9 = 48$ y G_p actúa transitivamente sobre $P \setminus \{p\}$, luego a su vez $|H| = 48/8 = 6$.

Precisamente porque la acción de G es doblemente transitiva no perdemos generalidad si suponemos que los puntos son $p = 1$, $q = 2$. Así toda $f \in H$ cumple $f(1) = 1$, $f(2) = 2$ y está determinada por $f(4)$, que puede ser cualquiera de los seis puntos distintos de $\{1, 2, 3\}$.

Consideremos por ejemplo la biyección $f \in H$ dada por $f(4) = 5$ y consideremos los cuadriláteros $Q = \{1, 2, 5, 4\}$ y $Q' = \{1, 2, 6, 5\}$.



Es fácil ver que $f(5) = 6$ (pues 5 es la intersección de la paralela a 12 por 4 con la paralela a 14 por 2, por lo que $f(5)$ tiene que ser la intersección de la paralela a 12 por $f(4) = 5$ con la paralela a 15 por 2), luego $f[Q] = \{1, 2, 6, 5\} = Q'$ y similarmente vemos que $f(6) = 4$, luego $f[Q'] = \{1, 2, 4, 6\}$.

Pero Q es de tipo $\{\Pi_1, \Pi_2\}$, luego está en Ω_1 y Q' es de tipo $\{\Pi_1, \Pi_3\}$, luego está en Ω_2 y $f[Q']$ es de tipo $\{\Pi_1, \Pi_4\}$, luego está en Ω_3. Esto significa que f induce un ciclo de longitud 3 en Σ_Ω.

Dejamos al lector la comprobación de que si tomamos $f(4) = 7$ entonces $f[Q] = \{1, 2, 8, 7\} \in \Omega_1$, mientras que $f[Q'] = \{1, 2, 9, 8\} \in \Omega_3$, luego ahora f induce la trasposición que intercambia Ω_2 y Ω_3. Esto prueba que la imagen de H es todo Σ_Ω. ∎

En particular, $\mathrm{Af}(2, 3)$ es triplemente transitivo sobre Ω, por lo que el estabilizador H de una de las tres clases cumple $|H| = 432/3 = 144$ y actúa transitivamente sobre las otras dos, luego el estabilizador de dos clases (y, por lo tanto, de las tres) es un subgrupo $M_9 \leq \mathrm{Af}(2, 3)$ de orden $|M_9| = 72$ (pero todavía no hemos probado que sea el grupo de Mathieu definido en 7.22).

El grupo M_9 es doblemente transitivo, pues si $p, q, p', q' \in P$, con $p \neq q$, $p' \neq q'$, podemos tomar un $f \in \mathrm{Af}(2, 3)$ tal que $f(p) = p'$ y $f(q) = q'$ y, por el teorema anterior, podemos componer f con un automorfismo de P que fije a p' y q' y que haga corresponder las clases $f[\Omega_i] \mapsto \Omega_i$, luego, cambiando f por la composición, tenemos que $f \in M_9$ y cumple $f(p) = p'$ y $f(q) = q'$. El teorema 7.3 nos da que M_9 es estrictamente doblemente transitivo sobre P.

El interés de las tres clases de cuadriláteros que hemos definido estriba en el teorema siguiente:

Teorema 7.26 *Para cada $i = 1, 2, 3$, cada triángulo de P está contenido en un único cuadrilátero de la clase Ω_i, y las tres clases $\Omega_1, \Omega_2, \Omega_3$ son las únicas clases de cuadriláteros con esta propiedad.*

Demostración: Como las clases se transforman una en otra por las biyecciones afines, no perdemos generalidad si consideramos únicamente Ω_1.

Si $T = \{P_1, P_2, P_3\}$ es un triángulo, sus lados están en tres clases de paralelas distintas. Supongamos por ejemplo que la cuarta es Π_4. Si añadimos un punto P_4 para formar un cuadrilátero, reordenando P_1, P_2, P_3 si es necesario, podemos exigir que $P_1P_2 \parallel P_3P_4$ y $P_1P_4 \parallel P_2P_3$, y sabemos que P_1P_2 y P_2P_3 no están en la clase Π_4, luego ninguna de las cuatro rectas lo está, luego T no está contenido en ninguno de los 9 paralelogramos de la clase $\mathcal{Q}_1$ con lados en Π_3 y Π_4.

Estamos suponiendo que los lados de T están en las clases Π_1, Π_2, Π_3. Renumerando sus vértices podemos suponer que $P_1P_2 \in \Pi_1$ y $P_2P_3 \in \Pi_2$. La paralela a P_1P_2 por P_3 y la paralela a P_2P_3 por P_1 se cortarán en un punto P_4 que formará un paralelogramo $\{P_1, P_2, P_3, P_4\} \in \mathcal{Q}_1$, claramente el único posible. Así pues, las clases $\mathcal{Q}_i$ tienen la propiedad requerida.

Supongamos ahora que $\mathcal{Q}$ es una clase de cuadriláteros de P con la propiedad de que cada triángulo está contenido exactamente en uno de sus miembros. Ya hemos visto que hay $9 \cdot 8 \cdot 6 = 432$ ternas ordenadas (P_1, P_2, P_3) de puntos no alineados (sistemas de referencia afines), y cada triángulo $\{P_1, P_2, P_3\}$ se obtiene desordenando 6 de dichas ternas, luego hay $432/6 = 72$ triángulos. Como cada cuadrilátero contiene 4, la clase $\mathcal{Q}$ tiene que contener al menos $72/4 = 18$ cuadriláteros.

Llamemos $\mathcal{Q}(i, j)$ al conjunto de todos los cuadriláteros que contienen al par $\{i, j\}$. En el caso concreto de $\mathcal{Q}(1, 2)$, si nombramos a sus elementos por los dos vértices adicionales, son los 9 siguientes:

$$Q_{45}, \quad Q_{46}, \quad Q_{56}, \quad Q_{78}, \quad Q_{79}, \quad Q_{89}, \quad Q_{57}, \quad Q_{48}, \quad Q_{69}.$$

La clase $\mathcal{Q}$ tiene que contener un cuadrilátero que contenga al triángulo $\{1, 2, 4\}$, y sólo hay tres posibilidades: $Q_{45} \in \mathcal{Q}$, o bien $Q_{46} \in \mathcal{Q}$ o bien $Q_{48} \in \mathcal{Q}$.

Ahora bien, si $Q_{45} \in \mathcal{Q}$, entonces $\mathcal{Q}$ ya no puede contener ningún otro cuadrilátero que contenga a $\{1, 2, 4\}$ ni a $\{1, 2, 5\}$, luego los posibles miembros restantes de $\mathcal{Q} \cap \mathcal{Q}(1, 2)$ son

$$Q_{78}, \quad Q_{79}, \quad Q_{89}, \quad Q_{69}.$$

Pero $\mathcal{Q}$ tiene que contener un cuadrilátero que contenga a $\{1, 2, 6\}$, y la única posibilidad es Q_{69}, pero entonces en $\mathcal{Q}$ no puede haber ningún otro cuadrilátero que contenga a $\{1, 2, 9\}$, lo que nos deja únicamente a Q_{78} como posible miembro adicional de $\mathcal{Q} \cap \mathcal{Q}(1, 2)$, y necesariamente debe contenerlo, pues tiene que haber un cuadrilátero que contenga a $\{1, 2, 7\}$. Así pues, en este caso

$$\mathcal{Q} \cap \mathcal{Q}(1, 2) = \{Q_{45}, Q_{69}, Q_{78}\} \subset \mathcal{Q}_1.$$

Igualmente se razona que si $Q_{46} \in \mathcal{Q}$, entonces

$$\mathcal{Q} \cap \mathcal{Q}(1, 2) = \{Q_{46}, Q_{57}, Q_{89}\} \subset \mathcal{Q}_3,$$

mientras que si $Q_{48} \in \mathcal{Q}$, entonces

$$\mathcal{Q} \cap \mathcal{Q}(1, 2) = \{Q_{48}, Q_{79}, Q_{56}\} \subset \mathcal{Q}_2.$$

Así pues, en cualquier caso $\mathcal{Q} \cap \mathcal{Q}(1,2) \subset \mathcal{Q}_k$, para cierto índice $k = 1, 2, 3$. Más en general, si $i, j \in P$ son puntos distintos, $\mathcal{Q} \cap \mathcal{Q}(i,j) \subset \mathcal{Q}_k$, para cierto k.

En efecto, tomamos $f \in \mathrm{Af}(2,3)$ tal que $f(1) = i$, $f(2) = j$ y entonces, si $Q \in \mathcal{Q} \cap \mathcal{Q}(i,j)$, tenemos que $f^{-1}[Q] \in f^{-1}[\mathcal{Q}] \cap \mathcal{Q}(1,2)$, pero $f^{-1}[\mathcal{Q}]$ cumple también la propiedad del enunciado, luego aplicándole lo que hemos probado $f^{-1}[Q] \in \mathcal{Q}_k$, para cierto k, luego $Q \in f[\mathcal{Q}_k] = \mathcal{Q}_{k'}$, para cierto k'.

Ahora vamos a probar que k no depende de i, j, es decir, que todas las intersecciones $\mathcal{Q} \cap \mathcal{Q}(i,j)$ están contenidas en una misma clase $\mathcal{Q}_k$.

En caso contrario, existirían pares $\{i,j\}$, $\{i',j'\}$ tales que $\mathcal{Q} \cap \mathcal{Q}(i,j) \subset \mathcal{Q}_k$, $\mathcal{Q} \cap \mathcal{Q}(i',j') \subset \mathcal{Q}_{k'}$, con $k \neq k'$.

Distinguiendo casos, es fácil ver que siempre existen dos triángulos T y T' tales que $\{i,j\} \subset T$, $\{i',j'\} \subset T'$ y $|T \cap T'| = 2$. Tienen que existir cuadriláteros $T \subset Q \in \mathcal{Q}$, $T' \subset Q' \in \mathcal{Q}$, pero entonces $Q, Q' \in \mathcal{Q} \cap \mathcal{Q}(T \cap T') \subset \mathcal{Q}_{k''}$, para cierto k'', pero las tres clases $\mathcal{Q}_k$ son disjuntas, luego tiene que ser $k = k'' = k'$.

Esto prueba que $\mathcal{Q} \subset \mathcal{A}_k$, para cierto k, y como $18 \leq |\mathcal{Q}| \leq |\mathcal{A}_k| = 18$, tiene que darse la igualdad $\mathcal{Q} = \mathcal{Q}_k$. ∎

En lo sucesivo, cuando hablemos de "las clases de cuadriláteros" de un plano afín P (de orden 3), nos referiremos a las tres clases que hemos definido en 7.24 y que acabamos de caracterizar.

Supongamos que $(X, \mathcal{B})$ es un sistema de Steiner de tipo $S(3,4,10)$. Por el teorema 7.19 debe constar de 30 bloques. Si llamamos $\infty \in X$ a uno de sus puntos, el derivado $P = X_\infty$ debe ser un sistema de Steiner de tipo $S(2,3,9)$, es decir, el plano afín P que hemos estudiado.

Por definición de sistema derivado, los bloques de $(X, \mathcal{B})$ que contienen el punto ∞ tienen que ser los 12 de la forma $L \cup \{\infty\}$, donde L recorre las 12 rectas de P. En cambio, los 18 bloques restantes tienen que ser subconjuntos de P con cuatro puntos cada uno. Más concretamente, tienen que ser cuadriláteros, pues cada recta L es un conjunto de 3 puntos que ya está contenido en el bloque $L \cup \{\infty\} \in \mathcal{B}$, luego L no puede estar contenido en ninguno de los 18 bloques que nos faltan.

Así, los 18 bloques que no contienen a ∞ tienen que ser 18 cuadriláteros con la propiedad de que cada triángulo tiene que estar contenido en uno solo de ellos (ya que no puede estar en ninguno de los 12 bloques de la forma $L \cup \{\infty\}$). Por el teorema anterior, esos 18 bloques tienen que ser los cuadriláteros de una de las tres clases $\mathcal{Q}_i$. Así pues:

Teorema 7.27 *Si $(X, \mathcal{B})$ es un sistema de Steiner de tipo $S(3,4,10)$ y $\infty \in X$, entonces el sistema derivado $P = X_\infty$ es un plano afín de orden 3 y sus 30 bloques son:*

1. *Los 12 conjuntos de la forma $L \cup \{\infty\}$, donde L es una recta en P.*
2. *Los 18 cuadriláteros de una de las clases $\mathcal{Q}_i$ definidas en 7.24.*

En particular, todos los sistemas de Steiner de tipo $S(3,4,10)$ son isomorfos.

DEMOSTRACIÓN: Sólo falta probar la última afirmación y, de hecho, vamos a probar algo más fuerte. Supongamos que $(X, \mathcal{B})$ y $(X', \mathcal{B}')$ son dos sistemas de Steiner de tipo $S(3, 4, 10)$ y fijemos tres puntos distintos $p, q, \infty \in X$ y otros tres puntos distintos p', q', ∞'. Entonces $P = X_\infty$ y $P' = X'_{\infty'}$ son dos planos afines de orden 3, luego existe una biyección afín $f : P \longrightarrow P'$ entre ellos. Más aún, podemos tomarla de modo que $f(p) = p'$ y $f(q) = q'$.

Dicha biyección transformará la clase de cuadriláteros $\mathcal{Q}_i$ contenida en $\mathcal{B}$ en una de las tres clases de cuadriláteros de $X'_{\infty'}$, no necesariamente la clase $\mathcal{Q}'_i \subset \mathcal{B}'$, pero, según el teorema 7.25, podemos componer f con un automorfismo de P' que fije a p', q' y que transforme $f[\mathcal{Q}_i]$ en $\mathcal{Q}'_i$ y, por lo tanto, podemos suponer que $f[\mathcal{Q}_i] = \mathcal{Q}'_i$. Si extendemos f a una biyección $\bar{f} : X \longrightarrow X'$ haciendo $\bar{f}(\infty) = \infty'$, tenemos que $\bar{f}$ es trivialmente un automorfismo, pues también transforma los 12 bloques de la forma $L \cup \{\infty\} \in \mathcal{B}$ en bloques $f[L] \cup \{\infty'\} \in \mathcal{B}'$, y además cumple que $\bar{f}(p) = p'$, $\bar{f}(q) = q'$, $\bar{f}(\infty) = \infty'$. ∎

A partir de aquí ya está justificada la notación W_{10} para nombrar cualquier sistema de Steiner de tipo $S(3, 4, 10)$. Es irrelevante cuál consideremos, pues todos ellos son isomorfos.

En la prueba del teorema anterior hemos demostrado que si tenemos dos sistemas de Steiner de tipo $S(3, 4, 10)$ y elegimos arbitrariamente tres puntos en cada uno de ellos, existe un isomorfismo entre ambos que hace corresponder los puntos seleccionados. En particular, si aplicamos esto a un mismo sistema de Steiner W_{10}, tenemos que el grupo $G = \mathrm{Aut}(W_{10})$ es triplemente transitivo sobre W_{10}.

Más aún, fijado $\infty \in W_{10}$, el estabilizador G_∞ está formado claramente por los automorfismos que, restringidos al plano afín $W_9 = (W_{10})_\infty$, fijan la clase $\mathcal{Q}_i$ contenida en $\mathcal{B}$. En otras palabras, el estabilizador de G_∞ es isomorfo al estabilizador de $\mathcal{Q}_i$ en el grupo $\mathrm{Af}(2, 3)$ respecto de su acción sobre el conjunto $\Omega = \{\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3\}$.

Esto nos permite hacer algunas cuentas. Como $\mathrm{Af}(2, 3)$ actúa transitivamente sobre Ω, sus estabilizadores tienen orden $432/3 = 144$, luego $|G_\infty| = 144$ y, como G también actúa transitivamente sobre W_{10}, concluimos que

$$|\mathrm{Aut}(W_{10})| = 1\,440.$$

Consideremos ahora un sistema de Steiner $(X, \mathcal{B})$ de tipo $S(4, 5, 11)$ y fijemos dos puntos $\infty_1, \infty_2 \in X$. El teorema 7.19 nos da que $\mathcal{B}$ consta de 66 bloques. El derivado $P = X_{\infty_1\infty_2}$ es un sistema de Steiner de tipo $S(2, 3, 9)$, luego sus bloques son las rectas de una estructura de plano afín. Así, los bloques de $\mathcal{B}$ que contienen a ∞_1, ∞_2 son necesariamente los 12 bloques de la forma $L \cup \{\infty_1, \infty_2\}$, donde L es una recta de P.

A su vez, el derivado X_{∞_2} es un sistema de tipo $S(3, 4, 10)$, luego su estructura es la que indica el teorema 7.27: sus bloques con el punto ∞_1 son de la forma $L \cup \{\infty_1\}$, donde L es una recta en P, mientras que sus bloques sin ∞_1 son los 18 cuadriláteros de una de las tres clases $\mathcal{Q}_i$. Vamos a llamarla $\mathcal{Q}_2$, de modo que los bloques de $\mathcal{B}$ que contienen a ∞_2, pero no a ∞_1, son los 18 de la forma $Q \cup \{\infty_2\}$, con $Q \in \mathcal{Q}_2$.

Similarmente, el derivado X_{∞_1} es un sistema de tipo $S(3,4,10)$ y consta de los bloques $L \cup \{\infty_2\}$ y de otros 18 bloques formados por cuadriláteros de otra de las clases dadas por el teorema 7.26, a la que llamaremos $\mathcal{Q}_1$, de modo que los bloques de $\mathcal{B}$ que contienen a ∞_1 pero no a ∞_2 son los 18 de la forma $Q \cup \{\infty_1\}$, con $Q \in \mathcal{Q}_1$. Notemos que tiene que ser $\mathcal{Q}_1 \neq \mathcal{Q}_2$, pues un mismo cuadrilátero no puede estar contenido a la vez en un bloque $Q \cup \{\infty_1\}$ y en otro $Q \cup \{\infty_2\}$.

Falta describir los bloques de $B \in \mathcal{B}$ que no contienen ni a ∞_1 ni a ∞_2, con lo que están formados por 5 puntos de P. Tienen que ser $66-12-18-18 = 18$ en total. Por el teorema 7.23, existe un cuadrilátero $Q \subset B$, que no puede ser de las clases $\mathcal{Q}_1$ o $\mathcal{Q}_2$, pues entonces estaría contenido también en un bloque de tipo $Q \cup \{\infty_i\}$. Por lo tanto, tiene que ser de tipo $\mathcal{Q}_3$. Como cada uno de los 18 bloques de este tipo tiene que contener un cuadrilátero distinto de $\mathcal{Q}_3$ y hay sólo 18 cuadriláteros, cada bloque contiene un único cuadrilátero, luego la propiedad 8) del teorema 7.23 nos dice que tiene que ser $B = Q \cup \{D\}$, donde D es el punto diagonal de Q. Así pues:

Teorema 7.28 *Si $(X, \mathcal{B})$ es un sistema de Steiner de tipo $S(4,5,11)$ y fijamos dos puntos $\infty_1, \infty_2 \in X$, el sistema derivado $P = X_{\infty_1,\infty_2}$ es un plano afín de orden 3 y sus 66 bloques son:*

1. *Los 12 conjuntos de la forma $L \cup \{\infty_1, \infty_2\}$, donde L es una recta en P.*
2. *Los 36 conjuntos de la forma $Q \cup \{\infty_i\}$, con $Q \in \mathcal{Q}_i$, para $i = 1, 2$.*
3. *Los 18 conjuntos de la forma $Q \cup \{D\}$, donde $Q \in \mathcal{Q}_3$ y D es el punto diagonal de Q.*

En particular, todos los sistemas de Steiner de tipo $S(4,5,11)$ son isomorfos.

Demostración: Sólo falta probar la unicidad. Más en general, consideramos dos sistemas de Steiner $(X, \mathcal{B})$ y $(X', \mathcal{B}')$ y fijamos puntos distintos $p, q, \infty_1, \infty_2 \in X$ y otros puntos, también distintos $p', q', \infty_1', \infty_2' \in X'$. Entonces $P = X_{\infty_1\infty_2}$, $P' = X'_{\infty_1\infty_2}$ son planos afines y podemos fijar una biyección afín $f : P \longrightarrow P'$ tal que $f(p) = p'$ y $f(q) = q'$. Sean $\mathcal{Q}_1$, $\mathcal{Q}_2$ y $\mathcal{Q}_3$ las clases de cuadriláteros en P que se corresponden con los bloques de $\mathcal{B}$ según el enunciado, y sean $\mathcal{Q}_1'$, $\mathcal{Q}_2'$ y $\mathcal{Q}_3'$ las correspondientes de P'. El teorema 7.25 nos permite componer f con un automorfismo de P' que fije a p', q' y que haga corresponder las clases $f[\mathcal{Q}_i] \mapsto \mathcal{Q}_i'$. Así podemos suponer que $f[\mathcal{Q}_i] = \mathcal{Q}_i'$, para $i = 1, 2, 3$, de donde se sigue que, si extendemos f a una biyección $\bar{f} : X \longrightarrow X'$ mediante $\bar{f}(\infty_i) = \infty_i'$ (para $i = 1, 2$), se cumple que $\bar{f}$ es un isomorfismo que además cumple $\bar{f}(p) = p'$, $\bar{f}(q) = q'$, $\bar{f}(\infty_1) = \infty_1'$, $\bar{f}(\infty_2) = \infty_2'$. ∎

A partir de aquí ya podemos llamar W_{11} a cualquier sistema de Steiner de tipo $S(4,5,11)$. La prueba de la unicidad del teorema anterior muestra que $M_{11} = \mathrm{Aut}(W_{11})$ es cuatro veces transitivo[1] sobre W_{11}.

[1] Todavía no hemos demostrado que este M_{11} es el que hemos definido en 7.22, es decir, el estabilizador de un punto en M_{12}.

Si fijamos dos puntos $\infty_1, \infty_2 \in W_{11}$, y consideramos el doble derivado $P = (W_{11})_{\infty_1\infty_2}$, es claro que los automorfismos que fijan los dos puntos infinitos se restringen a biyecciones afines de $\mathrm{Af}(2,3)$ que fijan las tres clases de cuadriláteros, es decir, elementos del subgrupo M_9 y, recíprocamente, cada $f \in M_9$ se extiende a un único automorfismo $\bar{f} \in (M_{11})_{\infty_1\infty_2}$.

Así pues, $|(M_{11})_{\infty_1\infty_2}| = |M_9| = 72$ y, por otra parte, como M_{11} es cuatro veces transitivo sobre W_{11}, tenemos que $|(M_{11})_{\infty_2}| = |M_{11}|/11$ y este estabilizador es tres veces transitivo sobre $W_{10} = (W_{11})_{\infty_1}$, luego resulta que $|(M_{11})_{\infty_1,\infty_2}| = |M_{11}|/(11 \cdot 10)$, y así

$$|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7\,920.$$

En particular, M_{11} es estrictamente cuatro veces transitivo sobre W_{11}.

A su vez, el estabilizador $(M_{11})_{\infty_2}$, a través de la restricción, es isomorfo a un subgrupo $M_{10} \trianglelefteq \mathrm{Aut}(W_{10})$ de modo que $|M_{10}| = 10 \cdot 9 \cdot 8 = 720$, y que es estrictamente triplemente transitivo.

Teorema 7.29 *Si $(X, \mathcal{B})$ es un sistema de Steiner de tipo $S(5,6,12)$ y fijamos tres puntos $\infty_1, \infty_2, \infty_3 \in X$, el sistema derivado $P = X_{\infty_1\infty_2\infty_3}$ es un plano afín de orden 3 y sus 132 bloques de X son:*

1. *Los 12 bloques de la forma $L \cup \{\infty_1, \infty_2, \infty_3\}$, donde L es una recta de P.*
2. *Los 54 bloques de la forma $Q \cup \{\infty_i, \infty_j\}$, donde Q es un cuadrilátero de la clase Ω_k, para $k \neq i, j$.*
3. *Los 54 bloques de la forma $Q \cup \{D\} \cup \{\infty_k\}$, donde Q es un cuadrilátero de la clase Ω_k y D es su punto diagonal.*
4. *Los 12 bloques de la forma $L_1 \cup L_2$, donde L_1 y L_2 son dos rectas paralelas distintas.*

En particular, todos los sistemas de Steiner de tipo $S(4,5,11)$ son isomorfos.

Demostración: En cuanto a la descripción de los bloques, lo único que no es inmediato es que los 12 bloques que no contienen ningún punto infinito sean precisamente los pares de rectas paralelas, pero ello se debe a que, por una parte, las seis rectas que pasan por los pares de puntos de un cuadrilátero contienen los 5 puntos de su complementario (sus dos diagonales contienen el mismo punto diagonal y los cuatro lados paralelos dos a dos los cuatro puntos restantes), por lo que todo conjunto de 5 puntos contiene al menos una recta (contiene un cuadrilátero y un punto más que forma al menos una recta). A su vez, si un conjunto $B = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ no consta de dos rectas paralelas y $L_1 = \{P_1, P_2, P_3\}$ es una recta, el conjunto $\{P_2, P_3, P_4, P_5, P_6\}$ debe contener otra recta, que no puede ser $\{P_4, P_5, P_6\}$ (pues sería paralela a L_1), luego no perdemos generalidad si suponemos que es $L_2 = \{P_3, P_4, P_5\}$, pero entonces resulta que $Q = \{P_1, P_2, P_4, P_5\}$ es un cuadrilátero y P_3 es su punto diagonal, luego B contendría un conjunto de tipo $Q \cup \{D\}$ que también estaría

contenido en un bloque de tipo 3), lo cual es imposible, luego un bloque que conste de 6 puntos de P tiene que estar formado por dos rectas paralelas. Como hay exactamente 12 pares de rectas paralelas y tiene que haber 12 bloques, se dan todas las posibilidades.

La unicidad se prueba igual que en 7.28, de modo que, en realidad, podemos probar que entre dos sistemas de Steiner de tipo $S(5,6,12)$ existe siempre un isomorfismo que transforma cinco puntos cualesquiera del primero en cinco puntos cualesquiera del segundo. ∎

Ahora ya podemos hablar del sistema W_{12} y, por la prueba de la unicidad del teorema anterior, el grupo $M_{12} = \mathrm{Aut}(W_{12})$ es cinco veces transitivo sobre W_{12}. Más aún, si fijamos tres puntos distintos $\infty_1, \infty_2, \infty_3 \in W_{12}$, es claro que el estabilizador $(M_{12})_{\infty_1,\infty_2,\infty_3}$ es isomorfo al subgrupo M_9 de los automorfismos de W_9 que fijan a las tres clases de cuadriláteros Ω_i (en otras palabras, que todo automorfismo de M_9 se extiende a un automorfismo de M_{12} que fija a los tres puntos ∞_i). Como $|M_9|) = 72$ y M_{12} es cinco veces transitivo, obtenemos que

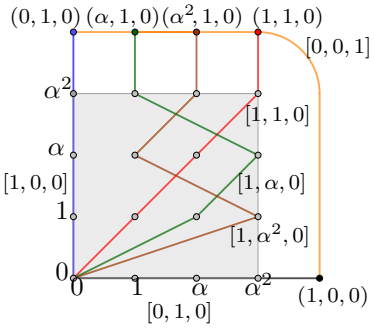
$$|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 72 = 95\,040,$$

luego M_{12} es estrictamente cinco veces transitivo en W_{12}.

A su vez, esto implica $|(M_{12})_{\infty_3}| = 95\,040/12 = 7\,920 = |M_{11}|$ y obviamente $(M_{12})_{\infty_3} \leq M_{11}$, luego de hecho tenemos la igualdad, es decir, que M_{11}, definido como $\mathrm{Aut}(W_{11})$, es también el estabilizador de un punto en M_{12}, de acuerdo con la definición 7.22.

Pasamos ahora a ocuparnos de los grupos de Mathieu grandes, y partimos de que, según [G 8.81], un sistema de Steiner de tipo $S(2,5,21)$ es un plano proyectivo de orden 4, y en [G 7.45] probamos que sólo existe un plano afín de orden 4, lo que a su vez implica que sólo existe un plano proyectivo de dicho orden, que será el plano $P = P(k^3)$, donde k es el cuerpo de cuatro elementos. Esto justifica ya la notación W_{21} para referirnos al único sistema de Steiner de tipo $S(2,5,21)$. Ahora vamos a estudiar su geometría:

El plano proyectivo de orden 4 Llamamos $P = P(k^3)$ al plano proyectivo sobre el cuerpo k de cuatro elementos. Concretamente, $k = \{0, 1, \alpha, \alpha^2\}$, donde $\alpha^2 + \alpha + 1 = 0$.



Representaremos los puntos de P en la forma $(a,b,c) = \langle (a,b,c) \rangle$, y la recta determinada por la ecuación $ax+by+cz = 0$ la representaremos como $[a,b,c]$. Podemos representar P gráficamente tomando como recta infinita la recta $z = 0$ (es decir, $[0,0,1]$), lo que nos permite representar los 16 puntos finitos de la forma $(a,b,1)$ mediante unos ejes coordenados, y aparte están los cinco puntos infinitos, cuatro de la forma $(a,1,0)$ más $(1,0,0)$. La figura muestra la recta infinita y las cinco rectas que pasan por el punto $(0,0)$.

El teorema siguiente no nos va a hacer falta más adelante, pero nos servirá para poner en contexto una definición que vamos a necesitar:

Teorema 7.30 *Si P es un plano proyectivo de orden q y $A \subset P$ es un conjunto de puntos no colineales tres a tres, entonces $|A| \leq q+2$ y si q es impar, de hecho, $|A| \leq q+1$.*

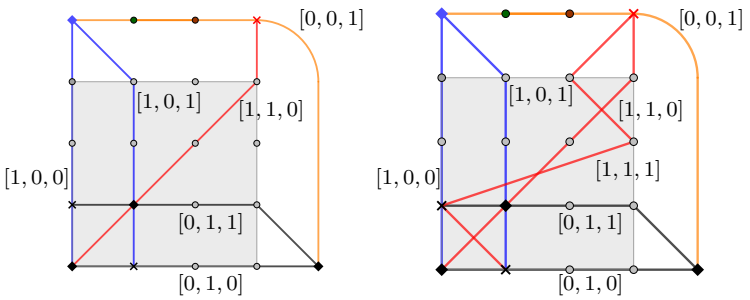
Demostración: Supongamos que A tiene n puntos y sea p uno de ellos. Entonces, para cada $q \in A \setminus \{p\}$, la aplicación $q \mapsto pq$ es una aplicación inyectiva de $A \setminus \{q\}$ en el haz de rectas que pasan por p, pero por un punto p pasan exactamente $q+1$ rectas, luego $n-1 \leq q+1$, y así $n \leq q+2$.

Si se da la igualdad, eso significa que todas las rectas que pasan por p cortan a A en otro punto, y esto vale para todo punto $p \in A$, luego concluimos que toda recta de P corta a A en 0 o 2 puntos. Sea $q \in P \setminus A$, de modo que cada recta que pasa por q y corta a A lo hace exactamente en 2 puntos (distintos para cada par de rectas, pues las rectas se cortan en q y no pueden coincidir en ningún punto de A), luego $|A|$ es igual al doble del número de rectas que pasan por q y cortan a A. Como $|A| = q+2$ y $|A|$ es par, es necesario que q también sea par. Por consiguiente, si q es impar tiene que ser $|A| < q+2$ o, equivalentemente, $|A| \leq q+1$. ∎

Un *arco* en un plano proyectivo es un conjunto de puntos no colineales tres a tres. Acabamos de probar que un arco en un plano proyectivo de orden impar q tiene a lo sumo $q+1$ elementos. Los arcos de cardinal $q+1$ se llaman *óvalos,* pero si q es par (como sucede en el caso $q=4$ que nos interesa) puede haber arcos de longitud $q+2$, y éstos reciben el nombre de *hiperóvalos.* En el caso $q=4$ los hiperóvalos son arcos de 6 puntos.

Recordemos [G 8.18] que un sistema de referencia proyectivo en un plano afín es un conjunto (ordenado) de 4 puntos tales que tres cualesquiera de ellos son proyectivamente independientes, es decir, no colineales. El teorema [G 8.20] afirma que cualquier sistema de referencia proyectivo se puede transformar en cualquier otro por una única homografía.

Un *cuadrilátero* es un arco de cuatro puntos, de modo que con los puntos de un mismo cuadrilátero se pueden formar 24 sistemas de referencia distintos. Hay 3 formas de dividir en dos pares los cuatro vértices de un cuadrilátero, lo que da lugar a 6 pares de rectas que se cortan en tres puntos llamados *puntos diagonales* del sistema.



La figura de la izquierda muestra el cuadrilátero formado por los puntos

$$(1,0,0), \quad (0,1,0), \quad (0,0,1), \quad (1,1,1),$$

que aparecen marcados con un rombo, y los tres puntos diagonales están señalados con un aspa. Se trata de los puntos $(1,0,1), (0,1,1), (1,1,0)$.

El determinante de estos tres vectores vale ± 2, lo que significa que, para un plano afín arguesiano, están alineados precisamente cuando q es potencia de 2, que es nuestro caso. Concretamente, están sobre la recta $[1,1,1]$.

Los cuatro puntos del cuadrilátero, junto con sus tres puntos diagonales y las siete rectas (figura de la derecha), forman un plano proyectivo de orden 2, es decir, un plano de Fano. (Esto era previsible: los puntos con coordenadas en el cuerpo de 2 elementos en un plano proyectivo de orden 4 forman un plano proyectivo de orden 2.)

Notemos que, puesto que cualquier cuadrilátero se convierte en cualquier otro mediante una homografía, lo que hemos obtenido es general: todo cuadrilátero se convierte en un plano de Fano cuando se le añaden sus tres puntos diagonales (y tomamos las 7 rectas que pasan por cada par de puntos).

Por otro lado, si consideramos de nuevo las 6 rectas determinadas por los pares de vértices de un cuadrilátero (sin añadir la determinada por sus puntos diagonales), vemos que pasan por 19 puntos en total o, equivalentemente, que no pasan por 2 puntos. Además de verse en la figura, es fácil razonarlo: cada una de las seis rectas consta de 5 puntos, que son dos vértices, un punto diagonal y otros 2 puntos más, luego entre todas pasan por 12 puntos "nuevos" aparte de los vértices y los tres puntos diagonales, lo que hace un total de 19 puntos. En el caso concreto del cuadrilátero canónico que estamos considerando, dichos puntos son $(\alpha^2, \alpha, 1)$ y $(\alpha, \alpha^2, 1)$.

Esto se traduce en que si queremos extender el cuadrilátero hasta un hiperóvalo, la única opción es añadir estos dos puntos (pues cualquier otro está alineado con dos puntos del cuadrilátero), y podemos comprobar que, ciertamente, la recta que los une, que es $[1,1,1]$, no pasa por ningún punto del cuadrilátero (pasa por los tres puntos diagonales), por lo que al añadir estos dos puntos al cuadrilátero obtenemos realmente un hiperóvalo. De nuevo esto es válido para cualquier cuadrilátero, y hemos probado casi todo el teorema siguiente:

Teorema 7.31 *Sea P un plano proyectivo de orden 4. Entonces:*

1. *Todo cuadrilátero se extiende a un único plano de Fano, concretamente al que resulta de añadirle sus tres puntos diagonales.*
2. *Todo cuadrilátero se extiende a un único hiperóvalo, concretamente al añadirle los dos puntos adicionales de la recta que pasa por sus puntos diagonales.*
3. *Todo óvalo se extiende a un único hiperóvalo.*
4. *P contiene 2 520 cuadriláteros, 360 planos de Fano y 168 hiperóvalos.*

DEMOSTRACIÓN: Sólo falta probar los dos últimos apartados. Un óvalo O contiene a un cuadrilátero Q, el cual está contenido en un único hiperóvalo H, que se obtiene añadiendo a Q los dos únicos puntos no alineados con dos puntos de Q, luego el quinto punto de O tiene que ser uno de esos dos, luego $O \subset H$ y la extensión es obviamente única.

Observemos que el número de sistemas de referencia proyectivos es igual a $|\mathrm{LGP}(3,4)| = 60\,480$. Como hay 24 sistemas de referencia proyectivos que corresponden a distintas ordenaciones de un mismo cuadrilátero, concluimos que el número de cuadriláteros es $60\,480/24 = 2\,520$.

Ahora observamos que cada plano de Fano contiene 7 cuadriláteros, resultantes de eliminar cualquiera de sus 7 rectas (el complementario de un cuadrilátero en un plano de Fano es siempre la recta que pasa por sus tres puntos diagonales). Como cada cuadrilátero está sólo en un plano, el número de planos es $2\,520/7 = 360$. Por último, cada hiperóvalo contiene 15 subconjuntos de 4 elementos, es decir, 15 cuadriláteros, por lo que el número de hiperóvalos es $2\,520/15 = 168$. ∎

Veamos una caracterización de los planos de Fano:

Teorema 7.32 *Si P es un plano proyectivo de orden 4, un subconjunto $F \subset P$ de 7 puntos es un plano de Fano si y sólo si toda recta de P corta a F en 1 o 3 puntos.*

DEMOSTRACIÓN: Si F es un plano de Fano, hay 7 rectas de P que cortan a F en tres puntos (las rectas de P que contienen las 7 rectas del plano proyectivo de orden 2). Por cada punto de F pasan 5 rectas de P, de las cuales 3 cortan a F en tres puntos y las otras dos lo cortan en 1, ya que si lo cortaran en 2 automáticamente lo cortarían en 3. Esto nos da $7 \cdot 2 = 14$ rectas que cortan a F en 1 punto, que unidas a las 7 que lo cortan en 3 puntos suman las 21 rectas de P, luego toda recta de P está en uno de los dos casos.

Supongamos ahora que F tiene la propiedad indicada y sea $\mathcal{B}$ el conjunto de los conjuntos de tres puntos colineales de F. Tenemos entonces que por cada par de puntos distintos de F pasa un único elemento de $\mathcal{B}$ (pues la recta que los une no puede cortar a F en un único punto, luego corta en 3 puntos, que determinan un elemento de $\mathcal{B}$, necesariamente único). Esto significa que $(F, \mathcal{B})$ es un sistema de Steiner de tipo $S(2,3,7)$, luego es un plano proyectivo de orden 2. Dados dos puntos $P_1, P_2 \in F$, están en elemento de $\mathcal{B}$ que tiene 3 puntos, luego podemos tomar otro punto P_3 no colineal con los dos anteriores, y los 3 elementos de $\mathcal{B}$ que pasan por ellos contienen 6 puntos, luego hay un séptimo punto P_4 y F, de modo que $Q = \{P_1, P_2, P_3, P_4\} \subset F$ es un cuadrilátero, y F tiene que contener sus puntos diagonales, luego F es el plano de Fano de Q. ∎

Nota En realidad hemos probado que si $F \subset P$ es un conjunto de 7 puntos tal que toda recta que corta a F en al menos un punto lo corta exactamente en 3 puntos, entonces F es un plano de Fano. No necesitamos suponer que no hay rectas disjuntas con F, aunque de hecho es así. ∎

El grupo $\mathrm{Aut}(P)$ de los automorfismos de P es, por definición, el grupo de las colineaciones de P, que por [G 8.27] es isomorfo al grupo $\mathrm{L\Gamma P}(3,4)$ de las semihomografías de P que no coincide con el grupo $\mathrm{LGP}(3,4)$ de las homografías, porque el cuerpo k de 4 elementos tiene un (único) automorfismo no trivial σ, de orden 2, que determina un semiisomorfismo $\sigma : k^3 \longrightarrow k^3$ dado por $\sigma(a,b,c) = (\sigma(a), \sigma(b), \sigma(c))$, que a su vez induce una semihomografía $\sigma : P \longrightarrow P$. Según se ve tras [G 8.27], se cumple que

$$\mathrm{L\Gamma P}(3,4) = [\mathrm{LGP}(3,4)]\,\langle\sigma\rangle\,,$$

por lo que en particular $|\mathrm{L\Gamma P}(3,4) : \mathrm{LGP}(3,4)| = 2$. Consideramos también el subgripo $\mathrm{LEP}(3,4)$, que tiene índice 3 en $\mathrm{LGP}(3,4)$, luego

$$|\mathrm{LEP}(3,4)| = 20\,160, \qquad |\mathrm{LGP}(3,4)| = 60\,480, \qquad |\mathrm{L\Gamma P}(3,4)| = 120\,960.$$

Llamemos $G = \mathrm{LGP}(3,4)$ y $G^* = \mathrm{LEP}(3,4)$.

Si H es un hiperóvalo, podemos considerar el subgrupo $G_H \leq G$ formado por las homografías $f \in G$ que cumplen $f[H] = H$. Entonces G_H actúa sobre H, de modo que tenemos un homomorfismo de grupos $G_H \longrightarrow \Sigma_H \cong \Sigma_6$. De hecho, se trata de un monomorfismo, pues H contiene un sistema de referencia proyectivo, luego si $f \in G_H$ fija a todos los puntos de H es que es la identidad. Así pues, G_H es un grupo de permutaciones sobre H.

Más aún, como cualquier cuádrupla de elementos de H distintos dos a dos es un sistema de referencia proyectivo, y H es el único hiperóvalo que lo contiene, tenemos que G_H es cuatro veces transitivo sobre H (la única homografía que transforma un sistema de referencia contenido en H en otro tiene que transformar H en H).

La imagen de G_H en Σ_H no puede ser todo Σ_H. Por ejemplo, no contiene ninguna trasposición, pues una trasposición fijaría a cuatro de los seis elementos de H, es decir, fijaría a un sistema de referencia proyectivo, luego tendría que ser la identidad. Sin embargo, dicha imagen contiene a todos los ciclos de longitud 3, pues, por la transitividad cuádruple, tiene que existir $f \in G_H$ tal que, si $H = \{P_1, \ldots, P_6\}$, se cumple $f(P_1) = P_2$, $f(P_2) = P_3$, $f(P_3) = P_1$, $f(P_4) = P_4$, y esto implica que la permutación inducida por f es $(1,2,3)$ o bien $(1,2,3)(5,6)$, pero en el segundo caso, elevando a la cuarta, concluimos que $(1,2,3)$ también está en la imagen. El teorema 2.19 implica que la imagen es A_6, con lo que $G_H \cong A_6$.

Consideremos ahora el caso concreto en que H es el hiperóvalo canómico que hemos considerado más arriba. La homografía que permuta cíclicamente los puntos $(1,0,0), (0,1,0), (0,0,1)$ y fija $(1,1,1)$ es la dada por la matriz

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

que tiene determinante 1, luego está en realidad en G^*. Vamos a probar que cualquier homografía que permuta cíclicamente tres de los puntos de H está

también en G^*. Sean $P, Q, R, S \in H$ puntos distintos y sea $g \in G_H$ la homografía dada por

$$g(1,0,0) = P, \quad g(0,1,0) = Q, \quad g(0,0,1) = R, \quad g(1,1,1) = S.$$

Entonces $g \circ f \circ g^{-1}$ es la homografía que permuta cíclicamente P, Q, R y tiene determinante 1. Concluimos que, en realidad, $G_H \leq \mathrm{LEP}(3,4)$ o, equivalentemente, que si llamamos G_H^* al subgrupo formado por las homografías que cumplen $f[H] = H$, tenemos que $G_H^* = G_H$.

Hemos visto que la acción de G sobre el conjunto de los hiperóvalos es transitiva, pero esto ya no es así si consideramos la acción de G^*, pues $|G^*| = 20\,160$ y el orden de un estabilizador G_H^* es $|A_6| = 6!/2 = 360$, luego las órbitas tienen longitudes $20\,160/360 = 56$. Esto prueba parte del teorema siguiente:

Teorema 7.33 *Sea P el plano proyectivo sobre el cuerpo de 4 elementos. El grupo $\mathrm{LEP}(3,4)$ divide a los 168 hiperóvalos de P en tres órbitas de 56 hiperóvalos cada una, y a los 360 planos de Fano de P en tres órbitas de 120 planos cada una.*

Demostración: Falta probar la afirmación correspondiente a los planos de Fano. Seguimos llamando G y G^* a los grupos de homografías de P. No perdemos generalidad si consideramos el plano canónico F que contiene a los puntos

$$(1,0,0), \quad (0,1,0), \quad (0,0,1) \quad (1,1,1).$$

En efecto, si F' es otro plano de Fano, existe $g \in G$ tal que $g[F'] = F$ y, para cada $f \in \mathrm{LEP}(3,4)$, se cumple que

$$f[F'] = f[g^{-1}[F]] = g^{-1}[g[f[g^{-1}[F]]] = g^{-1}[f^g[F]],$$

por lo que g biyecta la órbita de F' con la de F.

Nuevamente, como F contiene un sistema de referencia proyectivo, el subgrupo G_F formado por las homografías $f \in G$ tales que $f[F] = F$ es un grupo de permutaciones sobre F, es decir, que la aplicación $G_F \longrightarrow \Sigma_F$ es un monomorfismo de grupos.

Ahora bien, como los elementos de G son homografías, los elementos de G_F determinan colineaciones sobre F y, como el cuerpo de 2 elementos no tiene automorfismos no triviales, las colineaciones de un plano de Fano son sus homografías [G. 8.27], luego en realidad $G_F \longrightarrow \mathrm{LGP}(3,2)$.

Pero las homografías de P inducidas por matrices cuyos coeficientes están en el cuerpo de 2 elementos son precisamente $\mathrm{LGP}(3,2)$, luego $G_F = \mathrm{LGP}(3,2)$. Pero las matrices regulares cuyos coeficientes están en el cuerpo de 2 elementos tienen todas determinante 1, luego $G_F \leq G^*$ y, de hecho, $G_F = G_F^*$. Exactamente igual en el caso de los hiperóvalos, ahora podemos concluir que la acción de G^* determina tres órbitas de planos de Fano. ∎

Llamamos $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$ a las tres órbitas de 56 hiperóvalos determinadas por $\mathrm{LEP}(3,4)$ y $\mathcal{F}_i$ a la clase de los planos de Fano generados por los cuadriláteros contenidos en los hiperóvalos de $\mathcal{H}_i$, que son claramente las tres clases de planos de Fano consideradas en el teorema anterior.

Teorema 7.34 *Si P es el plano proyectivo de orden 4, cada triángulo en P está contenido en un único hiperóvalo de cada órbita $\mathcal{H}_i$, y las tres órbitas son las únicas clases de hiperóvalos con esta propiedad.*

DEMOSTRACIÓN: Sea T_0 un triángulo prefijado. Para cualquier otro triángulo T, existe $f \in \mathrm{LGP}(3,4)$ tal que $f[T_0] = T$, pero si f tiene matriz A en el sistema de referencia canónico y $\alpha = |A|$, la homografía g que resulta de dividir una fila de A entre α cumple $g \in G = \mathrm{LEP}(3,4)$ y sigue cumpliendo que $g[T_0] = T$, luego G actúa transitivamente sobre los triángulos (y fija a las tres clases $\mathcal{H}_i$). De aquí se sigue que si un triángulo T está contenido exactamente en m hiperóvalos de $\mathcal{H}_i$, entonces todos los triángulos están contenidos exactamente en m hiperóbalos de $\mathcal{H}_i$.

Ahora consideramos todas las cuádruplas (P_1, P_2, P_3, H) tales que el conjunto $\{P_1, P_2, P_3\}$ es un triángulo contenido en $H \in \mathcal{H}_i$ (para un i fijo). Cada uno de los 56 hiperóvalos de $\mathcal{H}_i$ contiene $6 \cdot 5 \cdot 4 = 120$ ternas (P_1, P_2, P_3), luego hay $56 \cdot 120 = 6\,720$ cuádruplas. Por otra parte, hay $21 \cdot 20 \cdot 16 = 6\,720$ ternas (P_1, P_2, P_3) que forman triángulos, luego el número de cuádruplas debe ser $6\,720m$, de donde $m = 1$. Esto prueba la primera parte del teorema.

Antes de probar la segunda, vamos a extraer de ella unas consecuencias. En primer lugar, es claro que hay 12 hiperóvalos en P que contienen dos puntos distintos dados P_1, P_2. En efecto, hay $16 \cdot 9/2 = 72$ cuadriláteros que los contienen, cada uno de los cuales está contenido en un único hiperóvalo, pero cada hiperóvalo contiene $4 \cdot 3/2 = 6$ cuadriláteros que contienen a los dos puntos, luego hay $72/6 = 12$ hiperóvalos.

En segundo lugar: si H es un hiperóvalo y $P_1, P_2 \in H$ son dos puntos distintos, existen exactamente 3 hiperóvalos H' tales que $H \cap H' = \{P_1, P_2\}$.

En efecto, H contiene cuatro triángulos con P_1, P_2 entre sus vértices y cada uno de dichos triángulos está contenido en un único hiperóvalo de $\mathcal{H}_i$, lo que nos da tres hiperóvalos, el propio H y otros dos. Estos ocho hiperóvalos son distintos dos a dos, pues, si dos coincidieran, tendríamos un hiperóvalo distinto de H que contendría dos triángulos $\{P_1, P_2, P_3\}$ y $\{P_1, P_2, P_4\}$, es decir, que tendría cuatro puntos en común con H, lo cual es imposible (cada cuadrilátero está contenido en un único hiperóvalo). Así pues, de los 12 hiperóvalos que contienen a $\{P_1, P_2\}$, uno es H, otros 8 cortan a H en 3 puntos y quedan 3 que cortan a H en $\{P_1, P_2\}$.

Pasemos ya a probar la segunda parte del teorema, es decir, suponemos que $\mathcal{H}$ es una clase de hiperóvalos con la propiedad de que cada triángulo está contenido en un único hiperóvalo de $\mathcal{H}$. Como hay $21 \cdot 20 \cdot 16/6 = 1\,120$ triángulos y cada hiperóvalo contiene 20 triángulos, necesariamente $|\mathcal{H}| = 56$.

Si $H \in \mathcal{H}$, cada hiperóvalo $H' \in \mathcal{H}$ corta a H a lo sumo en dos puntos (pues en caso contrario un triángulo estaría en dos elementos de $\mathcal{H}$).

Si $P_1, P_2 \in H$, hay 16 triángulos en P que contienen a ambos puntos, cada uno de los cuales está en un hiperóvalo de $\mathcal{H}$, pero un mismo hiperóvalo contiene 4 triángulos con vértices P_1, P_2, luego $\{P_1, P_2\}$ está contenido en 4 hiperóvalos de $\mathcal{H}$, de los cuales uno es H, por lo que hay exactamente 3 hiperóvalos

en $\mathcal{H}$ que cortan a H en dos puntos. Ahora bien, hemos probado que en P sólo hay tres hiperóvalos en tales condiciones. Por lo tanto, lo que tenemos es que si $P_1, P_2 \in H$ son puntos distintos, los tres hiperóvalos que cortan a H en dichos puntos están en $\mathcal{H}$. Pero esto vale también para las clases $\mathcal{H}_i$, luego podemos afirmar que si $H \in \mathcal{H} \cap \mathcal{H}_i$, para cada par de puntos $P_1, P_2 \in H$, los tres hiperóvalos que cortan a H en dichos puntos están en $\mathcal{H} \cap \mathcal{H}_i$. Como H contiene 15 pares de puntos, concluimos que si $H \in \mathcal{H} \cap \mathcal{H}_i$, los 45 hiperóvalos que cortan a H en dos puntos están en $\mathcal{H} \cap \mathcal{H}_i$.

Esto implica que $\mathcal{H}$ no puede cortar a dos clases $\mathcal{H}_i$, ya que entonces debería contener al menos 90 hiperóvalos, pero sólo tiene 56. Por lo tanto, existe un i tal que $\mathcal{H} \subset \mathcal{H}_i$ y, como ambas clases tienen 56 elementos, de hecho $\mathcal{H} = \mathcal{H}_i$. ∎

Observemos ahora que el grupo $\mathrm{Aut}(P) = \mathrm{L\Gamma P}(3,4)$ actúa sobre el conjunto $\Omega = \{\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3\}$, ya que si $H, H' \in \mathcal{H}_i$, existe $f \in \mathrm{LEP}(3,4)$ tal que $H' = f[H]$ y, si $g \in \mathrm{Aut}(P)$, entonces $g[H'] = g[f[H]] = f^{g^{-1}}[g[H]]$, donde $f^{g^{-1}} \in \mathrm{LE}(3,4)$, por lo que $g[H']$ y $g[H]$ están en una misma órbita $g[\mathcal{H}_i]$. Tenemos así un homomorfismo de grupos $\mathrm{Aut}(P) \longrightarrow \Sigma_\Omega$ que resulta ser suprayectivo. Más precisamente:

Teorema 7.35 *Sea P un plano proyectivo de orden 4, sea $G = \mathrm{Aut}(P)$, sean $p_1, p_2 \in P$ dos puntos distintos y sea $H = G_{p,1}$ el estabilizador de ambos puntos respecto de la acción de G en P. Entonces, el homomorfismo $H \longrightarrow \Sigma_\Omega$ inducido por la acción de G es un epimorfismo.*

Demostración: Eligiendo el sistema de referencia adecuado, no perdemos generalidad si suponemos que los puntos p_1, p_2 tienen coordenadas $(1,0,0)$ y $(0,1,0)$, respectivamente.

Sabemos que $\mathrm{LGP}(3,4)$ es transitivo sobre Ω, mientras que $\mathrm{LEP}(3,4)$ actúa trivialmente, luego el cociente $\mathrm{LGP}(3,4)/\mathrm{LEP}(3,4)$ actúa también transitivamente sobre Ω, y es un grupo de orden 3. Esto implica que cualquier $f \in \mathrm{LGP}(3,4)$ que no esté en $\mathrm{LEP}(3,4)$ permuta cíclicamente las tres clases de Ω. Consideremos, por ejemplo, la homografía determinada por la matriz

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

Observemos que $f \in H$ y, según acabamos de razonar, induce un ciclo de longitud 3 en Σ_Ω. Si hacemos actuar $1, f, f^2$ sobre el cuadrilátero canónico obtenemos los cuadriláteros

$$\begin{array}{c|cccc} Q_1 & (1,0,0) & (0,1,0) & (0,0,1) & (1,1,1) \\ Q_2 & (1,0,0) & (0,1,0) & (0,0,\alpha) & (1,1,\alpha) \\ Q_3 & (1,0,0) & (0,1,0) & (0,0,\alpha^2) & (1,1,\alpha^2) \end{array}$$

Por consiguiente, los hiperóvalos que los contienen están cada uno en una de las tres clases de Ω. Si llamamos g a la semihomografía inducida por el automorfismo no trivial σ del cuerpo k, es decir, la dada por $g(a,b,c) = (\sigma(a), \sigma(b), \sigma(c))$,

vemos que $\sigma \in H$, $\sigma[Q_1] = Q_1$, $\sigma[Q_2] = Q_3$, $\sigma[Q_3] = Q_2$, luego σ induce una transposición sobre Ω. Así pues, la imagen de H en Σ_Ω contiene al menos un ciclo de longitud 3 y una transposición, luego tiene que ser todo Σ_Ω. ∎

A su vez, esto implica que el núcleo del homomorfismo $\mathrm{Aut}(P) \longrightarrow \Sigma_\Omega$ tiene que tener índice 6 en $\mathrm{Aut}(P)$ y tiene que contener a $\mathrm{LEP}(3,4)$, luego es $\mathrm{LEP}(3,4)$. Por lo tanto:

> *Los automorfismos de P que fijan las tres clases de hiperóvalos $\mathcal{H}_i$ son exactamente los elementos de* $\mathrm{LEP}(3,4)$.

Con esto ya tenemos suficiente para probar la unicidad de los sistemas de Steiner que hemos construido:

Teorema 7.36 *Si $(X, \mathcal{B})$ es un sistema de Steiner de tipo $S(3,6,22)$ y $\infty \in X$, entonces el sistema derivado $P = X_\infty$ es un plano proyectivo de orden 4 y sus 77 bloques son:*

1. *Los 21 conjuntos de la forma $L \cup \{\infty\}$, donde L es una recta en P.*
2. *Los 56 hiperóvalos de una de las órbitas $\mathcal{H}_i$ definidas por* $\mathrm{LEP}(3,4)$

En particular, todos los sistemas de Steiner de tipo $S(3,6,22)$ son isomorfos.

La prueba es completamente análoga a la de 7.27 y muestra que, si usamos la notación W_{22} para referirnos a cualquier sistema de Steiner de tipo $S(3,6,22)$, el grupo $\mathrm{Aut}(W_{22})$ es triplemente transitivo sobre W_{22}. A su vez, es claro que el estabilizador de un punto $\infty \in W_{22}$ es isomorfo al estabilizador de una clase $\mathcal{H}_i$ en $\mathrm{Aut}(P)$, cuyo orden es $120\,960/3 = 40\,320$, luego

$$|\mathrm{Aut}(W_{22})| = 22 \cdot 40\,320 = 887\,040.$$

Teorema 7.37 *Si $(X, \mathcal{B})$ es un sistema de Steiner de tipo $S(4,7,23)$ y fijamos dos puntos $\infty_1, \infty_2 \in X$, el sistema derivado $P = X_{\infty_1,\infty_2}$ es un plano proyectivo de orden 4 y, numerando adecuadamente las clases $\mathcal{H}_i$, sus 253 bloques son:*

1. *Los 21 conjuntos de la forma $L \cup \{\infty_1, \infty_2\}$, donde L es una recta en P.*
2. *Los 112 conjuntos de la forma $H \cup \{\infty_i\}$, con $H \in \mathcal{H}_i$, para $i = 1, 2$.*
3. *Los 120 planos de Fano de la clase $\mathcal{F}_3$.*

En particular, todos los sistemas de Steiner de tipo $S(4,7,23)$ son isomorfos.

Demostración: Ciertamente, por definición de sistema derivado, los bloques que contienen a ∞_1, ∞_2 tienen que ser los descritos en el punto 1). A su vez, los bloques que contienen a ∞_1 pero no a ∞_2 son de la forma $B \cup \{\infty_1\}$, donde B es un bloque del sistema derivado X_{∞_1} que no contienen a ∞_2, luego, según el teorema anterior, forman una clase de hiperóvalos de P que podemos numerar como $\mathcal{H}_1$. Lo mismo vale para X_{∞_2}, que tiene que tener asociada una

clase distinta, que podemos etiquetar como $\mathcal{H}_2$. Esto significa que los bloques que contienen a uno de los puntos ∞_i (pero no al otro) son de la forma descrita en 2). Falta identificar los 120 bloques que no contienen a ninguno de los puntos ∞_1, ∞_2. Vamos a llamar $\mathcal{F}$ a la familia de todos ellos y vamos a probar que es $\mathcal{F} = \mathcal{F}_3$.

Empezamos observando que si $F \in \mathcal{F}$ y $P_1, P_2 \in F$ son puntos distintos, la recta L que pasa por ambos no puede tener más de tres puntos en común con F, pues, si tuviera cuatro, dichos puntos estarían en F y en un bloque de tipo 1), lo cual es imposible. Por otra parte, el sistema derivado $X_{P_1P_2}$ es un plano proyectivo de orden 4 que contiene como rectas a $F \setminus \{P_1, P_2\}$ y también a $(L \cup \{\infty_1, \infty_2\}) \setminus \{P_1, P_2\}$, pero dos rectas se tienen que cortar en un punto, que no puede ser ∞_1, ∞_2 (pues estos puntos no están en F), por lo que existe un tercer punto $P_3 \in P$ tal que $L = \{P_1, P_2, P_3\}$. En otras palabras: toda recta que pasa por dos puntos de F corta a F en tres puntos. Por el teorema 7.32 (véase la nota posterior) tenemos que los elementos de $\mathcal{F}$ son planos de Fano.

Si Q es un cuadrilátero contenido en un hiperóvalo de $\mathcal{H}_3$, no puede estar contenido en ningún bloque de tipo 1 o 2, luego tiene que estar contenido en un elemento de $\mathcal{F}$, por lo que $\mathcal{F}_3 \subset \mathcal{F}$ y, como ambas clases tienen el mismo número de elementos, se da la igualdad.

Supongamos ahora que tenemos dos sistemas de Steiner $(X, \mathcal{B})$, $(X', \mathcal{B}')$ del tipo considerado y seleccionemos arbitrariamente un cuatro de puntos en cada uno, digamos $p, q, \infty_1, \infty_2 \in X$, $p', q', \infty_1', \infty_2' \in X'$. Entonces $P = X_{\infty_1,\infty_2}$, $P' = X'_{\infty_1',\infty_2'}$ son planos proyectivos de orden 4, luego podemos considerar un isomorfismo $f : P \longrightarrow P'$. Más aún, como podemos enviar cualquier sistema de referencia proyectivo de P a cualquier sistema de referencia proyectivo de P', podemos exigir que $f(p) = p'$, $f(q) = q'$. Si numeramos las clases de hiperóvalos de P y P' de acuerdo con el enunciado (es decir, de modo que $\mathcal{H}_1$ es la clase de los hiperóvalos contenidos en bloques que contienen a ∞_1, etc.) tenemos que $f[\mathcal{H}_i]$ son las tres clases de hiperóvalos de P', y por el teorema 7.35, componiendo f con un automorfismo de P' que fije a p_1, p_2, podemos exigir que $f[\mathcal{H}_i] = \mathcal{H}_i'$, para $i = 1, 2, 3$, luego también $f[\mathcal{F}_i] = \mathcal{F}_i'$. Así, si extendemos f a X mediante $f(\infty_i) = \infty_i'$ tenemos un isomorfismo entre los sistemas de Steiner dados. ∎

Ya podemos llamar W_{23} a cualquier sistema de Steiner de tipo $S(4, 7, 23)$. De la prueba de la unicidad del teorema anterior se desprende que el grupo $M_{23} = \mathrm{Aut}(W_{23})$ es cuatro veces transitivo sobre W_{23}. Además, el estabilizador de ∞_1, ∞_2 es isomorfo al subgrupo de $\mathrm{Aut}(P)$ que fija a las tres clases $\mathcal{H}_i$, y tras el teorema 7.35 hemos visto que dicho subgrupo es $M_{21} = \mathrm{LEP}(3, 4)$, luego

$$|M_{23}| = 23 \cdot 22 \cdot |\mathrm{LEP}(3, 4)| = 23 \cdot 22 \cdot 20\,160 = 10\,200\,960.$$

Teorema 7.38 *Si $(X, \mathcal{B})$ es un sistema de Steiner de tipo $S(5, 8, 24)$ y fijamos tres puntos $\infty_1, \infty_2, \infty_3 \in X$, el sistema derivado $P = X_{\infty_1,\infty_2,\infty_3}$ es un plano proyectivo de orden 4 y, numerando adecuadamente las clases $\mathcal{H}_i$, sus 759 bloques son los de la forma:*

1. *Los 21 conjuntos $L \cup \{\infty_1, \infty_2, \infty_3\}$, donde L es una recta en P.*

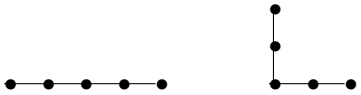
2. *Los* 168 *conjuntos* $H \cup \{\infty_i, \infty_j\}$, *con* $H \in \mathcal{H}_k$, $i \neq k \neq j$.

3. *Los* 360 *conjuntos* $F \cup \{\infty_i\}$, *con* $F \in \mathcal{F}_i$.

4. *Los* 210 *conjuntos* $(L \cup L') \setminus (L \cap L')$, *con* L *y* L' *rectas distintas en* P.

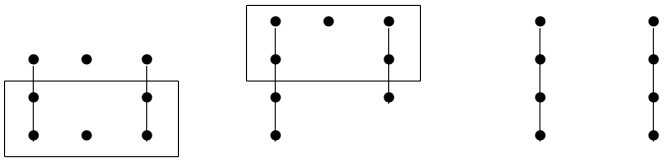
En particular, todos los sistemas de Steiner de tipo $S(5, 8, 24)$ *son isomorfos.*

De los dos teoremas anteriores se sigue fácilmente que los bloques tienen que ser de la forma indicada salvo los 210 que no contienen ninguno de los tres puntos infinitos. Llamemos $\mathcal{B}_0$ al conjunto de estos bloques. Cada $B \in \mathcal{B}_0$ es un conjunto de 8 puntos de P que no puede tener 5 puntos en común con una recta, un hiperóvalo o un plano de Fano. Explícitamente, esto significa, por una parte, que B no puede contener subconjuntos de 5 puntos de la forma



En el primer caso B contendría una recta y en el segundo contendría un cuadrilátero junto con uno de sus puntos diagonales, y al añadir los otros dos tendríamos un plano de Fano. Por otro lado, como todo óvalo se extiende a un hiperóvalo, B no puede contener óvalos, es decir, que todo subconjunto de 5 puntos contiene al menos tres puntos colineales.

Así pues, B contiene tres puntos colineales, y entre los otros 5 puntos de B tiene que haber otros tres más, de modo que la situación es la que muestra la figura de la izquierda. Entre los cinco puntos rodeados por el rectángulo tiene que haber también tres colineales, pero la única posibilidad que no da lugar a subconjuntos de 5 puntos de los dos tipos que hemos excluido es la que muestra la figura central.



De entre los cinco puntos rodeados en dicha figura, tiene que haber tres colineales, y nuevamente la única opción que no da lugar a subconjuntos de los tipos excluidos es la que muestra la figura de la derecha, de modo que B es la unión de dos rectas menos su punto de intersección.

Esto prueba que todos los bloques de $\mathcal{B}_0$ son del tipo descrito en 4, pero hay precisamente 210 pares de rectas en P, luego $\mathcal{B}_0$ consta necesariamente de todos los conjuntos de la forma indicada.

La unicidad se prueba de la forma habitual: si tenemos dos sistemas $(X, \mathcal{B})$, $(X', \mathcal{B}')$, podemos fijar cinco puntos distintos en cada uno, digamos

$$p_1, p_2, \infty_1, \infty_2, \infty_3 \in X, \qquad p'_1, p'_2, \infty'_1, \infty'_2, \infty'_3 \in X',$$

de modo que los derivados $P = X_{\infty_1,\infty_2,\infty_3}$ y $P' = X'_{\infty'_1,\infty'_2,\infty'_3}$ son planos proyectivos de orden 4, con lo que existe una homografía $f : P \longrightarrow P'$ que podemos exigir que cumpla $f(p_i) = p'_i$, para $i = 1, 2$. Más aún, en virtud del teorema 7.35, componiendo con un automorfismo de P' que fije a p_1, p_2, podemos exigir que f haga corresponder la clase de planos de Fano asociada a ∞_i con la asociada a ∞'_i, lo que nos permite extender f a un isomorfismo entre los sistemas dados mediante $f(\infty_i) = \infty'_i$. ∎

Esto justifica la notación W_{24} para los sistemas de Steiner de tipo $S(5, 8, 24)$, y además tenemos que el grupo de Mathieu $M_{24} = \mathrm{Aut}(W_{24})$ es cinco veces transitivo sobre W_{24}.

Más aún, si fijamos tres puntos distintos $\infty_1, \infty_2, \infty_3 \in W_{24}$, el estabilizador $(M_{24})_{\infty_1,\infty_2,\infty_3}$ se identifica claramente con el subgrupo $M_{21} = \mathrm{LEP}(3, 4)$ de $\mathrm{Aut}(W_{21})$ formado por los automorfismos que fijan a las tres clases de hiperóvalos (luego también a las de planos de Fano). Como M_{24} es cinco veces transitivo, esto implica que

$$|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 20\,160 = 244\,823\,040.$$

A su vez, de aquí se sigue que $(M_{24})_{\infty_3} = |M_{24}|/24 = 10\,200\,960 = |M_{23}|$, y tenemos la inclusión $(M_{24})_{\infty_3} \leq \mathrm{Aut}(W_{23}) = M_{23}$, por lo que se da la igualdad, y esto prueba que M_{23}, definido como $\mathrm{Aut}(W_{23})$ es ciertamente el grupo de Mathieu M_{23} según la definición 7.22.

La tabla siguiente muestra los órdenes de los grupos de Mathieu:

n	$\lvert M_n\rvert$	$\lvert\mathrm{Aut}(W_n) : M_n\rvert$
9	72	6
10	720	2
11	7 920	1
12	95 040	1
21	20 160	6
22	443 520	2
23	10 200 960	1
24	244 823 040	1

También hemos demostrado que $M_{21} = \mathrm{LEP}(3, 4)$, que es un grupo simple, por 7.17. Como M_{22} es triplemente transitivo y 22 no es potencia de 2, el teorema 7.12 implica que M_{22} también es simple y, a su vez esto implica, por el mismo teorema, la simplicidad de M_{23} y M_{24}. A continuación vamos a probar que M_{11} también es simple, con lo que 7.12 implicará que M_{12} también lo es. Vamos a dar un argumento que se apoya esencialmente en que 11 es primo, y que es aplicable igualmente al caso de M_{23}.

Teorema 7.39 *Sea $G \leq \Sigma_p$ un subgrupo transitivo, donde p es un número primo, y supongamos que $|G| = pnr$, donde $n \equiv 1$ (mód p) y $r < p$ también es primo. Entonces G es simple.*

DEMOSTRACIÓN: Supongamos de momento que $G \leq \Sigma_p$ es un subgrupo transitivo arbitrario donde p es primo, sin suponer las hipótesis restantes del teorema.

Sea $\Omega = \{1, \dots, p\}$. La transitividad implica que $|G| = p|G_1|$, luego

$$p \mid |G| \mid |\Sigma_p| = p!$$

Por lo tanto, $|G| = pm$, donde $m \mid (p-1)!$, por lo que $p \nmid m$. Así pues, si P es un p-subgrupo de Sylow de G, tenemos que $|P| = p$, luego $P = \langle\sigma\rangle$, donde σ es un ciclo de longitud p. La teoría de Sylow nos da que el número de p-subgrupos de Sylow es $\nu_p = |G : N_G(P)|$, luego podemos descomponer

$$|G| = |P||N_G(P) : P||G : N_G(P)| = p\nu_p r_p,$$

donde $r_p = |N_G(P) : P|$ y $\nu_p \equiv 1 \pmod p$. Por otra parte,

$$P \leq N_G(P) \leq N_{\Sigma_p}(P).$$

En Σ_p hay $p!/p = (p-1)!$ ciclos de longitud p, que forman $(p-2)!$ subgrupos de orden p. Es claro que Σ_p actúa transitivamente sobre todos ellos por conjugación, y $N_{\Sigma_p}(P)$ es el estabilizador de P respecto de dicha acción, luego $|N_{\Sigma_p}(P)| = p!/(p-2)! = p(p-1)$. Por consiguiente,

$$r_p = |N_G(P) : P| \mid p - 1.$$

Observemos por último que si $\nu_p \neq 1$, entonces $r_p \neq 1$. En efecto, supongamos que $r_p = 1$, es decir, que $N_G(P) = P$, con lo que $|G| = p\nu_p$. El número de elementos de orden p en G es $\nu_p(p-1) = |G| - \nu_p$, y todos ellos son ciclos de longitud p que, por consiguiente, no tienen puntos fijos en Ω. Por otro lado, si $x \in \Omega$, tenemos que $|G_x| = |G|/p = \nu_p$, lo que significa que G_x contiene todos los elementos de G que tienen al menos un punto fijo. Por consiguiente, todos los estabilizadores son el mismo conjunto: $G_1 = G_2 = \cdots = G_p$, pero esto significa que $G_1 = 1$, luego $\nu_p = |G_1| = 1$.

A partir de aquí suponemos que $|G|$ admite la descomposición del teorema:

$$|G| = pnr = p\nu_p r_p.$$

Simplificando p y tomando restos módulo p resulta que $r \equiv r_p \pmod p$, pero ambos valores son menores que p, luego $r = r_p$ y a su vez $n = \nu_p$.

Pasemos ya a probar que G es simple. En caso contrario posee un subgrupo normal propio N. Por el teorema 7.8 sabemos que N actúa transitivamente sobre Ω, luego $p \mid |N|$, luego N contiene un p-subgrupo de Sylow P de G, pero al ser normal los contiene a todos, luego $\nu_p(N) = \nu_p(G) = n$.

Aplicando a N lo que hemos probado en general para subgrupos transitivos de Σ_p, tenemos que

$$|N| = pnr_p(N) \mid pnr,$$

luego $r_p(N) \mid r$ y estamos suponiendo que r es primo. Además sabemos que, como $\nu_p(N) \neq 1$, también $r_p(N) \neq 1$, luego $r_p(N) = r$, luego $|N| = |G|$. ∎

Este teorema se aplica al grupo M_{11}, pues $|M_{11}| = 7\,920 = 11 \cdot 720$ y observamos que $720 \equiv 5$ (mód 11), luego la descomposición $|M_{11}| = 11 \cdot 144 \cdot 5$ está en las condiciones del teorema anterior, lo que nos permite concluir que M_{11} es simple.

Aunque no lo necesitamos, un cálculo análogo puede usarse para probar que el grupo M_{23} es simple. Así pues:

Teorema 7.40 *Los grupos de Mathieu $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ son simples.*

Podríamos haber incluido también $M_{21} \cong \mathrm{LEP}(3,4)$, que también es simple, pero cuando se habla de "los grupos de Mathieu" es frecuente entender que se está haciendo referencia a estos cinco grupos, pues no sólo son grupos simples, sino que son grupos simples esporádicos, es decir, grupos simples que no pertenecen a ninguna familia infinita de grupos simples, al contrario que M_{21}, que pertenece a la familia de los grupos simples $\mathrm{LEP}(n,q)$.

Nota Ahora podemos precisar el resultado que hemos anunciado más arriba: los únicos grupos de permutaciones seis veces transitivos son los grupos Σ_n para $n \geq 6$ y A_n para $n \geq 8$, mientras que los grupos cinco veces transitivos son Σ_n para $n \geq 5$ y A_n para $n \geq 7$ y además los grupos M_{12} y M_{24}, y los únicos grupos cuatro veces transitivos son los grupos Σ_n para $n \geq 4$ y A_n para $n \geq 6$, más los cuatro grupos M_{11}, M_{12}, M_{23}, M_{24}.

Sin embargo, la prueba de estos hechos se apoya en el teorema de clasificación de los grupos simples finitos. ∎

El grupo M_{10} Vamos a estudiar más a fondo el grupo M_{10} y, en particular, demostraremos que no es simple. Notemos que tiene orden $|M_{10}| = 6!$, igual que Σ_6 y que $\mathrm{LGP}(2,9)$. Vamos a probar que estos tres grupos no son isomorfos, pero están muy relacionados.

Sea k el cuerpo de 9 elementos y sea $k_0 = \{0, 1, -1\}$ el cuerpo de 3 elementos. Puesto que k^* es cíclico de orden 8, contiene un elemento i de orden 4, que cumplirá $i^2 = -1$, y es claro entonces que cada elemento de k se expresa de forma única como $a + bi$, con $a, b \in k_0$. Observemos también que los cuadrados de k^* forman el subgrupo $k^{*2} = \{\pm 1, \pm i\}$. El cuerpo k tiene un único automorfismo no trivial σ, de orden 2, que fija a los elementos de k_0 y que viene dado por $\sigma(a + bi) = a - bi$.

Sea $P = P(k^2)$ la recta proyectiva sobre k, de modo que $G = \mathrm{LGP}(2,9)$ es el grupo de las homografías de P, que es un subgrupo del grupo $A = \mathrm{L\Gamma P}(2,9)$ formado por las semihomografías de P. Según se ve tras el teorema [G 8.27], se cumple que $G \trianglelefteq A$ y $A = [G]\langle\sigma\rangle$, donde $\sigma : P \longrightarrow P$ es ahora la semihomografía dada por $\sigma(a,b) = (\sigma(a), \sigma(b))$.

El grupo G tiene como subgrupo de índice 2 a $G^+ = \mathrm{LEP}(2,9)$, formado por las homografías determinadas por automorfismos de k^2 de determinante 1,

aunque, como dos automorfismos determinan la misma homografía si se diferencian en una homotecia lineal, de hecho G^+ está formada por las homografías determinadas por automorfismos de determinante en k^{*2}. Así

$$G/G^+ = \{G^+, G^-\},$$

donde G^- es la clase de las homografías inducidas por automorfismos de determinante en $k^* \setminus k^{*2}$. En la sección 7.2 hemos visto que $G^+ = \mathrm{LEP}(2,9) \cong A_6$.

Es claro que $G^+ \trianglelefteq A$, pues $[f]^{[\sigma]} = [f^\sigma]$ y $\det f^\sigma = \sigma(\det f)$, luego podemos considerar el cociente A/G^+, que tiene al menos dos subgrupos de orden 2, a saber, G/G^+ y S/G^+, donde $S = G^+\langle\sigma\rangle$. Por lo tanto, $A/G^+ \cong C_2 \times C_2$ y tiene un tercer subgrupo M/G^+ de orden 2, donde es claro que M puede describirse explícitamente así:

$$M = G^+ \cup \{\sigma f \mid f \in G^-\}.$$

(El elemento no trivial de M/G^+ es el producto de las clases σG^+ y G^-, luego es la clase de las semihomografías de la forma σgh, con $g \in G^+$ y $h \in G^-$, que no son sino las homografías σf con $f \in G^-$.)

Así pues, A tiene tres subgrupos de índice 2 (luego de orden 6!), a saber, G, S y M. Vamos a probar que $S \cong \Sigma_6$ y $M \cong M_{10}$.

De momento observemos que G, S y M tienen un único subgrupo de índice 2, pues ya sabemos que tienen uno isomorfo a A_6 y, si tuvieran otro N, el producto A_6N sería todo el grupo, luego $|A_6 \cap N| = 360 \cdot 360/720 = 180$, luego sería un subgrupo normal propio en A_6, lo cual es imposible.

Similarmente, A contiene un único subgrupo de índice 4, pues, si tuviera otro H, el producto A_6H tendría orden 1 440 o bien 720, y la intersección $A_6 \cap H$ sería un subgrupo de A_6 de índice 2 o 4, lo que contradice a 2.29.

En el enunciado del teorema siguiente incluimos el hecho de que $M \cong M_{10}$, que demostraremos más adelante:

Teorema 7.41 *Sea $A = \mathrm{L\Gamma P}(2,9)$ el grupo de las semihomografías de la recta proyectiva de orden 9. Entonces:*

1. *A tiene un único subgrupo de índice 4, que es normal e isomorfo a A_6.*
2. *A tiene exactamente tres subgrupos de índice 2 que contienen a A_6, que no son isomorfos entre sí. Uno es isomorfo a Σ_6, otro a $\mathrm{LGP}(2,9)$ y el tercero al grupo de Mathieu M_{10}.*
3. *El homomorfismo $A \longrightarrow \mathrm{Aut}(A_6)$ que a cada elemento de A le asigna el automorfismo que induce por conjugación es un isomorfismo.*

Demostración: Ya hemos probado 1), así como que $A/A_6 \cong C_2 \times C_2$, luego hay únicamente tres subgrupos intermedios entre A_6 y A, que son los grupos G, S, M de orden 720 que hemos descrito. Vamos a probar que G, Σ_6 y M no son isomorfos entre sí. Luego veremos que $S \cong \Sigma_6$.

Que G no es isomorfo a Σ_6 es inmediato, pues si $\lambda \in k^*$ tiene orden 8, la homografía determinada por la matriz

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$$

tiene orden 8 en G, mientras que es claro que Σ_6 no tiene elementos de orden 8. Por otro lado, un hipotético isomorfismo entre M y G o Σ_6 haría corresponder sus únicos subgrupos isomorfos a A_6, pero vamos a probar que M no tiene elementos de orden 2 fuera de su subgrupo A_6, mientras que G y Σ_6 sí que tienen, por lo que no pueden ser isomorfos.

Obviamente las transposiciones son elementos de orden 2 en Σ_6 que no están en A_6. Similarmente, un elemento de orden 2 en $G \setminus \mathrm{LEP}(2,9)$ es la homografía f determinada por la matriz

$$\begin{pmatrix} 1+i & i \\ i & -1-i \end{pmatrix}.$$

Su determinante es $1 + i \notin k^{*2}$, por lo que no está en $\mathrm{LEP}(2,9)$, y un simple cálculo muestra que tiene orden 2.

Supongamos ahora que $f \in M \setminus \mathrm{LEP}(2,9)$ tiene orden 2. Entonces existe un $a \in P$ tal que $f(a) = b \neq a$. Es fácil ver que $\mathrm{LEP}(2,9)$ es 2-transitivo en P (siempre podemos tomar una matriz 2×2 que transforme dos vectores dados en otros dos y, multiplicando una de sus filas por el número adecuado, podemos hacer que su determinante sea 1 sin alterar la homografía que induce). Por lo tanto, podemos tomar $g \in \mathrm{LEP}(2,\ 9)$ tal que $g(a) = 0$ y $g(b) = \infty$. Así $f^g \in M \setminus \mathrm{LEP}(2,9)$ tiene también orden 2 y cumple

$$f^g(0) = g(f(g^{-1}(0))) = g(f(a)) = g(b) = \infty.$$

Por lo tanto, no perdemos generalidad si suponemos que $f(0) = \infty$, luego $f(\infty) = 0$. Esto se traduce en que la matriz de f es de la forma

$$\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix},$$

donde el determinante $-bc$ no es un cuadrado, luego tampoco lo son bc o b/c. Por definición de M, tenemos que f es una antihomografía, es decir, que

$$f(x,y) = (c\sigma(y), b\sigma(x)), \qquad f^2(x,y) = (c\sigma(b)x, b\sigma(c)y).$$

Como $f^2 = 1$, tiene que ser $c\sigma(b) = b\sigma(c)$, luego $\sigma(b/c) = b/c$, luego $b/c \in k_0$ es un cuadrado, y tenemos una contradicción.

Ahora observamos que los homomorfismos $G, M \longrightarrow \mathrm{Aut}(A_6)$ son inyectivos. Ciertamente, sus restricciones a $A_6 \longrightarrow \mathrm{Aut}(A_6)$ tienen que serlo, pues A_6 es simple no abeliano. Por lo tanto, los núcleos tienen que tener intersección trivial con A_6, luego, si no son triviales, tienen que tener orden 2. Esto ya descarta el

caso de M, pues hemos probado que no tiene elementos de orden 2 fuera de A_6. Supongamos que $z \in G\setminus G^+$ tiene orden 2 y está en el núcleo del homomorfismo, es decir, que conmuta con todos los elementos de G^+. Pongamos que z está determinado por el automorfismo de matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Entonces tiene que cumplirse que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \lambda \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

lo cual equivale a

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \lambda \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

En particular $c = \lambda c$, luego si $c \neq 0$, tiene que ser $\lambda = 1$, y entonces $a = a + c$ implica $c = 0$, con lo que tenemos una contradicción, luego $c = 0$, pero entonces $d \neq 0$ (pues la matriz dada no puede tener determinante nulo), y de nuevo $d = \lambda d$ nos da que $\lambda = 1$ y de $a + b = b + d$ resulta que $a = d$, pero entonces el determinante de la matriz dada es a^2, y corresponde a un elemento de G^+, en contra de lo requerido.

Ahora vamos a probar 3) sin suponer que A es concretamente $\mathrm{L\Gamma P}(2, 9)$, sino usando únicamente que es un grupo con un subgrupo normal de índice 4 isomorfo a A_6 que tiene dos subgrupos intermedios isomorfos a G y M. Consideramos el homomorfismo $A \longrightarrow \mathrm{Aut}(A_6)$, cuyo núcleo tiene que tener intersección trivial con G, luego, si no es trivial, tiene orden 2. Pongamos que es $N = \langle z\rangle$, donde z conmuta con todos los elementos de A_6. Puesto que las restricciones del homomorfismo a G y M son inyectivas, tiene que ser $z \notin G$ y $z \notin M$.

Si $f \in G \setminus A_6$, el cociente A/A_6 está formado por las clases A_6, fA_6, zA_6 y zfA_6, donde $G = A_6 \cup fA_6$ y $M = A_6 \cup zfA_6$. Esto se traduce en que G y M tienen la misma imagen en $\mathrm{Aut}(A_6)$, pues, si $a \in A_6$, la conjugación por fa es la misma en A_6 que la conjugación por zfa. Pero esto es imposible, porque G y M son isomorfos a sus imágenes, luego serían isomorfos entre sí, cuando hemos probado que no lo son.

Así pues, el homomorfismo $A \longrightarrow \mathrm{Aut}(A_6)$ es un monomorfismo, pero ambos grupos tienen orden 1 440 (por 2.34 y 2.37), luego se trata de un isomorfismo.

Finalmente, el grupo $\mathrm{Aut}(A_6) \cong \mathrm{Aut}(\Sigma_6)$ contiene un subgrupo isomorfo a Σ_6, luego lo mismo vale para A, pero hemos probado que sus únicos subgrupos de orden 6! son G, S y M, así como que G y M no son isomorfos a Σ_6, luego tiene que ser $S \cong \Sigma_6$.

Con esto hemos probado el enunciado con M en lugar de M_{10}. Cuando hayamos probado que $M \cong M_{10}$ (teorema 7.42) quedará probado el teorema tal y como lo hemos enunciado. ∎

Observemos ahora que M es estrictamente triplemente transitivo sobre la recta proyectiva P. En efecto, tres puntos cualesquiera de P forman un sistema de referencia proyectivo, luego, si $P_1, P_2, P_3 \in P$ son distintos dos a dos, existe un único $f \in G$ tal que

$$f(1,0) = P_1, \qquad f(0,1) = P_2, \qquad f(1,1) = P_3,$$

pero σ fija a los tres puntos $(1,0), (0,1), (1,1)$, luego también

$$(\sigma f)(1,0) = P_1, \qquad (\sigma f)(0,1) = P_2, \qquad (\sigma f)(1,1) = P_3,$$

y esto hace que, tanto si $f \in G^+$ como si $f \in G^-$, existe un $g \in M$ (ya sea f o bien σf) tal que

$$g(1,0) = P_1, \qquad g(0,1) = P_2, \qquad g(1,1) = P_3.$$

Esto implica que M es triplemente transitivo (al igual que G) y, teniendo en cuenta su orden, el teorema 7.3 implica que la transitividad es estricta.

La relación con el grupo de Mathieu M_{10} se basa en que, llamando $a = (a,1)$ e $\infty = (0,1)$, podemos ver la recta P como $P = k \cup \{\infty\}$, es decir, como una recta afín completada con un punto infinito y, más aún, el isomorfismo de k_0-espacios vectoriales $k \cong k_0^2$ nos permite ver la recta afín k sobre el cuerpo de 9 elementos como un plano afín sobre el cuerpo k_0 de 3 elementos. Explícitamente, podemos identificar cada $\alpha = a + bi \in k$ con el par $(a,b) \in k_0^2$. Así, una recta de k vista como plano afín de orden 3 es la formada por los puntos $L_0 = \{-1, 0, 1\}$ (que se corresponden con los pares $(-1,0), (0,0), (1,0)$). Llamemos $B_0 = L_0 \cup \{\infty\}$ y sea

$$\mathcal{B} = \{f[B_0] \mid f \in G\} = \{f[B_0] \mid f \in M\}.$$

La segunda igualdad se debe a que σ fija a los elementos de B_0.

A continuación observamos que podemos identificar el grupo $\mathrm{LGP}(2,3)$ con el subgrupo de G (de orden 24) formado por las homografías que admiten una matriz con coeficientes en k_0. Notemos que el determinante de una matriz de esta forma tiene que ser ± 1, luego es un cuadrado en k^*, por lo que

$$\mathrm{LGP}(2,3) \leq G^+ \leq G \cap M.$$

Vamos a ver que

$$\mathrm{LGP}(2,3) = \{f \in G \mid f[B_0] = B_0\} = \{f \in M \mid f[B_0] = B_0\}.$$

En efecto, B_0 está formado por todos los puntos de P que admiten coordenadas en k_0, y puede identificarse con una recta proyectiva sobre k_0. Es claro entonces que los elementos de $\mathrm{LGP}(2,3)$ permutan los elementos de B_0, lo que nos da una inclusión. Por otro lado, si $f \in G$ (o $f \in M$) cumple $f[B_0] = B_0$, tendremos que $f(1,0)$, $f(0,1)$, $f(1,1)$ serán tres puntos de B_0, pero $(1,0), (0,1), (1,1)$ forman un sistema de referencia proyectivo de la recta de orden 3, luego existe $g \in \mathrm{LGP}(2,3)$ que cumple $g(1,0) = f(1,0)$, $g(0,1) = f(0,1)$, $g(1,1) = f(1,1)$, pero la transitividad estricta de G o M implica entonces que $f = g \in \mathrm{LGP}(2,3)$.

El conjunto $\mathcal{B}$ es la órbita de B_0 respecto de la acción de G (o de M) sobre el conjunto de los subconjuntos de 4 elementos de P, luego consta de $|\mathcal{B}| = 720/24 = 30$ bloques. La transitividad triple de G (o M) implica que cada subconjunto de L con 3 elementos está contenido en un elemento de $\mathcal{B}$. Veamos que es único.

Para ello observamos que si un subconjunto de P de 3 elementos está contenido en λ elementos de $\mathcal{B}$, entonces cada subconjunto de P de 3 elementos está contenido en el mismo número λ de elementos de $\mathcal{B}$, pues un elemento de G (o M) que transforme un conjunto en otro (que existe por la transitividad triple) transforma los bloques de $\mathcal{B}$ que contienen a uno en los bloques que contienen al otro. Por lo tanto, $(P, \mathcal{B})$ es un sistema de Steiner generalizado de tipo $S_\lambda(3, 4, 10)$ y, como hay 30 bloques, el teorema 7.19 implica que $\lambda = 1$.

Por la unicidad de los sistemas de Steiner de este tipo, podemos identificar $W_{10} = (P, \mathcal{B})$, y ahora es claro que tanto G como M son subgrupos de índice 2 en el grupo de automorfismos $\mathrm{Aut}(W_{10})$, al igual que M_{10}.

Los elementos de G que fijan a ∞ son los determinados por matrices de la forma

$$\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}$$

que podemos expresar en la forma $f(x) = ax + b$, y el determinante es $a \in k^*$. En términos de k_0, podemos expresar $a = u + vi$, $b = p + qi$, con lo que

$$f(x, y) = (u + vi)(x + yi) + (p + qi) = (ux - vy + p, vx + uy + q)$$
$$= (p, q) + (x, y)\begin{pmatrix} u & v \\ -v & u \end{pmatrix}.$$

Es claro entonces que las imágenes de la recta L_0 por los elementos de G (o de M) que fijan a ∞ son rectas del plano afín k_0^2, y tiene que haber 12 (porque en W_{10} hay 12 bloques con un mismo punto ∞), luego son todas las rectas del plano afín. En otras palabras, hemos demostrado que la estructura de espacio afín en k determinada por el sistema derivado $(W_{10})_\infty$ es precisamente la estructura natural que estamos considerando a través de la identificación $k \cong k_0^2$.

El grupo $\mathrm{Aut}(W_{10})$ tiene orden 1 440 y ahora sabemos que contiene dos subgrupos isomorfos a G y a M (que a su vez contienen un subgrupo común isomorfo a A_6). En la prueba del teorema 7.41 hemos visto que esto basta para concluir que el homomorfismo $\mathrm{Aut}(W_{10}) \longrightarrow \mathrm{Aut}(A_6)$ determinado por la conjugación es un isomorfismo. Por lo tanto, podemos concluir que $\mathrm{Aut}(W_{10})$ contiene exactamente tres subgrupos de orden 6!, que son M, G y otro S isomorfo a Σ_6. Uno de los tres tiene que ser M_{10}, y vamos a probar que es concretamente M.

Fijemos un elemento en concreto $f \in G \setminus G^+$, por ejemplo, el que fija a ∞ y, sobre los puntos finitos, viene dado por $f(x) = (1 + i)x$, que tiene determinante $1 + i \notin k^{*2}$. Entonces, un elemento de $M \setminus G^+$ es σf, y un elemento de $S \setminus G^+$ es σf^2 o, como $f^2 \in G^*$, también σ. Así pues:

$$G = A_6\langle f\rangle, \qquad M = A_6\langle \sigma f\rangle, \qquad S = A_6\langle \sigma\rangle.$$

Para determinar cuál de los tres es M empezamos calculando explícitamente un bloque de W_{10} que no contenga a ∞. Consideramos para ello la homografía determinada por la matriz

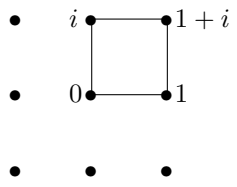
$$\begin{pmatrix} 1 & -i \\ 0 & 1+i \end{pmatrix}$$

Un simple cálculo muestra que la imagen de B_0 por esta homografía consta de los puntos

$$Q = \{(0,1),(1,1),(i,1),(1+i,1)\} = \{0,1,i,1+i\} = \{(0,0),(1,0),(0,1),(1,1)\},$$

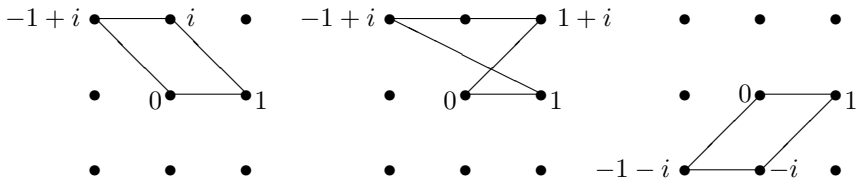
donde la primera representación corresponde a las coordenadas homogéneas en la recta proyectiva P, la segunda a la coordenada afín en dicha recta y la tercera a las coordenadas en el plano afín k_0^2.

Por lo tanto, uno de los bloques de $\mathcal{B}$ es el cuadrilátero que muestra la figura, cuyos pares de rectas paralelas están en las clases Π_1 y Π_2, si entendemos que Π_1 corresponde a las rectas horizontales y Π_2 a las verticales. Por lo tanto, los bloques que no contienen a ∞ forman la clase $\mathcal{Q}_1$ de cuadriláteros de tipo $\{\Pi_1,\Pi_2\}$ o $\{\Pi_3,\Pi_4\}$.



Ahora recordamos que $(M_{10})_\infty = M_9$ es el subgrupo formado por los automorfismos que, restringidos al plano afín k, fijan las tres clases $\mathcal{Q}_i$ de cuadriláteros. Por lo tanto, si comprobamos que f y σ no fijan las tres clases, habremos probado que ni G ni S son M_{10}, y tendrá que ser $M_{10} = M$.

Tomamos para ello un cuadrilátero de la clase $\{\Pi_1,\Pi_3\},\{\Pi_2,\Pi_4\}$ y calculamos su imagen por f y por σ:



Vemos que las dos imágenes son cuadriláteros con lados en las clases Π_1 y Π_4, con lo que corresponden a la clase $\{\Pi_1,\Pi_4\},\{P_2,\Pi_3\}$, lo que prueba que si G si S son M_{10}. El lector puede comprobar que los elementos de M_∞ sí que conservan las tres clases, aunque no es necesario, ya que por exclusión podemos concluir que M_{10} tiene que ser M. El teorema siguiente recoge lo que hemos obtenido:

Teorema 7.42 *El grupo de Mathieu M_{10} es isomorfo al subgrupo de* $\mathrm{L\Gamma P}(2,9)$ *dado por*

$$M_{10} = \mathrm{LEP}(2,9) \cup \sigma(\mathrm{LGP}(2,9) \setminus \mathrm{LEP}(2,9)),$$

donde σ es la semihomografía de la recta proyectiva de orden 9 determinada por la matriz identidad y el automorfismo no trivial del cuerpo de nueve elementos.

Además el grupo $\mathrm{Aut}(W_{10}) \cong \mathrm{L\Gamma P}(2,9) \cong \mathrm{Aut}(A_6)$ *contiene al subgrupo* $\mathrm{LEP}(2,9) \cong A_6$ *y a tres subgrupos intermedios de orden* 720 *no isomorfos entre sí, que son* M_{10}, $\mathrm{LGP}(2,9)$ *y* $\Sigma_6 = A_6\langle\sigma\rangle$.

En particular vemos que M_{10} no es simple, aunque contiene un subgrupo simple de índice 2. Ahora demostramos un hecho que teníamos pendiente:

Teorema 7.43 $\mathrm{LEP}(4,2) \cong A_8$.

Demostración: Sea B un bloque de W_{24} y sea $H \leq M_{24}$ el estabilizador de B como conjunto. Observemos que M_{24} actúa transitivamente sobre los 759 bloques de W_{24}, pues, dados dos bloques B y B', existe $f \in M_{24}$ que transforma 5 puntos de B en 5 puntos de B', pero si $f[B]$ y B' tienen 5 puntos en común, entonces $f[B] = B'$, por definición de sistema de Steiner. Por lo tanto, $|H| = |M_{24}|/759 = 322\,560$.

Tenemos una acción $H \longrightarrow \Sigma_B \cong \Sigma_8$. Vamos a probar que su imagen es A_8, para lo cual basta probar que la imagen contiene a todos los ciclos de longitud 3, pero no contiene transposiciones. Para ello fijamos tres elementos $a, b, c \in B$ y vamos a probar que la imagen de H contiene el ciclo (a,b,c), pero no la transposición (a,b). Sean $\infty_1, \infty_2, \infty_3$ otros tres puntos del bloque B, de modo que $P = (W_{24})_{\infty_1,\infty_2,\infty_3}$ es un plano proyectivo de orden 4 y $B = L \cup \{\infty_1, \infty_2, \infty_3\}$, donde L es una recta de P. Un elemento $f \in M_{24}$ que induzca el ciclo (a,b,c) o la transposición (a,b) está en $M_{21} = \mathrm{LEP}(3,4)$ y fija al menos dos puntos de la recta L, luego fija a L como conjunto.

Podemos considerar $f|_L : L \longrightarrow L$, que es una homografía de la recta L, luego está determinada por la imagen de tres puntos cualesquiera. Esto significa que $f|_L$ no puede ser (a,b), porque entonces fijaría a tres puntos, y tendría que ser la identidad.

Por el contrario, sí que existe una homografía $g : L \longrightarrow L$ que permuta cíclicamente a, b, c. Si los otros dos puntos de la recta son d, e, tiene que ser $g = (a,b,c)$ o bien $g = (a,b,c)(d,e)$, pero el segundo caso es imposible, ya que entonces $g^3 = (d,e)$, pero ya hemos observado que una homografía no puede ser una transposición. Ahora basta observar que toda homografía g se extiende a una homografía $g \in \mathrm{LEP}(3,4)$. En efecto, si $L = P(V)$, para cierto subespacio $V \leq k^3$, tenemos que g está determinada por un automorfismo $\tilde{g} : V \longrightarrow V$, que podemos extenderlo a un automorfismo $\tilde{f} : k^3 \longrightarrow k^3$ de determinante 1, el cual determina $f \in \mathrm{LEP}(3,4)$ que extiende a g. A su vez, $f \in M_{21}$ se extiende a $f \in M_{24}$ que fija a los puntos ∞_i, luego $f \in H$ e induce el ciclo (a,b,c).

Así pues, tenemos un epimorfismo $H \longrightarrow A_8$. Sea V su núcleo, de modo que V es el subgrupo de los elementos de H que fijan a todos los elementos de B. Así $H/V \cong A_8$. Observemos que $|V| = |H|/|A_8| = 16$.

Cada $f \in H$ se restringe a una homografía $f \in \mathrm{LEP}(3,4)$ que fija a todos los puntos de la recta L. Vamos a probar que si una homografía del plano fija a todos los puntos de una recta, tiene orden 2 (o es la identidad). No perdemos generalidad si suponemos que la recta es $z = 0$, es decir, $L = \langle(1,0,0),(0,1,0)\rangle$,

con lo que la matriz de f en la base canónica de k^3 será de la forma

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ a & b & \lambda \end{pmatrix},$$

y es inmediato comprobar que esta matriz tiene orden 2 (si no es la identidad). Por lo tanto $V \cong C_2^4$ puede verse como un espacio vectorial de dimensión 4 sobre el cuerpo de 2 elementos, por lo que $\mathrm{Aut}(V) \cong \mathrm{LG}(4,2) = \mathrm{LEP}(4,2)$.

Ahora consideramos el homomorfismo $H \longrightarrow \mathrm{Aut}(V)$ que a cada $h \in H$ le asigna el automorfismo de V que determina por conjugación. Como V es abeliano, está en el núcleo del homomorfismo, luego en realidad tenemos un homomorfismo $A_8 \cong H/V \longrightarrow \mathrm{Aut}(V)$. Como A_8 es simple y ambos grupos tienen el mismo orden, si probamos que el homomorfismo no es trivial (es decir, que H no centraliza a V), de hecho será un isomorfismo y el teorema quedará probado. Ahora bien, es fácil ver que las matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

determinan una homografía de V y una de H (notemos que la segunda fija la recta $z = 0$ como conjunto), pero no conmutan. ∎

El grupo M_{12} no sólo contiene subgrupos isomorfos a $M_{11} = \mathrm{Aut}(W_{11})$ y M_{10}, sino que también tiene subgrupos isomorfos a $\mathrm{Aut}(W_{10}) \cong \mathrm{Aut}(\Sigma_6)$. Concretamente, mientras M_{10} es, por definición, el subgrupo formado por los automorfismos de M_{12} que fijan a dos puntos ∞_2, ∞_3, se cumple que $\mathrm{Aut}(W_{10})$ es isomorfo al subgrupo $(M_{12})_{\{\infty_2,\infty_3\}} \leq M_{12}$ formado por los automorfismos que fijan al conjunto $\{\infty_2, \infty_3\}$.

En efecto, es obvio que todo $f \in M_{12}$ que cumpla $f[\{\infty_2, \infty_3\}] = \{\infty_2, \infty_3\}$ se restringe a un automorfismo de W_{10}, pues si B es un bloque de W_{10}, entonces $B \cup \{\infty_2, \infty_3\}$ es un bloque de W_{12}, luego $f[B] \cup \{\infty_2, \infty_3\}$ también lo es, luego $f[B]$ es un bloque de W_{10}. Esto prueba que la restricción determina un homomorfismo de grupos $(M_{12})_{\{\infty_2,\infty_3\}} \longrightarrow \mathrm{Aut}(W_{10})$.

Se trata de un monomorfismo, porque si dos elementos $f, g \in M_{12}$ coinciden en $W_{12} \setminus \{\infty_2, \infty_3\}$, entonces fg^{-1} fija a todos los elementos de W_{12} salvo a lo sumo ∞_2, ∞_3, luego restringiendo a W_{10} menos tres de los puntos fijados, obtenemos una biyección afín del plano afín de orden 3 que fija a todos los puntos salvo a lo sumo a dos de ellos, pero entonces fija a un sistema de referencia afín y, por lo tanto es la identidad.

Ahora basta probar que ambos grupos tienen el mismo número de elementos, es decir, que el primero tiene orden 1 440. Para ello observamos que M_{12} actúa transitivamente sobre los $12 \cdot 11/2 = 66$ subconjuntos de W_{12} de dos elementos, luego el estabilizador de uno de ellos tiene orden $95\,040/66 = 1\,440$.

El grupo M_9 Tenemos dos descripciones alternativas del grupo de Mathiew M_9, pero ninguna de ellas es especialmente manejable. Una es la que define M_9

como el estabilizador de un punto en M_{10}, pero también hemos visto que M_9 puede verse como el subgrupo de $\mathrm{Aut}(W_9)$ formado por las biyecciones afines que dejan invariantes las tres clases de paralelogramos Ω_i definidas en 7.24. Vamos a calcular su estructura.

En primer lugar observamos que $M_9 \trianglelefteq \mathrm{Aut}(W_9)$ (pues si una biyección afín fija las tres clases Ω_i sus conjugadas también lo hacen).

Tras la definición [G 5.1] vimos que el grupo $\mathrm{Aut}(W_9)$ de las biyecciones afines del plano afín sobre el cuerpo de 3 elementos contiene como subgrupo normal al grupo de las traslaciones, que es isomorfo al grupo aditivo del espacio vectorial $\vec{E}$ asociado al espacio afín, luego en este caso es $C_3 \times C_3$, y por otro lado $\mathrm{Aut}(W_9)$ contiene al subgrupo de las biyecciones afines que fijan a un punto O, que es isomorfo a $\mathrm{LG}(\vec{E})$ o, en nuestro caso, a $\mathrm{LG}(2,3)$ y el grupo de automorfismos es el producto semidirecto de ambos:

$$\mathrm{Aut}(W_9) = \mathrm{LG}(2,3)[C_3 \times C_3],$$

con la acción natural de $\mathrm{LG}(2,3)$ sobre $C_3 \times C_3$ visto como espacio vectorial sobre el cuerpo de tres elementos. Recordemos que $|\mathrm{LG}(2,3)| = 2^4 \cdot 3$.

Un subgrupo de índice 2 en $\mathrm{Aut}(W_9)$ es $N = \mathrm{LE}(2,3)[C_3 \times C_3]$, y sucede que es el único, pues si N^* fuera otro, no puede ser que $\mathrm{LE}(2,3) \leq N^*$, pues entonces $2^4 \mid |N^*|$, luego $N^*\mathrm{LE}(2,3) = \mathrm{Aut}(W_9)$, y esto implica que $|N^* \cap \mathrm{LE}(2,3)| = 12$, pero en la sección 3.7 hemos visto que $\mathrm{LE}(2,3)$ no tiene subgrupos de orden 12.

Ahora, el cociente $\mathrm{Aut}(W_9)/M_9$ tiene orden 6, luego tiene que contener un subgrupo de orden 3, luego $M_9 \trianglelefteq \mathrm{LE}(2,3)[C_3 \times C_3] \leq \mathrm{Aut}(W_9)$.

Los nueve estabilizadores de M_9 en su acción sobre W_9 tienen índice 9, luego tienen orden 8, luego son sus 2-subgrupos de Sylow. Todos ellos son 2-subgrupos de Sylow de $\mathrm{LE}(2,3)[C_3 \times C_3]$ y, como M_9 es normal, todo 2-subgrupo de Sylow de $\mathrm{LE}(2,3)[C_3 \times C_3]$ está de hecho en M_9, es decir, ambos grupos tienen los mismos subgrupos de Sylow, que son conjugados con el único 2-subgrupo de Sylow de $\mathrm{LE}(2,3)$, que según vimos en la sección 3.7 es isomorfo a Q_8.

Así pues M_9 tiene 9 subgrupos conjugados isomorfos a Q_8 y, por otra parte, como las traslaciones transforman una recta en otra paralela, es obvio que fijan las tres clases Ω_i, luego $C_3 \times C_3 \leq M_9$. Concluimos así que

$$M_9 = Q_8[C_3 \times C_3],$$

donde la acción es la que resulta de considerar $Q_8 \leq \mathrm{LE}(2,3)$.

De este modo, continuando la relación en virtud de la cual M_n es el estabilizador de un punto en M_{n+1}, podemos considerar que el grupo de Mathieu de orden 8 es $M_8 = Q_8$.

Inmersión de M_{12} en M_{24} En principio no tenemos ninguna conexión entre los grupos de Mathieu pequeños y los grandes, pero vamos a demostrar que M_{24} contiene subgrupos isomorfos a M_{12}, con lo que contiene de hecho subgrupos

isomorfos a todos los grupos de Mathieu. Para ello empezamos demostrando un hecho general sobre sistemas de Steiner que tiene interés en sí mismo.

Si $(X, \mathcal{B})$ es cualquier sistema de Steiner de tipo $S(l, m, n)$ y $0 \leq s \leq l$, el número de bloques b_s que contienen a un conjunto dado $S \subset X$ con $|S| = s$ viene dado por el teorema 7.19, mientras que si $l \leq s \leq m$, es obviamente $b_s = 1$, pues si S estuviera contenido en dos bloques, cualquier subconjunto de S con l elementos estaría también contenido en ellos, en contra de la definición de sistema de Steiner (con $\lambda = 1$). Naturalmente, para $s > m$ sería $b_s = 0$.

Más en general, para $s + t \leq m$, podemos definir $b_{s,t}$ como el número de bloques que contienen a un determinado conjunto S con $|S| = s$ y son disjuntos de otro conjunto T con $|T| = t$ y $S \cap T = \varnothing$. No es inmediato que $b_{s,t}$ sólo dependa del cardinal de S y de T y no de los conjuntos concretos, pero en realidad es consecuencia de que así sucede con $b_s = b_{s,0}$, como hemos probado en el teorema 7.19. En efecto, basta considerar el triángulo siguiente:

$$\begin{array}{ccccccccc}
 & & & & b_{0,0} & & & & \\
 & & & b_{1,0} & & b_{0,1} & & & \\
 & & b_{2,0} & & b_{1,1} & & b_{0,2} & & \\
 & b_{3,0} & & b_{2,1} & & b_{1,2} & & b_{0,3} & \\
b_{4,0} & & b_{3,1} & & b_{2,2} & & b_{1,3} & & b_{0,4} \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{array}$$

Sabemos que los valores $b_{s,0}$ están bien definidos y, suponiendo que están bien definidos $b_{s,t}$ y $b_{s+1,t}$, entonces también está bien definido

$$b_{s,t+1} = b_{s,t} - b_{s+1,t}.$$

En efecto, si S y T son conjuntos disjuntos de cardinales s y $t+1$ y $a \in T$ (con lo que $a \notin S$), sabemos que hay $b_{s,t}$ bloques que contienen a S y son disjuntos de $T \setminus \{a\}$. Si B es uno de ellos, hay dos posibilidades: o bien $a \in B$, o bien $a \notin B$. En el primer caso se trata de un bloque que contiene a $S \cup \{a\}$ y es disjunto de $T \setminus \{a\}$, luego el número de bloques en este caso es $b_{s+1,t}$. Por lo tanto, el número de bloques en el segundo caso es $b_{s,t} - b_{s+1,t}$, y éstos son precisamente los bloques que contienen a S y son disjuntos de T, luego el número $b_{s,t+1} = b_{s,t} - b_{s+1,t}$ no depende de los conjuntos S y T considerados, sino únicamente de sus cardinales s y $t+1$.

De este modo, el hecho de que los números $b_{s,0}$ estén bien definidos implica que lo están todos los números $b_{s,1}$, y a su vez esto implica que están bien definidos todos los números $b_{s,2}$, etc.

Gráficamente, en el triángulo anterior, cada número es la suma de los dos que tiene por debajo (aunque para calcularlos usamos que cada uno es la diferencia del que tiene arriba a la izquierda menos el que tiene a la izquierda).

Por ejemplo, para un sistema de tipo $S(5, 6, 12)$, el teorema 7.19 y la observación que hemos hecho para el caso $l \leq s \leq m$ nos da los valores

$$b_{0,0} = 132, \quad b_{1,0} = 66, \quad b_{2,0} = 30, \quad b_{3,0} = 12, \quad b_{4,0} = 4, \quad b_{5,0} = 1, \quad b_{6,0} = 1.$$

A partir de ellos podemos calcular el triángulo:

					132							
				66		66						
			30		36		30					
		12		18		18		12				
	4		8		10		8		4			
1		3		5		5		3		1		
1	0		3		2		3		0		1	
c_6	c_5		c_4		c_3		c_2		c_1		c_0	

Su fila m-sima es especialmente interesante. Contiene los números

$$c_s = b_{s,m-s},$$

que, dado un bloque B y un subconjunto $S \subset B$ con $|S| = s$, nos dan el número c_s de bloques C tales que $B \cap C = S$.

En efecto, c_s es, en principio, el número de bloques C que contienen a S y son disjuntos de $B \setminus S$, pero esto equivale a que $B \cap C = S$.

Por ejemplo, hemos calculado $c_0 = 1$, y esto significa que, en un sistema de tipo $S(5, 6, 12)$, el número de bloques que cortan a un bloque dado en el conjunto vacío es 1 o, lo que es lo mismo, (teniendo en cuenta que hay 12 puntos y que los bloques tienen 6 puntos), que el complementario de un bloque es necesariamente un bloque, cosa que ya habíamos observado más arriba.

Para un sistema de tipo $S(5, 8, 24)$ el triángulo de intersecciones es

							759									
						253		506								
					77		176		330							
				21		56		120		210						
			5		16		40		80		130					
		1		4		12		28		52		78				
	1		0		4		8		20		32		46			
1		0		0		4		4		16		16		30		
1	0		0		0		4		0		16		0		30	
c_8	c_7		c_6		c_5		c_4		c_3		c_2		c_1		c_0	

De aquí se desprende que la intersección de dos bloques distintos de W_{24} tiene $0, 2, 4$ elementos. También vemos que $b_5 = b_{5,0} = 5$, lo que significa que cada conjunto de 4 puntos está contenido en 5 bloques.

La *diferencia simétrica* de dos conjuntos se define como[2]

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

[2]Podemos identificar los subconjuntos de un conjunto $X = \{x_1, \ldots, x_n\}$ con los elementos del espacio vectorial $V = k^n$, donde $k = \{0, 1\}$ es el cuerpo de dos elementos (cada conjunto A se representa como una sucesión $v \in V$ tal que $v_i = 1$ si y sólo si $x_i \in A$. Entonces, si $A, B \subset X$, la diferencia simétrica $A \triangle B$ se corresponde con la suma en V, de donde se sigue que la suma directa es asociativa, conmutativa, etc.

El teorema siguiente recoge algunos resultados técnicos sobre W_{24} que vamos a necesitar:

Teorema 7.44 *En el sistema de Steiner W_{24} se cumple:*

1. *Si dos bloques se cortan en cuatro puntos, su diferencia simétrica también es un bloque.*
2. *Si $A \subset W_{24}$ es un conjunto de cuatro puntos y B es un bloque disjunto de A, entonces, los cinco bloques que contienen a A están en uno de los dos casos siguientes:*
   (a) *Dos cortan a B en cuatro puntos y los otros tres son disjuntos.*
   (b) *Cuatro cortan a B en dos puntos y el quinto es disjunto.*

DEMOSTRACIÓN: Pongamos que $B_1 \cap B_2 = \{a, b, c, d\}$. El derivado $(W_{24})_{a,b,c}$ es un plano proyectivo de orden 4 que tiene entre sus rectas a $L_i = B_i \setminus \{a, b, c\}$, luego el teorema 7.38 nos da que $(L_1 \cup L_2) \setminus \{d\}$ es un bloque, que no es sino $B_1 \triangle B_2$.

Sean B_1, B_2, B_3, B_4, B_5 los bloques que contienen a A. Como dos bloques no pueden cortarse en más de 4 puntos, la intersección de dos de ellos es exactamente A. Supongamos que $|B_1 \cap B| = 4$. Entonces, por el apartado anterior, $B_2 = B_1 \triangle B$ es un bloque que contiene a A. Si existe $b \in B_3 \cap B$, entonces $b \notin A = B_1 \cap B_3$, luego $b \in B \setminus B_1 \subset B_1 \triangle B = B_2$, luego $b \in B_2 \cap B_3 = A$, contradicción. Así pues, $B_3 \cap B = \varnothing$, y lo mismo vale para B_4 y B_5.

Por el contrario, si $|B \cap B_i| \neq 4$ para todo i, tenemos que $|B \cap B_i| = 0, 2$, para todo i. Para cada $b \in B$, hay un único bloque que contiene a $A \cup \{b\}$, luego tiene que haber exactamente cuatro bloques B_1, B_2, B_3, B_4 que corten a B en dos puntos. ∎

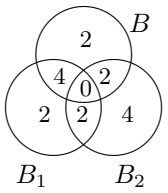
Llamaremos *dodécadas* en W_{24} a las diferencias simétricas de pares de bloques que se cortan en dos puntos. Así, toda dodécada es un conjunto de 12 puntos. Vamos a probar que el estabilizador de una dodécada en M_{24} es un subgrupo isomorfo a M_{12}.

Teorema 7.45 *Sea $D \subset W_{24}$ una dodécada y B un bloque que corte a D en al menos 5 puntos. Entonces $|B \cap D| = 6$ y existe un único bloque B^* tal que $D = B \triangle B^*$.*

DEMOSTRACIÓN: Pongamos que $D = B_1 \triangle B_2$. Distinguiendo casos según si $|B \cap B_1 \cap B_2|$ es par o impar y sabiendo que $|B \cap B_i|$ es par, es fácil ver que $|B \cap D|$ tiene que ser par, luego tiene que constar de 6 u 8 elementos. Vamos a ver que 8 es imposible, es decir, que una dodécada no puede contener un bloque. En efecto, si $B \subset D$, como $B \cap B_i$ puede tener a lo sumo cuatro elementos, tendría que ser $|B \cap B_1| = |B \cap B_2| = 4$.

Llamando $A = B \cap B_1$, tenemos que B_2 es un bloque disjunto con A, pero, por una parte, B es un bloque que contiene a A y corta a B_2 en cuatro puntos, luego deberíamos estar en el caso (a) del apartado 2) del teorema anterior. Sin embargo, por otra parte B_1 es un bloque que contiene a A y corta a B_2 en dos puntos, luego deberíamos estar en el caso (b), y tenemos una contradicción.

Tenemos, pues, que $B \cap D = 6$. Intercambiando B_1 y B_2 si es necesario, podemos suponer que $|B \cap B_1| = 4$ y $|B \cap B_2| = 2$. Por el teorema anterior $B_1 \triangle B$ es un bloque que corta a B_2 en cuatro puntos (véase la figura), y a su vez $B^* = (B_1 \triangle B) \triangle B_2$ es un bloque tal que



$$B \triangle B^* = B \triangle B_1 \triangle B \triangle B_2 = B_1 \triangle B_2 = D.$$

Además B^* es único, pues si $B \triangle B^* = B \triangle \tilde{B}$, entonces $B^* = \tilde{B}$. ∎

Teorema 7.46 *En W_{24} hay 2 576 dodécadas.*

Demostración: Una dodécada D tiene 792 subconjuntos de 5 elementos, cada uno de los cuales está contenido en un único bloque, el cual corta a D en 6 puntos. Por lo tanto, un mismo bloque se corresponde con 6 subconjuntos de D de cinco elementos, luego hay exactamente $792/6 = 132$ bloques B que cortan a D en 6 puntos. Cada uno de ellos da lugar a una única expresión $D = B \triangle B^*$, pero así estamos contando dos veces cada par (B, B^*), luego concluimos que una dodécada admite exactamente $132/2 = 66$ expresiones como diferencia simétrica de bloques.

Cada bloque B tiene 28 subconjuntos de 2 elementos y, como en el triángulo de intersecciones vemos que $c_2 = 16$, hay exactamente 16 bloques que cortan a B en cada uno de ellos, luego hay $28 \cdot 16 = 448$ bloques que cortan a B en dos puntos. Como hay 759 bloques en total, vemos que hay $759 \cdot 448$ pares ordenados de bloques que se cortan en dos puntos, o $759 \cdot 448/2 = 170\,016$ pares desordenados. Pero cada 66 pares dan lugar a la misma dodécada, luego en total hay $170\,016/66 = 2\,576$ dodécadas. ∎

Teorema 7.47 *Si $D \subset W_{24}$ es una dodécada y $\mathcal{B}_D$ es el conjunto de las intersecciones $D \cap B$, donde B es un bloque de W_{24} tal que $|D \cap B| = 6$, entonces $(D, \mathcal{B}_D)$ es un sistema de Steiner de tipo $S(5, 6, 12)$.*

Demostración: Si $A \subset D$ es un conjunto de 5 puntos, existe un único bloque B en W_{24} tal que $A \subset B$, pero entonces $|B \cap D| = 6$ por el teorema anterior, luego $A \subset \tilde{B} = B \cap D \in \mathcal{B}_D$, y $\tilde{B}$ es único, pues si hubiera otro, sería de la forma $B' \cap D$, donde B' sería un bloque distinto de B que también contendría a A, lo cual es imposible. ∎

Teorema 7.48 *Si $D \subset W_{24}$ es una dodécada, el estabilizador $(M_{24})_{\{D\}}$ de D como conjunto es un subgrupo de M_{24} isomorfo a M_{12}.*

Demostración: La restricción $(M_{24})_{\{D\}} \longrightarrow M_{12}$ es inyectiva, es decir, que si un elemento $f \in M_{24}$ fija a todos los puntos de una dodécada, es la identidad. En efecto, si $D = B_1 \triangle B_2$, al restringir f al derivado de W_{24} respecto de dos puntos $\infty_1, \infty_2 \in B_1$ y un punto $\infty_3 \in B_2$ es una homografía en el plano

proyectivo W_{21} de orden 4 que fija a cuatro puntos del hiperóvalo $B_1\setminus\{\infty_1,\infty_2\}$, que forman un sistema de referencia proyectivo, luego $f|_{W_{21}}$ es la identidad y f también.

Ahora sólo falta probar que $|(M_{24})_{\{D\}}| \geq 95\,040 = |M_{12}|$, pues entonces la restricción será un isomorfismo. Equivalentemente, hay que probar que el índice del estabilizador es $\leq 2\,776$, pero dicho índice es el cardinal de la órbita de D por la acción de M_{24} el el conjunto de las dodécadas, que obviamente será menor o igual que el número total de dodécadas, que es precisamente 2 776. Así pues, $|(M_{24})_{\{D\}}| = 95\,040 = |M_{12}|$, lo que prueba el teorema, e incidentalmente hemos probado la igualdad $|M_{24} : (M_{24})_{\{D\}}| = 2\,776$, lo que significa que M_{24} actúa transitivamente sobre el conjunto de todas las dodécadas. ∎

7.4 El código de Golay

El sistema de Steiner W_{24} está relacionado con un código de corrección de errores de gran interés. En el apéndice B de [G] mostramos el código de Hamming, que permite corregir errores a condición de que se produzca a lo sumo uno en cada paquete de 7 dígitos binarios transmitidos. Se trata de uno de los códigos más antiguos y hoy en día se conocen otros más eficientes. El código de Golay que vamos a describir aquí tiene mucho más interés práctico y, de hecho, lo ha usado la NASA en la transmisión de imágenes en varias misiones espaciales, entre ellas las misiones *Voyager* 1 y 2 a Júpiter y Saturno, así como en la sonda Magallanes a Venus.

Con la nomenclatura introducida en [G], el *código de Golay extendido* no es más que un código binario de corrección de errores de tipo $[24, 12, 8]$, es decir, un subespacio C de dimensión 12 del espacio vectorial $V = k^{24}$ (donde $k = \{0, 1\}$ es el cuerpo de 2 elementos) con la propiedad de que dos cualesquiera de sus elementos se diferencian al menos en 8 dígitos. Probaremos que sólo hay uno salvo isomorfismo.

Recordemos de [G] que podemos identificar cada $x \in V$ con un subconjuntos $A_x \subset X = \{1, \ldots, 24\}$, de modo que la suma en V se corresponde con la diferencia simétrica de conjuntos.

Teorema 7.49 *Si $\mathcal{C}$ es un código de Golay extendido, los elementos de $\mathcal{C}$ de cardinal 8 son un sistema de Steiner de tipo $S(5, 12, 24)$.*

Demostración: Fijemos un índice $i \in X$ y llamemos $\mathcal{M}$ al conjunto de todos los subconjuntos $A \subset X$ que, o bien cumplen $|A| \leq 3$ o bien $|A| = 4$ e $i \in A$. Claramente

$$|\mathcal{M}| = \binom{24}{0} + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} + \binom{23}{3} = 2^{12}.$$

Si $A, B \in \mathcal{M}$, entonces, o bien $|A| = |B| = 4$, en cuyo caso $i \in A \cap B$, luego $|A \triangle B| \leq 7$, o bien $|A| \leq 3$ o $|B| \leq 3$, en cuyo caso $|A \triangle B| \leq 7$. En cualquier

caso $A \triangle B \notin \mathcal{C}$. Esto significa que los elementos de $\mathcal{M}$ determinan clases distintas en el espacio cociente $V/\mathcal{C}$, pero éste tiene dimensión $24 - 12 = 12$, luego consta de 2^{12} clases, luego cada clase de $V/\mathcal{C}$ tiene un único representante en $\mathcal{M}$.

Sea ahora $U \subset X$ un conjunto de 5 puntos. Sea $i \in U$ uno de ellos, de modo que $B = U \setminus \{i\} \notin \mathcal{M}$. Sin embargo, acabamos de probar que existe un $A \in \mathcal{M}$ tal que $A \triangle B \in \mathcal{C}$, pero $|A \triangle \mathcal{B}| \leq 8$ y no puede ser $A \triangle B = \varnothing$, pues eso equivale a $A = B$, pero $A \in \mathcal{M}$ y $B \notin \mathcal{M}$. Por lo tanto, para estar en $\mathcal{C}$, la diferencia simétrica tiene que cumplir $|A \triangle B| = 8$, lo que requiere que $|A| = |B| = 4$, $A \cap B = \varnothing$, lo que a su vez implica que $i \in A$. Por lo tanto $U = B \cup \{i\} \in A \triangle B \in \mathcal{C}$.

Supongamos que $U \subset C_1 \cap C_2$, donde $C_1, C_2 \in \mathcal{C}$ son conjuntos de 8 elementos. Entonces $|C_1 \triangle C_2| \leq 6$, pero $C_1 \triangle C_2 \in \mathcal{C}$, luego tiene que ser $C_1 = C_2$. ∎

Recíprocamente:

Teorema 7.50 *El código $\mathcal{C} \leq V = k^{24}$ generado por los bloques de W_{24} es un código de Golay extendido formado por:*

1. $\varnothing, V$.
2. *Los* 759 *bloques de W_{24} y sus* 759 *complementos.*
3. *Las* 2 576 *dodécadas.*

Demostración: Veamos en primer lugar que $\dim \mathcal{C} \leq 12$. Para ello consideramos en V el producto escalar

$$x \cdot y = \sum_{i=1}^{24} x_i y_i,$$

de modo que, identificando dos subconjuntos $X, Y \subset W_{24}$ con elementos de V, el producto $X \cdot Y$ es $|X \cap Y|$ (mód 2). En particular, si A, B son bloques de W_{24}, hemos visto que se cortan en $0, 2$ o 4 puntos, por lo que $A \cdot B = 0$. Como los bloques generan $\mathcal{C}$, concluimos que, más en general, $x \cdot y = 0$, para todo par de vectores $x, y \in \mathcal{C}$.

Si $v_1, \ldots, v_d$ es una base de $\mathcal{C}$, tenemos que todos los elementos de $\mathcal{C}$ son soluciones del sistema de ecuaciones lineales $v_i \cdot x = 0$, que son linealmente independientes, luego $d = \dim \mathcal{C} \leq 24 - d$, luego $d \leq 12$.

El árbol de intersecciones de $S(5, 8, 24)$ que hemos calculado muestra que $b_{1,0} = 253$, es decir que cada índice está en 253 bloques, luego al sumar las palabras correspondientes a todos los bloques, como el número de palabras con la coordenada i-ésima no nula es impar, resulta que la suma es la palabra 1, correspondiente a V, luego $V \in \mathcal{C}$.

Los 259 bloques de W_{24} están en $|\mathcal{C}$ por definición y, como $V \in \mathcal{C}$, también tienen que estar sus complementarios. A su vez, las 2 576 dodécadas también tienen que estar en $\mathcal{C}$, pues son sumas de bloques. Esto nos da ya un total de

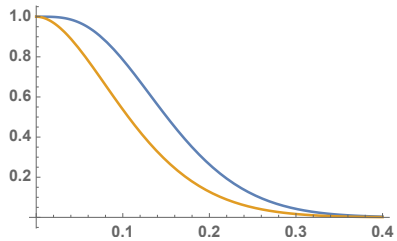
$2 + 759 \cdot 2 + 2\,576 = 2^{12}$ palabras en $\mathcal{C}$, pero tenemos que $|\mathcal{C}| \leq 2^{12}$, luego se tiene que dar la igualdad $\dim \mathcal{C} = 12$ y no puede haber más palabras en $\mathcal{C}$. Así, como todas las palabras no nulas de $\mathcal{C}$ tienen peso $8, 12, 16, 24$, podemos concluir que $\mathcal{C}$ es un código de Golay extendido. ∎

Así, si $\mathcal{C}$ es un código de Golay extendido, sus palabras de peso 8 forman un sistema de Steiner de tipo $S(5, 12, 24)$, cuyos bloques generan un código de Golay $\mathcal{C}'$ claramente contenido en $\mathcal{C}$, pero, como tienen la misma dimensión, tiene que ser $\mathcal{C}$. Así pues, todo código de Golay extendido está definido a partir de un sistema de Steiner W_{24} y, como todos ellos son isomorfos, es claro que todos los códigos de Golay extendidos son isomorfos (en el sentido de uno se transforma en otro sin más que reordenar las coordenadas).

De acuerdo con lo expuesto en el apéndice B de [G], un código de Golay asocia a cada sucesión de 12 dígitos binarios un código de 24 dígitos de modo que si se corrompe con un máximo de $e = E[(d-1)/2] = E[3.5] = 3$ errores, se puede reconstruir la sucesión de datos inicial, pues hay una única palabra del código a una distancia menor o igual que 3. Más aún, el código permite detectar la presencia de un máximo de $d - 1 = 7$ errores.

Si comparamos esto con el código de Hamming extendido que presentamos en el apéndice B de [G], éste, duplicando la longitud de la información, puede reconstruir mensajes con a lo sumo un error cada 8 dígitos transmitidos, mientras que el código de Golay permite 3 errores cada 24 dígitos. Puede parecer que es lo mismo, pero no es así, porque si transmitimos 12 dígitos de información codificados en 3 palabras del código de Hamming, con 24 dígitos en total, éste sólo permite reconstruir la información si se producen a lo sumo tres errores separados para que esté uno en cada palabra, mientras que con el código de Golay extendido necesitamos igualmente 24 dígitos, pero podemos reconstruir la información si se produce un máximo de tres errores cualquiera que sea la forma en que se distribuyan en la palabra, por lo que las probabilidades de corregir un error de hasta tres dígitos son mucho mayores.

Más precisamente, la gráfica muestra la probabilidad de que los códigos puedan corregir un mensaje de 24 dígitos (con 12 dígitos de datos) en función de la probabilidad p de que se produzca un error cada vez que se transmite un dígito. La tabla muestra algunos valores concretos:

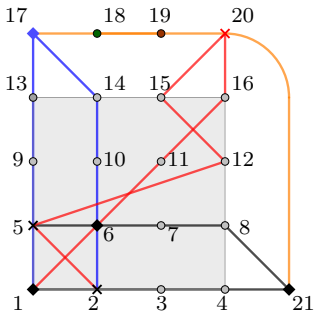


p	Hamming	Golay
5%	83.8%	97%
7%	72%	91.7%
9.5%	56.7%	81.1%
10%	53.8%	78.6%

Para valores pequeños de p las probabilidades de que un error no pueda corregirse es baja en ambos casos, pero estadísticamente la diferencia sigue siendo sustancial. Por ejemplo, imaginemos que queremos transmitir 1Mb de

información, es decir, $8 \cdot 2^6$ dígitos, que fragmentamos en bloques de 8 dígitos para aplicar el código de Hamming o en bloques de 24 para aplicar el código de Golay. Si la probabilidad de error fuera $p = 0.3\%$, sin el empleo de ningún código corrector el número esperado de dígitos corruptos sería precisamente de un 0.3%, con el código de Hamming, el número esperado de bloques de 8 dígitos con errores incorregibles sería de 249, lo que supone un máximo de 1992 dígitos corruptos, es decir, a lo sumo un 0.025%; mientras que, con el código de Golay, la esperanza es de "medio" bloque de 12 dígitos incorregible, lo que supone como máximo un 0.00008% de los dígitos.

A partir de la descripción que conocemos de W_{24} no es difícil encontrar una base del código de Golay. Por ejemplo, si numeramos los puntos del plano proyectivo de orden 4 como muestra la figura, el plano de Fano señalado, es decir, el formado por los puntos



$$(0,0,1),(1,0,1),(1,0,0),(0,1,1),$$

$$(1,1,1),(0,1,0),(1,1,0),$$

se corresponde con la palabra

$$1100\,1100\,0000\,0000\,10011\,100,$$

si convenimos en que los tres últimos dígitos corresponden a $\infty_1, \infty_2, \infty_3$ y consideramos que el plano pertenece a la clase $\mathcal{F}_1$. Si le aplicamos la homografía de matriz

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

que no está en $\mathrm{LEP}(3,4)$, obtendremos un plano de Fano de otra clase, que podemos tomar como $\mathcal{F}_2$, y que resulta ser

$$(0,0,1),(\alpha,0,1),(\alpha,0,0),(0,1,1),(\alpha,1,1),(0,1,0),(\alpha,1,0),$$

y si a éste le aplicamos la misma homografía (que tiene orden 3) obtenemos un plano de $\mathcal{F}_3$:

$$(0,0,1),(\alpha^2,0,1),(\alpha^2,0,0),(0,1,1),(\alpha^2,1,1),(0,1,0),(\alpha^2,1,0),$$

con los que tenemos las palabras linealmente independientes

$$\begin{array}{c} 1100\ 1100\ 0000\ 0000\ 10011\ 100 \\ 1010\ 1010\ 0000\ 0000\ 11001\ 010 \\ 1001\ 1001\ 0000\ 0000\ 10101\ 001 \end{array}$$

A partir de aquí podemos buscar 9 palabras más que no contengan puntos infinitos, es decir, que sean diferencias simétricas de pares de rectas en el plano

proyectivo. Por ejemplo, si consideramos los pares formados por cada una de las 5 rectas que pasan por el punto 1 y la recta infinita (véase la figura de la página 262) obtenemos:

1100 1100 0000 0000 10011 100
1010 1010 0000 0000 11001 010
1001 1001 0000 0000 10101 001
1000 1000 1000 1000 01111 000
1000 0010 0001 0100 10111 000
1000 0001 0100 0010 11011 000
1000 0100 0010 0001 11101 000
1111 0000 0000 0000 11110 000

y las 8 palabras resultan ser linealmente independientes. Para completar una base de 12 palabras, con un poco de tanteo y un ordenador que compruebe los rangos de las matrices, vemos que nos basta considerar dos pares de rectas horizontales y dos pares de rectas verticales:

1100 1100 0000 0000 10011 100
1010 1010 0000 0000 11001 010
1001 1001 0000 0000 10101 001
1000 1000 1000 1000 01111 000
1000 0010 0001 0100 10111 000
1000 0001 0100 0010 11011 000
1000 0100 0010 0001 11101 000
1111 0000 0000 0000 11110 000
1111 1111 0000 0000 00000 000
1111 0000 1111 0000 00000 000
1100 1100 1100 1100 00000 000
1010 1010 1010 1010 00000 000

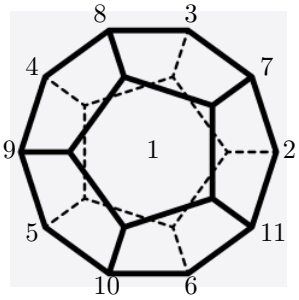
Tenemos así una base del código de Golay, que podemos mejorar sustancialmente si observamos que podemos intercambiar filas y columnas (lo segundo equivale a cambiar la numeración de los puntos, con lo que pasamos a un código "isomorfo") y a una fila podemos sumarle otra. Esto nos permite pasar a otra base que contenga una matriz identidad:

100000000000 111110010010
010000000000 111000101011
001000000000 110101001110
000100000000 110011111000
000010000000 101100111100
000001000000 101011100110
000000100000 100111010101
000000010000 011101011001
000000001000 000001111111
000000000100 001110001111
000000000010 010111100011
000000000001 011010110101

Ésta es una matriz G generadora del código, que nos permite extender cualquier sucesión x de 12 dígitos binarios a una única palabra xG del código de Golay. Los dígitos añadidos son controles de paridad, en el sentido de que, por ejemplo, el primero de ellos valdrá 1 si y sólo si en las 7 primeras posiciones de x hay un número impar de unos. Similarmente, el segundo dígito determina la paridad de los unos en las posiciones $\{1, 2, 3, 4, 8, 10, 12\}$. Los 12 conjuntos cuya paridad determina los dígitos añadidos depende de la base elegida, y la que hemos obtenido no es especialmente regular. Vamos a mostrar una construcción alternativa que es conceptualmente mucho más simple (pero no ayuda mucho a probar la unicidad del código de Golay, que hemos demostrado con nuestra construcción).

Numeremos las caras de un dodecaedro regular, como muestra la figura (donde la cara trasera es la número 12). Para cada cara, formamos el conjunto formado por su número, los de las cinco caras contiguas y el de la cara opuesta:

1	2	3	4	5	6	12
2	1	3	7	11	6	9
3	1	2	7	8	4	10
4	1	3	8	9	5	11
5	1	4	9	10	6	7
6	1	5	10	11	2	8
7	2	11	12	8	3	5
8	3	7	12	9	4	6
9	4	5	10	12	8	2
10	5	6	11	12	9	3
11	2	7	12	10	6	4
12	7	8	9	10	11	1



Para codificar una sucesión $d_1d_2d_3d_4d_5d_6d_7d_8d_9d_{10}d_{11}d_{12}$ de 12 dígitos binarios mediante el código de Golay extendido le añadimos doce dígitos más, digamos $p_1p_2p_3p_4p_5p_6p_7p_8p_9p_{10}p_{11}p_{12}$, de modo que p_i toma el valor 1 si en las 7 posiciones correspondientes a la fila i-ésima de la tabla anterior hay un número impar de unos, y 0 en caso contrario. Si aplicamos esto a las 12 sucesiones de datos con un único uno obtenemos las filas de la matriz generadora

$$G = \left(\begin{array}{cccccccccccc|cccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&1&1&0&1&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&1&1&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&1&1&1&0&1&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&0&1&1&0&0&1&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&1&1&1&0&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&1&0&0&1&1&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&1&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&1&1&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&1&1&1&1&1
\end{array}\right).$$

Un ordenador comprueba inmediatamente que las 2^{12} combinaciones lineales de estas 12 palabras tienen longitudes $0, 8, 12, 16, 24$, luego las filas de G son la base de un código de Golay $\mathcal{C}$ (necesariamente equivalente al que hemos obtenido antes, o a cualquier otro). Para codificar una sucesión de datos x, basta multiplicar xG. Para comprobar si una palabra recibida x está en el código, tenemos que ver si tiene un número par de unos en cada uno de los 12 conjuntos de posiciones determinadas por el dodecaedro. Esto se consigue calculando Hx^t, donde H es la matriz

$$H = \left(\begin{array}{cccccccccccc|cccccccccccc}
1&1&1&1&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&1&1&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&1&1&0&1&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&1&1&1&0&0&1&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0\\
1&0&0&1&0&1&1&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&1&0&0&1&1&0&1&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&1&0&1&0&1&1&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&1&1&0&1&1&1&1&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&0&1&1&0&0&1&1&1&0&1&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&1&1&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0\\
0&1&0&1&0&1&1&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&1
\end{array}\right).$$

Por construcción, si $x \in \mathcal{C}$ se cumple que $Hx^t = 0$, y el conjunto de las palabras que cumplen esta condición es un subespacio vectorial de V de dimensión $24 - 12 = 12$ que contiene al código $\mathcal{C}$, luego tiene que ser exactamente $\mathcal{C}$.

Así pues, se cumplen los hechos siguientes:

1. Una palabra $x \in V = k^{24}$ está en $\mathcal{C}$ si y sólo si $Hx^t = 0$.
2. Si enviamos una palabra $c \in \mathcal{C}$ y recibimos la palabra $x = c + e$, donde la palabra e tiene unos en los dígitos corruptos, se cumple $Hx^t = He^t$.
3. Si el peso de e es menor o igual que 7, se cumplirá $x \notin \mathcal{C}$, luego $Hx^t \neq 0$ y así detectamos que ha habido errores.
4. Si e_1 y e_2 tienen peso a lo sumo 3 y $He_1^t = He_2^t$, entonces $H(e_1 - e_2)^t = 0$, luego $e_1 - e_2 \in \mathcal{C}$, pero la resta tiene peso a lo sumo 6, luego $e_1 - e_2 = 0$ y $e_1 = e_2$.
5. Por lo tanto, si enviamos $c \in \mathcal{C}$ y recibimos $x = c + e$, donde el peso de e es a lo sumo 3, el vector e está unívocamente determinado por He^t.

Hay

$$\binom{24}{3} + \binom{24}{2} + 24 = 2\,324$$

errores posibles de peso menor o igual que 3. Haciendo una tabla con los 2 324 valores posibles para He^t y leyéndola en sentido inverso, a partir de cada resultado Hx^t podemos deducir los dígitos que se han corrompido, suponiendo que no hayan sido más de 3.

Más aún, si e tiene peso 4 y e' tiene peso ≤ 3 entonces $e - e'$ tiene peso no nulo ≤ 7, luego $H(e-e')^t \neq 0$, luego $He^t \neq He'^t$, es decir, que He^t no coincidirá con ningún valor de la tabla, con lo que sabremos que se ha producido un error que no podemos corregir.

El *código de Golay* (no extendido) es el que resulta de eliminar el último dígito de todas las palabras del código de Golay extendido. Es inmediato comprobar que es un código de tipo $[23, 12, 7]$. La dimensión del código no disminuye porque todas las palabras del código de Golay extendido tienen un número par de unos, luego la palabra extendida puede reconstruirse a partir de su proyección. Es claro que el código de Golay puede también corregir errores de hasta tres dígitos y detecta errores de hasta 6 dígitos, pero no permite identificar los errores de 4 dígitos como incorregibles.

Este código de Golay es perfecto, en el sentido de que cada palabra de k^{23} dista a lo sumo 3 unidades de una única palabra del código.

En efecto, cada palabra del código tiene

$$\binom{23}{3} + \binom{23}{2} + \binom{23}{1} + 1 = 2\,048 = 2^{11}$$

palabras a una distancia ≤ 3 y estos conjuntos de palabras son disjuntos dos a dos, luego su unión tiene $2^{12} \cdot 2^{11} = 2^{23}$ palabras, que son todas las de k^{23}.

También es claro que los grupos de Mathieu M_{11} y M_{12} son los grupos de automorfismos del código de Golay y del código de Golay extendido, respectivamente, es decir, los grupos de permutaciones de 24 elementos que transforman palabras del código en palabras del código.

Capítulo VIII

Métodos geométricos

En el capítulo anterior hemos presentado la familia de los grupos lineales especiales proyectivos, que es una de las cuatro familias clásicas de grupos simples descritas por Jordan en 1870, como se explica en la introducción. En este capítulo presentaremos otra más a la vez que introduciremos los conceptos necesarios para introducir las otras dos en el capítulo siguiente.

8.1 Formas sesquilineales

En [G 3.19] introdujimos el concepto de producto escalar en un espacio vectorial V sobre un cuerpo ordenado pitagórico, que, para el caso particular del cuerpo $\mathbb{R}$ de los números reales, es una aplicación $F : V \times V \longrightarrow \mathbb{R}$ que cumple las condiciones siguientes:

1. $F(v,v) \geq 0$ y $F(v,v) = 0$ si y sólo si $v = 0$.
2. $F(u, v+w) = F(u,v) + F(u,w)$, $F(u+v, w) = F(u,w) + F(v,w)$.
3. $F(\alpha u, v) = \alpha F(u,v)$, $F(u, \alpha v) = \alpha F(u,v)$.
4. $F(u,v) = F(v,u)$.

El ejemplo típico es el producto escalar canónico en $V = \mathbb{R}^n$ dado por

$$F(x,y) = x_1y_1 + \cdots + x_ny_n.$$

Sin embargo, en [An] vimos que, a la hora de extender la noción a espacios vectoriales sobre el cuerpo $\mathbb{C}$ de los números complejos, es conveniente adoptar la definición [An 3.36], en la que la última propiedad de simetría se sustituye por $F(u,v) = \overline{F(v,u)}$, donde la barra representa la conjugación compleja, lo cual obliga a su vez a modificar así la tercera: $F(u, \alpha v) = \bar{\alpha} F(u,v)$.

Esto es necesario para que el producto escalar canónico en $V = \mathbb{C}^n$, dado por

$$F(x,y) = x_1\bar{y}_1 + \cdots + x_n\bar{y}_n$$

sea realmente un producto escalar, y aquí la conjugación es necesaria para garantizar que

$$\|x\|^2 = F(x,x) = |x_1|^2 + \cdots + |x_n|^2$$

sea un número real no negativo al que podamos extraerle la raíz cuadrada y que sólo se anule en el vector nulo. Similarmente, introducir la conjugación es necesario para extender al caso complejo otros productos escalares definidos de forma natural en el caso real, como el producto escalar en los espacios $L^2(\mu)$ asociados a una medida, etc.

La definición siguiente incluye a las dos anteriores como casos particulares:

Definición 8.1 Sea C un cuerpo, sea $\alpha \mapsto \bar{\alpha}$ un automorfismo de C (al que llamaremos *conjugación*) y sea V un C-espacio vectorial. Una *forma sesquilineal* en V (respecto de la conjugación fijada) es una aplicación $F : V \times V \longrightarrow C$ que cumpla las propiedades siguientes:[1]

$$F(x+y,z) = F(x,z) + F(y,z), \quad F(x,y+z) = F(x,y) + F(x,z),$$

$$F(\alpha x, y) = \alpha F(x,y), \qquad F(x,\alpha y) = \bar{\alpha} F(x,y).$$

Cuando la conjugación es la identidad se dice que F es una *forma bilineal,* y si además se cumple la relación $F(x,y) = F(y,x)$, se dice que F es una *forma bilineal simétrica.* Por otro lado, si la conjugación tiene orden 2 (es decir, si no es la identidad y $\overline{\overline{\alpha}} = \alpha$) y F cumple la relación $F(x,y) = \overline{F(y,x)}$, se dice que F es una *forma hermitiana.*

Notemos que la definición anterior no incluye nada equivalente a la condición 1 de la definición de producto escalar, por lo que no toda forma bilineal simétrica es un producto escalar en un $\mathbb{R}$-espacio vectorial ni toda forma hermitiana es un producto escalar en un $\mathbb{C}$-espacio vectorial. Por ejemplo, una forma bilineal simétrica en $\mathbb{R}^3$ que no es un producto escalar es la dada por

$$F(x,y) = x_1y_1 + x_2y_2 - x_3y_3.$$

Nota *En este capítulo supondremos tácitamente que todos los espacios vectoriales tienen dimensión finita.* ∎

Cuando hablemos de un espacio vectorial V dotado de una forma sesquilineal (o, en particular, bilineal), nos referiremos en realidad a un par (V,F), donde V es un espacio vectorial y F una forma en V del tipo indicado.

El propósito de este capítulo es estudiar la geometría de estos espacios (con algunas condiciones adicionales), pues veremos que a partir de los grupos de isometrías correspondientes (es decir, los subgrupos de $\mathrm{LG}(V)$ formados por los

[1] En general, una aplicación $f : V \longrightarrow V$ que cumpla $f(x+y) = f(x)+f(y)$ y $f(\alpha x) = \bar{\alpha} f(x)$ recibe el nombre de *aplicación semilineal,* con lo que, en estos términos, la forma F es lineal en su primer argumento y semilineal en el segundo, y de ahí el nombre de "sesquilineal", pues el prefijo "sesqui-" significa "vez y media".

automorfismos que conservan la estructura considerada) es posible obtener nuevas familias de grupos simples pasando a subgrupos y cocientes, análogamente a como hemos pasado a los grupos $\mathrm{LEP}(V)$ a partir de $\mathrm{LG}(V)$.

El teorema siguiente recoge algunos hechos básicos sobre los automorfismos de orden 2 sobre un cuerpo arbitrario:

Teorema 8.2 *Sea C un cuerpo y consideremos en él un automorfismo de orden 2 que representaremos por $\alpha \mapsto \bar{\alpha}$. Entonces:*

1. *El conjunto $R = \{\alpha \in C \mid \bar{\alpha} = \alpha\}$ es un subcuerpo de C tal que $|C : R| = 2$.*
2. *La traza $\mathrm{Tr} : C \longrightarrow R$ dada por $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$ es una aplicación R-lineal suprayectiva (pero no inyectiva).*

DEMOSTRACIÓN: Claramente $|C : R| \geq 2$, o de lo contrario sería $R = C$ y $\bar{\alpha} = \alpha$ para todo $\alpha \in C$, con lo que la conjugación sería la identidad y no tendría orden 2.

La traza es suprayectiva porque es claramente R-lineal, luego su imagen tiene que ser 0 o R, y no es nula porque en tal caso $\alpha + \bar{\alpha} = 0$ para todo $\alpha \in C$. Tomando $\alpha = 1$ vemos que $2 = 0$, luego $\bar{\alpha} = \alpha$ para todo $\alpha \in C$, con lo que volvemos a la misma contradicción.

Como C tiene dimensión sobre R mayor que 1, el núcleo de la traza tiene dimensión no nula, luego la traza no es inyectiva, luego podemos tomar $\alpha \in C$ no nulo tal que $\alpha + \bar{\alpha} = 0$. Si la característica de C no es 2, cualquier $\beta \in C$ puede expresarse como

$$\beta = \frac{\beta + \bar{\beta}}{2} + \frac{\beta - \bar{\beta}}{2} = \frac{\beta + \bar{\beta}}{2} + \frac{\beta - \bar{\beta}}{2\alpha}\alpha,$$

y los dos coeficientes están en R, luego $C = \langle 1, \alpha\rangle$. En el caso en que C tiene característica 2, tomamos cualquier $\alpha \in C \setminus R$, con lo que $\alpha + \bar{\alpha} \neq 0$, y descomponemos

$$\beta = \frac{\bar{\alpha}\beta + \bar{\beta}\alpha}{\alpha + \bar{\alpha}} + \frac{\beta + \bar{\beta}}{\alpha + \bar{\alpha}}\alpha,$$

y nuevamente los coeficientes están en R y así $C = \langle 1, \alpha\rangle$. ∎

Expresión matricial Si $v_1, \ldots, v_n$ es una base de un espacio vectorial V, toda forma sesquilineal F sobre V puede calcularse a partir de las coordenadas de los vectores, pues si u, v tienen coordenadas $x, y \in C^n$, entonces

$$F\Big(\sum_{i=1}^n x_i v_i, \sum_{j=1}^n y_j v_j\Big) = \sum_{i,j=1}^n x_i F(v_i, v_j)\bar{y}_j = xJ\bar{y}^t,$$

donde $J = (F(v_i, v_j))$ recibe el nombre de *matriz de la forma sesqulineal F* en la base considerada.

Cualquier matriz J define de este modo (fijada una base) una forma sesquilineal en V, pero para que sea simétrica/hermitiana (además de que la conjugación tenga orden 1 o 2, respectivamente), se tiene que cumplir que $xJ\bar{y}^t = \bar{y}\bar{J}x^t$, que equivale a $xJ\bar{y}^t = \bar{x}\bar{J}^t\bar{y}^t$ para todo par de n-tuplas $x, y \in C^n$ y, dando a x, y valores en la base canónica de C^n, esto equivale a que $J = \bar{J}^t$.

Cuando la conjugación es la identidad, las matrices que cumplen $J = J^t$ son simplemente las matrices simétricas, mientras que, para conjugaciones de orden dos, las matrices que cumplen $J = \bar{J}^t$ se llaman *matrices hermitianas.*

Así pues, cada base de V determina una correspondencia biunívoca entre las formas bilineales simétricas/hermitianas en V y las matrices simétricas/hermitianas $n \times n$ en C.

Fijadas dos bases B_1 y B_2 de V, podemos considerar la matriz M de cambio de base, de modo que si $x \in C^n$ son las coordenadas de un vector v en la base B_1, entonces xM son las coordenadas de v en la base B_2. Entonces, si J es la matriz de una forma sesquilineal F en la base B_2 y x, y son las coordenadas de dos vectores $v_1, v_2 \in V$ en la base B_1, resulta que

$$F(v_1, v_2) = xMJ\bar{M}^t\bar{y}^t,$$

por lo que la matriz de F en la base B_1 es $B = MJ\bar{M}^t$.

Cuando dos matrices cumplen la relación $J_2 = MJ_1M^t$, donde M es una matriz regular, se dice que son *congruentes.* Notemos que la congruencia es una relación de equivalencia en el conjunto $\mathrm{Mat}_n(C)$ de todas las matrices $n \times n$ sobre C, y también lo es restringida al subconjunto de las matrices simétricas o hermitianas.

Isometrías Una *isometría* $f : (V, F) \longrightarrow (W, G)$ entre dos C-espacios vectoriales dotados de formas sesquilineales (respecto de la misma conjugación), es un isomorfismo $f : V \longrightarrow W$ de espacios vectoriales tal que

$$G(f(u), f(v)) = F(u, v),$$

para todos los vectores $u, v \in V$.

Si $v_1, \ldots, v_n$ es una base de V, es fácil ver que f es una isometría si y sólo si cumple esta relación cuando u y v recorren $v_1, \ldots, v_n$. A su vez, esto significa que f es una isometría si y sólo si la matriz de f respecto a una base $v_1, \ldots, v_n$ es la misma que la matriz de G respecto de la base $f(v_1), \ldots, f(v_n)$.

Obviamente, si existe una isometría entre dos espacios V y W dotados de formas sesquilineales, ambos tienen las mismas propiedades definibles a partir de las formas correspondientes, y son, a todos los efectos, "el mismo espacio".

Si J_1 y J_2 son las matrices de F y G en bases respectivas de V y W y M es la matriz de un isomorfismo $f : V \longrightarrow W$, es claro que f será una isometría si y sólo si $xMJ_2\bar{M}^t\bar{y}^t = xJ_1\bar{y}$, para todo par de n-tuplas $x, y \in C^n$, lo que a su vez equivale a que

$$MJ_2\bar{M}^t = J_1.$$

Ortogonalidad Si V es un espacio vectorial dotado de una forma sesquilineal F, diremos que dos vectores $u, v \in V$ son *ortogonales* (y lo representaremos por $u \perp v$) si $F(u, v) = 0$.

Si F es bilineal simétrica o hermitiana, se cumple que $u \perp v$ es equivalente a $v \perp u$. Éste es el caso que nos va a interesar casi exclusivamente, pero conviene probar algunos resultados básicos sin suponer ninguna hipótesis de simetría.

Dado un subespacio $W \leq V$, definimos

$$W^\perp = \{v \in V \mid F(w, v) = 0 \text{ para todo } w \in W\},$$

$$^\perp W = \{v \in V \mid F(v, w) = 0 \text{ para todo } w \in W\}.$$

Es claro que se trata de dos subespacios vectoriales de V. Por ejemplo, $0 \in W^\perp$ porque

$$F(w, 0) = F(w, 0 + 0) = F(w, 0) + F(w, 0),$$

luego $F(w, 0) = 0$.

Si F es bilineal simétrica o hermitiana, se cumple que $^\perp W = W^\perp$, pero en general ambos subespacios pueden diferir.

Observemos que el grado de generalidad con el que estamos trabajando no impide que un vector no nulo pueda ser ortogonal a sí mismo. De hecho, se trata de un caso que nos aparecerá con frecuencia y que no podemos descartar, pero hay un caso extremo que sí que vamos a excluir, y es que un vector sea ortogonal a todos los vectores de V. A este respecto tenemos el teorema siguiente:

Teorema 8.3 *Si V es un espacio dotado de una forma sesquilineal F, las afirmaciones siguientes son equivalentes:*

1. $V^\perp = 0$.
2. $^\perp V = 0$.
3. *El determinante de F en una cierta base de V es no nulo.*
4. *El determinante de F en toda base de V es no nulo.*

Demostración: Sea $v_1, \ldots, v_n$ una base de V y sea B la matriz de F en dicha base. Sea $v \in V$ un vector no nulo y sea $x \in C^n$ su vector de coordenadas. Entonces $v \in {}^\perp V$ si y sólo si $F(w, v) = 0$ para todo $w \in V$, lo cual equivale a que $yB\bar{x}^t = 0$ para todo $y \in C^n$ y, dando a y valores en la base canónica de C^n, es claro que esto equivale a que $B\bar{x}^t = 0$ y esto, a su vez, significa que las columnas de B son linealmente dependientes, lo cual es equivalente a que $|B| = 0$. Esto prueba la equivalencia entre 2), 3) y 4), y análogamente se prueba la equivalencia con 1). ∎

Definición 8.4 Una forma sesquilineal F en un espacio vectorial V es *no degenerada* si cumple cualquiera de las condiciones del teorema anterior. En caso contrario se dice que es *degenerada.*

Consideremos el espacio dual V^*, formado por todas las aplicaciones lineales $V \longrightarrow C$, y definimos

$$\iota_i : V \longrightarrow V^*, \qquad \iota_d : V \longrightarrow V^*$$

mediante

$$\iota_i(v)(w) = \overline{F(v,w)}, \qquad \iota_d(v)(w) = F(w,v).$$

Es inmediato comprobar que $\iota_i(v), \iota_d(v) \in V^*$, así como que ι_i, ι_d son aplicaciones semilineales, pues cumplen $\iota_i(\alpha v) = \bar{\alpha}\iota_d(v)$, $\iota_i(\alpha v) = \bar{\alpha}\iota_d(v)$ (de modo que son aplicaciones lineales si y sólo si la conjugación en C es la identidad).

En estos términos, $V^\perp$ y ${}^\perp V$ son los núcleos de ι_i, ι_d, respectivamente, luego F es no degenerada si y sólo si cualquiera de las dos es inyectiva y, por consiguiente (dado que V y V^* tienen la misma dimensión) biyectiva.[2] Por lo tanto:

Teorema 8.5 *Si V es un espacio dotado de una forma sesquilineal no degenerada, para cada aplicación lineal $f : V \longrightarrow C$ existe un único vector $v \in V$ tal que $f(x) = F(x,v)$, para todo $x \in V$.*

En estas condiciones, si $W \leq V$, tenemos que las aplicaciones semilineales

$$\iota_i^W : V \longrightarrow W^*, \qquad \iota_d^W : V \longrightarrow W^*$$

definidas igualmente por

$$\iota_i^W(v)(w) = \overline{F(v,w)}, \qquad \iota_d^W(v)(w) = F(w,v)$$

son suprayectivas, pues toda $f \in W^*$ se extiende a una aplicación $\hat{f} : V^*$, que a su vez tiene una antiimagen $v \in V$ tal que $\iota_i^W(v) = \hat{f}|_W = f$ (resp. $\iota_d^W(v) = \hat{f}|_W = f$). Como los núcleos de estas aplicaciones son ${}^\perp W$ y $W^\perp$, respectivamente, tenemos el teorema siguiente:

Teorema 8.6 *Si V es un espacio dotado de una forma sesquilineal no degenerada y $W \leq V$, entonces*

$$\dim W + \dim W^\perp = \dim W + \dim {}^\perp W = \dim V.$$

Como trivialmente se cumple que $W \leq ({}^\perp W)^\perp$ y $W \leq {}^\perp(W^\perp)$, el teorema anterior implica que

$$W = ({}^\perp W)^\perp = {}^\perp(W^\perp).$$

[2]Es inmediato comprobar que, para toda aplicación semilineal $f : V \longrightarrow W$ entre dos C-espacios vectoriales de dimensión finita, se cumple que su núcleo y su imagen son subespacios vectoriales, que f es inyectiva si y sólo si $\mathrm{N}(f) = 0$, así como la relación

$$\dim V = \dim \mathrm{N}(f) + \dim \mathrm{Im}(f).$$

Por ejemplo, para probar la última igualdad tomamos una base $v_1, \ldots, v_r$ de $\mathrm{N}(f)$ y la antiimagen $u_1, \ldots, u_s$ de una base de $\mathrm{Im}(f)$ y se comprueba que $v_1, \ldots, v_r, u_1, \ldots, u_s$ es una base de V.

Definición 8.7 Una forma sesquilineal F en un espacio vectorial V es *ortosimétrica* si cumple que $F(v,w)=0$ si y sólo si $F(w,v)=0$.

Ya hemos señalado que esto se cumple cuando F es hermitiana o bilineal simétrica, pero hay un tercer caso que nos va a interesar:

Una forma bilineal F en un espacio vectorial V es *antisimétrica* si cumple que $F(v,w)=-F(w,v)$.

Obviamente las formas bilineales antisimétricas son ortosimétricas, y si el cuerpo de escalares C tiene característica 2, coinciden con las formas bilineales simétricas.

Si F es ortosimétrica y $W\leq V$, es claro que $W^\perp={}^\perp W$ y las igualdades que hemos obtenido tras el teorema 8.6 se reducen a que (si F es no degenerada)

$$W^{\perp\perp}=W.$$

Observemos que si F es una forma ortosimétrica, hermitiana, bilineal simétrica o antisimétrica no degenerada, su restricción a un subespacio W es del mismo tipo, pero puede ser degenerada.

Definición 8.8 Si V es un espacio dotado de una forma sesquilineal ortosimétrica no degenerada y $W\leq V$, diremos que W es *degenerado* o *no degenerado* según si lo es con la restricción de la forma F de V. Claramente esto equivale a que ningún vector no nulo de W sea ortogonal a todos los vectores de W o, equivalentemente, a que $W\cap W^\perp=0$

Un hecho elemental, pero de gran importancia es que si W no es degenerado, tampoco lo es $W^\perp$, ya que en ambos casos la condición de no degeneración es que $W\cap W^\perp=0$.

En tal caso se cumple que $\dim(W+W^\perp)=\dim V$, luego:

Teorema 8.9 *Si V es un espacio dotado de una forma sesquilineal ortosimétrica no degenerada y $W\leq V$ es un subespacio no degenerado, se cumple que $V=W\oplus W^\perp$.*

Se suele escribir $V=W_1\perp\cdots\perp W_r$ para indicar que $V=W_1\oplus\cdots\oplus W_r$ y que además los vectores de cada W_i son ortogonales a los de los demás subespacios W_j. En estos términos, lo que hemos probado es que, si W no es degenerado, entonces $V=W\perp W^\perp$.

8.2 Los grupos simplécticos

De las distintas geometrías que nos van a interesar, la más simple es la correspondiente a un espacio dotado de una forma bilineal antisimétrica, pero cuando el cuerpo de escalares tiene característica 2 es necesario imponer una condición más fuerte para que los resultados válidos en otras características sigan cumpliéndose:

Definición 8.10 Una forma bilineal $F : V \times V \longrightarrow C$ en un espacio vectorial V sobre un cuerpo C es *alternada* si cumple $F(v, v) = 0$, para todo $v \in V$.

Un *espacio simpléctico*[3] V es un par (V, F), donde V es un espacio vectorial sobre un cuerpo C y F es una forma bilineal alternada no degenerada.

Si F es una forma alternada, se cumple que

$$F(v + w, v + w) = F(v, w) + F(w, v) = 0,$$

o, equivalentemente, $F(v, w) = -F(w, v)$.

Así pues, toda forma alternada es antisimétrica y, si la característica de C es distinta de 2, ambas propiedades son equivalentes. En cambio, si la característica de C es 2, las formas alternadas son antisimétricas y también simétricas, pero no toda forma simétrica es alternada.

Las isometrías de un espacio simpléctico V en sí mismo se llaman *transformaciones simplécticas* y claramente forman un grupo al que llamaremos *grupo simpléctico* de V y lo representaremos por $\mathrm{Sp}(V)$.

Claramente, si en una base de V la forma bilineal tiene matriz J y un isomorfismo f tiene matriz M, entonces $f \in \mathrm{Sp}(V)$ si y sólo si $MJM^t = J$.

Veamos que todo espacio simpléctico posee bases en la que la matriz J de la forma bilineal es especialmente sencilla:

Si V es un espacio simpléctico y $u \in V$ es un vector no nulo, el hecho de que V sea no degenerado implica que existe $v \in V$ tal que $F(u, v) \neq 0$ y, cambiando v por un múltiplo, podemos exigir que $F(u, v) = 1$. Notemos que u y v tienen que ser linealmente independientes, pues si fuera $v = \alpha u$, entonces $F(u, v) = \alpha F(u, u) = 0$.

Un *par hiperbólico* en un espacio simpléctico V es un par de vectores (u, v) tales que $F(u, v) = 1$. Un *plano hiperbólico* es el subespacio generado por un par hiperbólico.

La matriz de la forma bilineal restringida a un plano hiperbólico tiene, en la base formada por el par hiperbólico, matriz

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

cuyo determinante vale 1, luego los planos hiperbólicos son no degenerados. Hemos probado que todo vector no nulo en un espacio simpléctico forma parte de un par hiperbólico. Más en general:

[3]"Simpléctico" en griego significa "complejo". El término fue introducido por Hemann Weyl en 1939 para referirse a los grupos simplécticos que introduciremos en el capítulo siguiente en el caso particular de espacios vectoriales definidos sobre el cuerpo de los números complejos.

Teorema 8.11 *Si V es un espacio simpléctico, entonces* $\dim V = 2m$ *es un número par, y*

$$V = H_1 \perp \cdots \perp H_m$$

es suma ortogonal de planos hiperbólicos.

DEMOSTRACIÓN: Si $u_1 \in V$ es no nulo, hemos visto que existe $v_1 \in V$ tal que $H_1 = \langle u_1, v_1\rangle$ es un plano hiperbólico, y entonces $H_1^\perp$ es un espacio simpléctico. Si es no nulo, podemos tomar en él otro vector no nulo u_2 y completarlo hasta un plano hiperbólico $H_2 = \langle u_2, v_2\rangle$. Tras un número finito de pasos tenemos que llegar a la descomposición del enunciado. ∎

Este teorema implica que dos espacios simplécticos de la misma dimensión son isométricos, pues ambos admiten una base formada por una unión de planos hiperbólicos, y respecto a dichas bases la matriz de las formas bilineales respectivas es la misma.

Si V es un espacio simpléctico, llamaremos $\mathrm{Sp}(V) \leq \mathrm{LG}(V)$ al grupo de todas las *transformaciones simplécticas* de V, es decir, el grupo de las isometrías de V en sí mismo.

En vista de la observación precedente, el grupo $\mathrm{Sp}(V)$ está determinado salvo isomorfismo por la dimensión de V y el cuerpo C de escalares, por lo que podemos llamar $\mathrm{Sp}(2m, C)$ al grupo simpléctico de cualquier espacio simpléctico de dimensión $2m$ sobre el cuerpo C. Si C es el cuerpo de q elementos escribiremos también $\mathrm{Sp}(2m, q)$.

Otra consecuencia del teorema anterior es que todo espacio simpléctico de dimensión 2 es un plano hiperbólico. Su grupo de isometrías es fácil de calcular:

Teorema 8.12 *Si V es un plano hiperbólico,* $\mathrm{Sp}(V) \cong \mathrm{LE}(V)$.

DEMOSTRACIÓN: Sea (u, v) un par hiperbólico en V. Los elementos de $\mathrm{Sp}(V)$ son los automorfismos de V cuya matriz en la base (u, v) cumple

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Al operar vemos que esto equivale a que $ad - bc = 1$, es decir, a que la matriz esté en el grupo $\mathrm{LE}(2, C)$ o, equivalentemente, a que la transformación esté en el grupo $\mathrm{LE}(V)$. ∎

Transvecciones simplécticas En el estudio de los grupos $\mathrm{LG}(V)$ que hemos presentado en la sección 7.2 ha sido fundamental el hecho de que el grupo $\mathrm{LE}(V)$ está generado por las transvecciones. Similarmente, vamos a probar que los grupos $\mathrm{Sp}(V)$ están generados por las transvecciones simplécticas.

Recordemos de [Al 6.20] que una transvección en un espacio vectorial V es un automorfismo $T : V \longrightarrow V$ de la forma

$$T(v) = v + f(v)a,$$

donde $f : V \longrightarrow C$ es una aplicación lineal cuyo núcleo es un hiperplano H y $a \in H$ no es nulo. En particular, T deja fijos a los vectores de H.

Vamos a ver qué tiene que cumplir una transvección para ser simpléctica.

Completando una base de H hasta una base de V podemos descomponer $V = H \oplus \langle x\rangle$ y considerar la proyección $\pi : V \longrightarrow C$ que a cada $v \in V$ le hace corresponder el escalar que permite expresar $v = h + \pi(v)x$, con $h \in H$. El teorema 8.5 nos da un $u \in V$ tal que $\pi(v) = F(v,u)$, para todo $v \in V$. Como $\pi(x) = 1$, $u \neq 0$ y, como π se anula en H, tiene que ser $F(h,u) = 0$ para todo $h \in H$, luego $u \in H^\perp$. Como $\dim H = n-1$, tenemos que $\dim H^\perp = 1$, luego $H^\perp = \langle u\rangle$.

Así, todo vector $v \in V$ se expresa en la forma $v = h + F(v,u)x$, con lo que

$$T(v) = T(h + F(v,u)x) = h + F(v,u)x + F(v,u)f(x)a = v + F(v,u)z,$$

donde $z = f(x)a \in H$ no es nulo, luego $F(z,u) = 0$. Esto vale para cualquier transvección. Que T sea simpléctica significa que

$$F(v,w) = F(T(v),T(w)) = F(v + F(v,u)z, w + F(w,u)z) =$$

$$F(v,w) + F(v,u)F(z,w) + F(w,u)F(v,z),$$

luego T es simpléctica si y sólo si

$$F(v,u)F(z,w) + F(w,u)F(v,z) = 0$$

para todo par de vectores $v, w \in V$.

En particular, si $w \in H$ tenemos que $F(v,u)F(z,w) = 0$ y, como podemos elegir v de modo que $F(v,u) \neq 0$, concluimos que $F(z,w) = 0$ para todo $w \in H$, luego $z \in H^\perp = \langle u\rangle$. Así, $H = \langle z\rangle^\perp$ y, si $u = \alpha z$, con $\alpha \neq 0$,

$$T(v) = v + \alpha F(v,z)z$$

y la condición para que T sea simpléctica se reduce a

$$F(v,z)F(z,w) + F(w,z)F(v,z) = 0,$$

que se cumple siempre, porque F es alternada. En resumen:

Teorema 8.13 *Si V es un espacio simpléctico, las transvecciones simplécticas en V son los automorfismos de la forma*

$$T_{z,\alpha}(v) = v + \alpha F(v,z)z,$$

donde $z \in V$ es no nulo y $\alpha \neq 0$.

Notemos que podemos tomar también $\alpha = 0$, en cuyo caso obtenemos simplemente $T_{z,\alpha} = 1$. Es inmediato comprobar las relaciones siguientes:

1. $T_z, \alpha T_{z,\beta} = T_{z,\alpha+\beta}$,
2. $T_{\beta z,\alpha} = T_{z,\alpha\beta^2}$,
3. Si $f \in \mathrm{Sp}(V)$, $f^{-1}T_{z,\alpha}f = T_{f(z),\alpha}$.

Si V es un espacio simpléctico, vamos a llamar temporalmente $\mathcal{T}(V) \leq \mathrm{Sp}(V)$ al subgrupo generado por las transvecciones simplécticas. Vamos a probar que $\mathcal{T}(V) = \mathrm{Sp}(V)$.

Teorema 8.14 *Si V es un espacio simpléctico, entonces $\mathcal{T}(V)$ actúa transitivamente sobre $V \setminus \{0\}$.*

DEMOSTRACIÓN: Sean $u \neq v$ dos vectores no nulos. Si $F(u,v) \neq 0$, llamemos $\alpha = F(u,v)^{-1}$ y $z = u - v$. Entonces

$$T_{z,\alpha}(u) = u + \frac{F(u,u-v)}{F(u,v)}(u-v) = v.$$

Supongamos ahora que $F(u,v) = 0$. Consideremos cualquier aplicación lineal $f : V \longrightarrow C$ que cumpla $f(u) \neq 0 \neq f(v)$. Por el teorema 8.5 existe $z \in V$ tal que $F(u,z) = f(u) \neq 0$ y $F(v,z) = f(v) \neq 0$. Por el apartado anterior existe una transvección que transforma u en z y otra que transforma z en v. ∎

Teorema 8.15 *Si V es un espacio simpléctico, el grupo $\mathcal{T}(V)$ actúa transitivamente sobre el conjunto de los pares hiperbólicos de V.*

DEMOSTRACIÓN: Si (u_1, v_1) y (u_2, v_2) son dos pares hiperbólicos, por el teorema anterior existe un elemento de $\mathcal{T}(V)$ que transforma (u_1, v_1) en un par (u_2, v_2'), luego no perdemos generalidad si suponemos que $u_1 = u_2 = u$, y tenemos que encontrar un $f \in \mathcal{T}(V)$ que cumpla $f(u) = u$ y $f(v_1) = v_2$. Si $f(v_1, v_2) \neq 0$, consideramos, como en el teorema anterior, $z = v_1 - v_2$ y $\alpha = F(v_1, v_2)^{-1}$, con lo que $T_{z,\alpha}(v_1) = v_2$, y además

$$T_{z,\alpha}(u) = u + \frac{F(u, v_1 - v_2)}{F(v_1, v_2)} z = u,$$

pues $F(u, v_1) - F(u, v_2) = 1 - 1 = 0$. Supongamos ahora que $F(v_1, v_2) = 0$. Entonces $(u, u+v_2)$ es un par hiperbólico y $F(v_1, u+v_2) \neq 0$, luego, por la parte ya probada, existe un elemento de $\mathcal{T}(V)$ que transforma (u, v_1) en $(u, u + v_2)$, pero $F(u+v_2, v_2) \neq 0$, luego también existe un elemento de $\mathcal{T}(V)$ que transforma $(u, u + v_2)$ en (u, v_2). ∎

Teorema 8.16 *Si V es un espacio simpléctico, el grupo $\mathrm{Sp}(V)$ está generado por las transvecciones simplécticas.*

DEMOSTRACIÓN: Sea $\dim V = 2m$ y razonemos por inducción sobre m. Si $m = 1$ V es un plano hiperbólico y $\mathrm{Sp}(V) = \mathrm{LE}(V)$, que está generado por las transvecciones por [Al 6.22].

Si $m \geq 2$, tomemos un plano hiperbólico $H = \langle u, v \rangle$ en V, de modo que $V = H \perp H^\perp$. Si $f \in \mathrm{Sp}(V)$, tenemos que $(f(u), f(v))$ es un par hiperbólico, luego por el teorema anterior existe $g \in \mathcal{T}(V)$ tal que $(g(u), g(v)) = (f(u), f(v))$. Así, $fg^{-1}|_H = 1|_H$ y $fg^{-1}|_{H^\perp} \in \mathrm{Sp}(H^\perp)$. Por hipótesis de inducción $fg^{-1}|_H$ es

composición de transvecciones, cada una de las cuales se extiende a una transvección en V que se restringe a la identidad en H, luego fg^{-1} es composición de transvecciones y f también. ∎

En particular, como las transvecciones tienen determinante 1, se cumple que $\mathrm{Sp}(V) \leq \mathrm{LE}(V)$. Esto hace que $\mathrm{Sp}(V)$ no contenga ningún "subgrupo especial" análogo al subgrupo $\mathrm{LE}(V)$ de $\mathrm{LG}(V)$, sino que todas las transformaciones simplécticas son ya "especiales". En cambio, sí que tenemos un centro no trivial que hay que eliminar si queremos obtener un grupo simple:

Teorema 8.17 *Si V es un espacio simpléctico, el centro de $\mathrm{Sp}(V)$ es $\{\pm 1\}$.*

Demostración: Sea $f \in Z(\mathrm{Sp}(V))$. Si $z \in V$ es cualquier vector no nulo, tenemos que $T_{z,1} = T_{z,1}^f = T_{f(z),1}$, luego $\langle z\rangle^\perp = \langle f(z)\rangle^\perp$ (porque ambos son el hiperplano de vectores fijados por la transvección), luego $\langle z\rangle = \langle f(z)\rangle$, luego existe un escalar a_z tal que $f(z) = a_z z$.

Si $y, z \in V$ son linealmente independientes, entonces

$$a_{y+z}(y+z) = f(y+z) = f(y) + f(z) = a_y y + a_z z,$$

luego $a_y = a_{y+z} = a_z$. Aplicando esto a los vectores de una base de V concluimos que existe un mismo escalar a tal que $f(z) = az$ para todo vector básico, luego para todo vector. Por último,

$$F(u,v) = F(f(u), f(v)) = F(au, av) = a^2 F(u,v),$$

de donde $a^2 = 1$, luego $a = \pm 1$ y así $f = \pm 1$. ∎

Los grupos simplécticos proyectivos En [Al 4.39] hemos visto que, si V es un espacio vectorial, el centro $Z(V)$ de $\mathrm{LG}(V)$ está formado por las homotecias lineales, es decir, por los automorfismos dados por $f(v) = \alpha v$, para un cierto $\alpha \in C$. Por lo tanto, teniendo en cuenta el teorema anterior, si V es un espacio simpléctico,

$$Z(V) \cap \mathrm{Sp}(V) = \{\pm 1\}.$$

Según vimos en la sección [G 8.2] el grupo $\mathrm{LGP}(V) = \mathrm{LG}(V)/Z(V)$ se identifica con el grupo de las homografías del espacio proyectivo $P(V)$, y ahora podemos considerar el *grupo simpléctico proyectivo*

$$\mathrm{SpP}(V) = \mathrm{Sp}(V)/\{\pm 1\}$$

al que podemos ver como subgrupo de $\mathrm{LGP}(V)$, es decir, que podemos considerar también a sus elementos como (parte de las) homografías del espacio $P(V)$.

Vamos a probar que estos grupos son simples salvo en unos pocos casos excepcionales. Para ello aplicaremos el teorema de Iwasawa, y entre otras cosas necesitaremos el hecho siguiente:

Teorema 8.18 *Si V es un espacio simpléctico, el grupo $\mathrm{SpP}(V)$ es primitivo sobre $P(V)$.*

DEMOSTRACIÓN: Si V es un plano hiperbólico, el teorema 8.12 nos da que $\mathrm{Sp}(V) = \mathrm{LE}(V)$, luego $\mathrm{SpP}(V) \cong \mathrm{LEP}(V)$, y en la prueba del teorema 7.17 hemos visto[4] que $\mathrm{LEP}(V)$ es doblemente transitivo sobre $P(V)$, luego en particular primitivo.

Así pues, podemos suponer que $\dim V = n = 2m$, con $m \geq 2$. Supongamos que $B \subset P(V)$ es un bloque con $|B| > 1$. Veamos en primer lugar que existen $\langle u\rangle, \langle v\rangle \in B$ tales que $F(u,v) \neq 0$.

En caso contrario, tomemos dos puntos distintos $\langle u\rangle, \langle v\rangle \in B$ y consideremos una aplicación lineal $f : V \longrightarrow C$ tal que $f(u) = 1$, $f(v) = 0$. Por 8.5 existe $x \in V$ tal que $F(u,x) = 1$, $F(v,x) = 0$. Así $H = \langle u, x\rangle$ es un plano hiperbólico y $v \in H^\perp$. Si $w \in H^\perp$ es no nulo, por el teorema 8.14 existe $f \in \mathrm{Sp}(H^\perp)$ que cumple $f(v) = w$, y podemos extenderla a $f \in \mathrm{Sp}(V)$ tal que $f|_H = 1|_H$. En particular $f(\langle u\rangle) = \langle u\rangle$, luego $f[B] = B$, luego $\langle w\rangle = \langle f(v)\rangle \in f[B] = B$. Así pues, $P(H^\perp) \subset B$, pero $H^\perp$ contiene vectores u, v tales que $F(u,v) = 1$ (los de un par hiperbólico) y tenemos una contradicción.

Por consiguiente, podemos tomar $\langle u\rangle, \langle v\rangle \in B$ tales que $F(u,v) \neq 0$ y, concretamente, podemos suponer que $F(u,v) = 1$. Sea ahora $\langle w\rangle \in P(V)$ un punto arbitrario. Si $F(u,w) \neq 0$, podemos suponer que $F(u,w) = 1$ y el teorema 8.15 nos da $f \in \mathrm{Sp}(V)$ tal que $f(u) = u$, $f(v) = w$, con lo que $f[B] = B$ y $\langle w\rangle \in f[B] = B$.

Por otra parte, si $F(u,w) = 0$, el teorema 8.5 nos da un vector $x \in V$ tal que $F(u,x) = F(w,x) = 1$. Por el caso precedente, como $F(u,x) \neq 0$, tenemos que $\langle x\rangle \in B$ y como $F(w,x) \neq 0$, también $\langle w\rangle \in B$. Esto prueba que $B = P(V)$. ∎

La aplicación del teorema de Iwasawa requiere también el resultado siguiente:

Teorema 8.19 *Si V es un espacio simpléctico, entonces $\mathrm{Sp}(V)' = \mathrm{Sp}(V)$ excepto en los casos de $\mathrm{Sp}(2,3)$, $\mathrm{Sp}(2,2)$ y $\mathrm{Sp}(4,2)$.*

DEMOSTRACIÓN: Supongamos en primer lugar que $|C| \geq 4$. Sea $z \in V$ cualquier vector no nulo, $\alpha \in C^*$ y $\beta \in C^*$ tal que $\beta \neq \pm 1$. Llamemos

$$\gamma = \frac{\alpha}{1-\beta^2}, \qquad \delta = -\beta^2\gamma.$$

Entonces $\delta + \gamma = \alpha$, luego $T_{z,\delta}T_{z,\gamma} = T_{z,\alpha}$. El teorema 8.14 nos da $f \in \mathrm{Sp}(V)$ tal que $f(z) = \beta z$, y así

$$[f, T_{z,\gamma}] = f^{-1}T_{z,\gamma}^{-1}fT_{z,\gamma} = f^{-1}T_{z,-\gamma}fT_{z,\gamma} = T_{\beta z,-\gamma}T_{z,\gamma} = T_{z,\delta}T_{z,\gamma} = T_{z,\alpha}.$$

Esto prueba que $\mathrm{Sp}(V)'$ contiene todas las transvecciones, luego es $\mathrm{Sp}(V)$ por el teorema 8.16.

Si $|C| = 3$ tenemos que suponer que $\dim V \geq 4$. Fijemos una base de V formada por pares hiperbólicos

$$u_1, v_1, u_2, v_2, \ldots, u_n, v_n$$

[4]Notemos que esa parte de la prueba es válida incluso en los casos exceptuados en el enunciado.

y consideremos los automorfismos f y g dados por

$$f(u_1) = u_2, \quad f(v_1) = v_1 + v_2, \quad f(u_2) = u_1 - u_2, \quad f(v_2) = v_1,$$

$$g(u_1) = u_1 + v_2, \quad g(v_1) = v_1, \quad g(u_2) = v_1 + u_2, \quad g(v_2) = v_2,$$

y que fijan a todos los demás vectores básicos (si los hay). Una comprobación rutinaria muestra que $f, g \in \mathrm{Sp}(V)$ (basta comprobar que las matrices en la base fijada cumplen $MJM^t = J$, donde J es la matriz de la forma cuadrática, y en la práctica sólo es necesario considerar las matrices de las restricciones a las cuatro primeras componentes). Igualmente se comprueba que $[f, g] = T_{v_1,1}$, luego $T_{v_1,1} \in \mathrm{Sp}(V)'$.

Ahora, dado cualquier $z \in V$ no nulo, podemos tomar $h \in \mathrm{Sp}(V)$ tal que $h(v_1) = z$, con lo que

$$T_{z,1} = T^h_{v_1,1} \in \mathrm{Sp}(V)', \qquad T_{z,-1} = T^{-1}_{z,1} \in \mathrm{Sp}(V)'$$

y de nuevo concluimos que $\mathrm{Sp}(V)'$ es todo el grupo simpléctico.

Finalmente, si $|C| = 2$ tenemos que suponer que $\dim V \geq 6$. El razonamiento es análogo al del caso anterior, pero tomando ahora

$$f(u_1) = u_3, \quad f(v_1) = v_1 + v_3, \quad f(u_2) = u_1 + u_3,$$

$$f(v_2) = v_1, \quad f(u_3) = u_2, \quad f(v_3) = v_2,$$

$$g(u_1) = u_1 + v_1 + v_3, \quad g(v_1) = v_1, \quad g(u_2) = u_2 + v_2 + v_3,$$

$$g(v_2) = v_2, \quad g(u_3) = v_1 + v_2 + u_3 + v_3, \quad g(v_3) = v_3.$$

■

Con esto ya podemos probar:

Teorema 8.20 *Si V es un espacio simpléctico, el grupo $\mathrm{SpP}(V)$ es simple excepto en los casos $\mathrm{Sp}(2,2)$, $\mathrm{Sp}(2,3)$ y $\mathrm{Sp}(4,2)$.*

Demostración: Aplicamos el teorema de Iwasawa. Hemos demostrado que $\mathrm{SpP}(V)$ es un grupo de permutaciones primitivo sobre $P(V)$ que coincide con su derivado. Si $Q = \langle z \rangle \in P(V)$, el estabilizador $\mathrm{SpP}(V)_Q$ contiene el subgrupo

$$A_Q = \{T_{z,\alpha} \mid \alpha \in C\} \cong C,$$

luego es abeliano, y claramente es normal en el estabilizador, pues si $f(Q) = Q$ es que $f(z) = \beta z$, luego $T^f_{z,\alpha} = T_{\beta z,\alpha} = T_{z,\alpha\beta^2} \in A_Q$, y la envoltura normal de A_Q contiene a todas las transvecciones simplécticas, luego es todo el grupo $\mathrm{SpP}(V)$. ■

Grupos simplécticos sobre cuerpos finitos Recordemos que hemos llamado $\mathrm{Sp}(2m,q)$ al grupo simpléctico de cualquier espacio simpléctico de dimensión $2m$ sobre el cuerpo de q elementos, que claramente es un grupo finito. Vamos a calcular su orden. Para ello basta observar que si V es un espacio simpléctico de dimensión $2m$, podemos fijar en él una *base simpléctica,*, es decir, una base formada por pares hiperbólicos $(u_1, v_1, \ldots, u_m, v_m)$. Un automorfismo de V está en $\mathrm{Sp}(2m,q)$ si y sólo si transforma esta base en otra base simpléctica, luego hay tantos elementos en $\mathrm{Sp}(2m,q)$ como bases simplécticas.

Hay $q^{2m}-1$ vectores no nulos en V, y cualquiera de ellos sirve como primer vector u_1 de una base simpléctica. Como $|\langle u_1\rangle^\perp| = q^{2m-1}$, hay $q^{2m}-q^{2m-1}$ vectores v que cumplen $F(u_1,v)\neq 0$, divididos en clases de $q-1$ vectores linealmente dependientes, de modo que en cada clase hay uno solo que cumple $F(u_1,v)=1$, luego hay

$$\frac{q^{2m}-q^{2m-1}}{q-1} = q^{2m-1}$$

posibilidades para elegir un vector v_1 que forme un par hiperbólico (u_1,v_1), luego en total tenemos $(q^{2m}-1)q^{2m-1}$ pares hiperbólicos en V. Llamando $H_1 = \langle u_1, v_1\rangle$, el espacio $H_1^\perp$ tiene dimensión $2(m-1)$, luego en él tenemos $(q^{2(m-1)}-1)q^{2(m-1)-1}$ posibilidades para elegir un segundo par hiperbólico (u_2,v_2). Repitiendo el proceso m veces, llegamos a que el número de bases simplécticas es

$$(q^{2m}-1)q^{2m-1}(q^{2(m-1)}-1)q^{2(m-1)-1}\cdots = q^{\sum_{i=1}^{m} 2i-1}\prod_{i=1}^{m}(q^{2i}-1).$$

En definitiva:

$$|\mathrm{Sp}(2m,q)| = q^{m^2}\prod_{i=1}^{m}(q^{2i}-1),$$

y a su vez:

$$|\mathrm{SpP}(2m,q)| = \frac{q^{m^2}}{(2,q-1)}\prod_{i=1}^{m}(q^{2i}-1).$$

El teorema 8.12 nos da que $\mathrm{SpP}(2,q)\cong \mathrm{LEP}(2,q)$. En particular

$$\mathrm{SpP}(2,2)\cong \mathrm{LEP}(2,2)\cong \Sigma_3, \qquad \mathrm{SpP}(2,3)\cong \mathrm{LEP}(2,2)\cong A_4,$$

y vamos a probar a continuación que

$$\mathrm{SpP}(4,2)\cong \Sigma_6,$$

con lo que todas excepciones del teorema 8.20 están justificadas. La fórmula para el orden que hemos obtenido muestra que ambos grupos tienen el mismo orden, luego basta probar que $\mathrm{SpP}(4,2)$ contiene un subgrupo isomorfo a Σ_6. Más en general:

Teorema 8.21 *Si $m\geq 2$, el grupo $\mathrm{SpP}(2m,2)$ contiene un subgrupo isomorfo a Σ_{2m+2}.*

DEMOSTRACIÓN: Sea Ω un conjunto con $2m+2$ elementos y sea V el conjunto de todos los pares $\{\Gamma, \Delta\}$ tales que

$$\Omega = \Gamma \cup \Delta, \qquad \Gamma \cap \Delta = \varnothing, \qquad 2 \mid |\Gamma|.$$

Observemos que $|V| = 2^{2m}$, pues V tiene 2^{2m+1} subconjuntos Γ de cardinal par (fijado $x \in \Omega$, cada subconjunto $A \subset \Omega \backslash \{x\}$ determina un único subconjunto de Ω de cardinal par, a saber, A o bien $A \cup \{x\}$). Porlo tanto, hay 2^{2m+1} pares ordenados (Γ, Δ) y 2^{2m} pares desordenados $\{\Gamma, \Delta\}$.

Consideramos en V la suma dada por

$$\{\Gamma_1, \Delta_1\} + \{\Gamma_2, \Delta_2\} = \{\Gamma_1 \triangle \Gamma_2, \Gamma_1 \triangle \Delta_2\},$$

donde $A \triangle B = (A \cup B) \setminus (A \cap B)$ es la diferencia simétrica de conjuntos.

Notemos que esta suma está bien definida, pues si tomamos cualquier elemento de un sumando y cualquier elemento del otro, los puntos que están en ambos o en ninguno forman uno de los conjuntos de la suma. Además, los cuatro subconjuntos que muestra la figura, tienen todos cardinal par o todos cardinal impar, por lo que la suma está formada por conjuntos de cardinal par.

	Γ_2	Δ_2
Γ_1	Γ	Δ
Δ_1	Δ	Γ

Es fácil ver que con esta operación V se convierte en un grupo abeliano con neutro $\{\varnothing, \Omega\}$ en el que todos los elementos no triviales tienen orden 2, y esto hace que admita una estructura obvia de espacio vectorial sobre el cuerpo $C = \mathbb{Z}/2\mathbb{Z}$ de dos elementos. Teniendo en cuenta el cardinal de V, su dimensión tiene que ser $2m$. Definimos

$$F(\{\Gamma_1, \Delta_1\}, \{\Gamma_2, \Delta_2\}) = |\Gamma_1 \cap \Gamma_2| + 2\mathbb{Z},$$

y se comprueba que F es una forma bilineal alternada no degenerada en V.

Cada $\sigma \in \Sigma_{2m+2}$ define un automorfismo de V dado por

$$\sigma(\{\Gamma, \Delta\}) = \{\sigma[\Gamma], \sigma[\Delta]\},$$

y es fácil ver que es una isometría. Tenemos así un homomorfismo

$$\Sigma_{2m+2} \longrightarrow \mathrm{Sp}(2m, 2)$$

que, de hecho es un monomorfismo, pues si σ fija a todas las particiones, para cada par de elementos $x, y \in \Omega$, se tiene que cumplir que $\sigma(\{x, y\}) = \{x, y\}$ y, aplicando esto a dos pares $\{x, y\}$, $\{x, z\}$, vemos que $\sigma(x) = x$, para todo $x \in \Omega$.

■

Dejando de lado los grupos $\mathrm{SpP}(2,q)$, que nos dan grupos de tipo $\mathrm{LEP}(2,q)$, que ya conocíamos, los siguientes tienen órdenes muy grandes. Los menores son

$$|\mathrm{SpP}(4,3)| = 25\,920, \qquad |\mathrm{SpP}(4,4)| = 979\,200, \qquad |\mathrm{SpP}(6,2)| = 1\,451\,520.$$

8.3 Espacios cuadráticos y unitarios

El resto del capítulo lo dedicamos a introducir los resultados geométricos necesarios para estudiar las dos familias restantes de grupos simples clásicos. De momento volvemos al caso general de un espacio vectorial dotado de una forma sesquilineal arbitraria.

La norma El concepto de norma en un espacio euclídeo admite la generalización siguiente a nuestro contexto:

Definición 8.22 Si V es un espacio dotado de una forma sesquilineal, definimos la *norma* $\mathrm{N} : V \longrightarrow R$ dada por

$$\mathrm{N}(v) = F(v,v).$$

Los vectores no nulos de norma nula se llaman *isótropos,* mientras que los vectores que no son isótropos (el 0 y los vectores de norma no nula) se llaman *anisótropos.*

Consideremos con más detalle la norma en un espacio V dotado de una forma bilineal simétrica no degenerada. En primer lugar observamos que

$$\mathrm{N}(u+v) = F(u+v,u+v) = F(u,u)+F(v,v)+2F(u,v) = \mathrm{N}(u)+\mathrm{N}(v)+2F(u,v).$$

Si la característica del cuerpo C no es 2, esto implica que la forma bilineal F está determinada por la norma N por la relación

$$F(u,v) = \frac{1}{2}(\mathrm{N}(u+v) - \mathrm{N}(u) - \mathrm{N}(v)).$$

Del mismo modo que en la definición de "espacio simpléctico" hemos tenido que sustituir el concepto de "forma bilineal antisimétrica" por el de "forma bilineal alternada" para que los resultados fueran aplicables al caso de espacios sobre cuerpos de característica 2, el hecho de que la expresión anterior no tenga sentido cuando el cuerpo de escalares tiene característica 2 nos obliga a restringir las formas bilineales simétricas que vamos a admitir en este caso. Para ello necesitamos un nuevo concepto:

Definimos una *forma cuadrática* en un C-espacio vectorial V como una aplicación $Q : V \longrightarrow C$ tal que, para todos los vectores $u, v \in V$,

$$Q(\alpha u + \beta v) = \alpha^2 Q(u) + \alpha\beta F(u,v) + \beta^2 Q(v),$$

donde $F(u,v)$ es una forma bilineal simétrica en V. Notemos que F está determinada por Q, pues

$$F(u,v) = Q(u+v) - Q(u) - Q(v).$$

Además, esta expresión muestra que F es necesariamente simétrica (de modo que la exigencia de que F sea simétrica es redundante en la definición de forma cuadrática).

Definición 8.23 Un *espacio unitario* es un par (V,F), donde V es un espacio vectorial y F es una forma bilineal hermitiana en V no degenerada.

Un *espacio cuadrático* en un par (V,Q), donde V es un espacio vectorial y Q es una forma cuadrática en V cuya forma bilineal asociada sea no degenerada.

Una *isometría* $f : (V,Q) \longrightarrow (W,Q')$ entre dos espacios cuadráticos es un isomorfismo $f : V \longrightarrow W$ de espacios vectoriales tal que $Q'(f(v)) = Q(v)$, para todo $v \in V$.

Así, para cuerpos C de característica distinta de 2, podríamos haber definido un espacio cuadrático como un par (V,F), donde F es una forma bilineal simétrica en V no degenerada, pues toda forma cuadrática determina una forma bilineal y viceversa, y las isometrías en el sentido que acabamos de definir coinciden con los isomorfismos que conservan la forma bilineal, en virtud de las relaciones

$$F(u,v) = Q(u+v) - Q(u) - Q(v), \qquad Q(u) = \frac{1}{2}F(u,u).$$

En cambio, la situación es muy diferente cuando el cuerpo C tiene característica 2. Si (V,Q) es un espacio cuadrático, la forma bilineal F asociada a Q no sólo es simétrica, sino que de hecho es alternada, pues

$$F(v,v) = Q(2v) - Q(v) - Q(v) = Q(0) + 2Q(v) = 0.$$

Así, (V,F) es un espacio simpléctico, pero dos espacios cuadráticos pueden ser isométricos como espacios simplécticos y no serlo como espacios cuadráticos, pues un isomorfismo puede conservar las formas bilineales y no las formas cuadráticas. (Véase la nota tras el teorema 8.32) Esto es otra forma de expresar que una misma forma bilineal alternada F puede ser inducida por varias formas cuadráticas que determinan espacios cuadráticos no isométricos.

En la práctica, siempre que consideremos un espacio cuadrático V, en él tendremos definida la forma bilineal F, la norma N y la forma cuadrática Q. Si la característica del cuerpo C no es 2, estos tres elementos se determinan mutuamente, mientras que si C tiene característica 2 tenemos que la forma cuadrática Q determina la forma bilineal F y que la norma N es nula, pues

$$\mathrm{N}(v) = F(v,v) = Q(2v) - 2Q(v) = 0.$$

En un espacio unitario definimos $Q = \mathrm{N}$.

Puesto que en un espacio cuadrático sobre un cuerpo de característica 2 todos los vectores son isótropos, conviene introducir el refinamiento siguiente:

Si V es un espacio cuadrático, un vector $v \in V$ es *singular* si es no nulo y $Q(v) = 0$ (lo que en característica distinta de 2 equivale a que sea isótropo). La misma definición es válida en los espacios unitarios, de modo que en ellos los vectores singulares coinciden también con los isótropos.

Veamos un primer resultado que no sería válido para espacios cuadráticos sobre cuerpos de característica 2 si los hubiéramos definido en términos de formas bilineales y no de formas cuadráticas. En realidad no es necesaria la regularidad de la forma bilineal, pero en el enunciado siguiente hay que sobrentender igualmente que en el caso simétrico la forma bilineal proviene de una forma cuadrática:

Teorema 8.24 *Si F es una forma bilineal simétrica/hermitiana no idénticamente nula en un espacio V, entonces existe $v \in V$ tal que $Q(v) \neq 0$.*

Demostración: Como F no es idénticamente nula, existen $u, v \in V$ tales que $F(u, v) \neq 0$ y, dividiendo u entre $F(u, v)$, podemos suponer que $F(u, v) = 1$. En el caso en que F es hermitiana, si fuera $F(v, v) = 0$ para todo $v \in V$, para todo $\alpha \in C$ tendríamos que

$$0 = F(u + \alpha v, u + \alpha v) = \alpha + \bar{\alpha}.$$

Esto significa que $\mathrm{Tr}(\alpha) = 0$ para todo $\alpha \in C$, en contra de 8.2, donde hemos visto que la traza es suprayectiva.

Si F es bilineal simétrica la conclusión es obvia, pues tenemos que

$$Q(u + v) - Q(u) - Q(v) = 1,$$

luego al menos uno de los vectores $u + v, u, v$ tiene que ser no singular. ∎

Un conjunto de vectores $v_1, \ldots, v_r$ en un espacio cuadrático/unitario es *ortogonal* si cumple que $v_i \perp v_j$ si y sólo si $i \neq j$ (en particular, esto supone que ninguno de ellos es isótropo). El conjunto es *ortonormal* si además cumple $\mathrm{N}(v_i) = 1$.

Todo conjunto ortogonal es linealmente independiente, pues si tenemos una combinación lineal

$$\alpha_1 v_1 + \cdots + \alpha_r v_r = 0,$$

basta aplicar $F(-, v_i)$ para concluir que $\alpha_i = 0$. Más aún, en tal caso el subespacio $W = \langle v_1, \ldots, v_r \rangle$ no es degenerado, pues la matriz en la base ortogonal de la restricción de F a W es diagonal con coeficientes no nulos en la diagonal, luego tiene determinante no nulo.

Teorema 8.25 *En un espacio cuadrático/unitario (salvo en un espacio cuadrático sobre un cuerpo de característica 2) todo conjunto ortogonal se extiende a una base ortogonal.*

DEMOSTRACIÓN: Si $v_1, \ldots, v_r$ es un conjunto ortogonal de vectores en un espacio V, entonces $V_r = \langle v_1, \ldots, v_r \rangle$ es un subespacio no degenerado, luego $V = V_r \oplus V_r^\perp$ y $V_r^\perp$ es no degenerado, luego, si no es nulo, por el teorema anterior contiene un vector v_{r+1} de norma no nula (aquí usamos que, salvo en el caso exceptuado, $Q(v) \neq 0$ equivale a $\mathrm{N}(v) \neq 0$). Es claro entonces que $v_1, \ldots, v_{r+1}$ es un conjunto ortogonal. Repitiendo el proceso un número finito de veces obtenemos una base ortogonal. ∎

Observemos que en un espacio cuadrático sobre un cuerpo de característica 2 no puede haber bases ortogonales, ni siquiera relajando la condición $\mathrm{N}(v_i) \neq 0$ a $Q(v_i) \neq 0$, pues la matriz de F respecto de una base ortogonal sería nula, luego la forma F sería degenerada.

Planos hiperbólicos Vamos a ver que cualquier espacio cuadrático / unitario (incluyendo el caso en que el cuerpo tiene característica 2) admite una descomposición en suma ortogonal de planos hiperbólicos similar a la que hemos encontrado para los espacios simplécticos, aunque ahora tenemos que introducir precisiones adicionales que no tenían sentido en el caso simpléctico, en el que todos los vectores son isótropos.

Definición 8.26 Un par de vectores (u, v) en un espacio cuadrático/unitario V forman un *par hiperbólico* si $Q(u) = Q(v) = 0$ y $F(u, v) = 1$. Un *plano hiperbólico* es un subespacio $H = \langle u, v \rangle$ de V generado por un par hiperbólico.

Notemos que las componentes de un par hiperbólico son linealmente independientes, pues si fuera $v = \lambda u$ sería $F(u, v) = 0$, luego los planos hiperbólicos son realmente planos (tienen dimensión 2). La matriz de la restricción de F respecto de la base formada por el par hiperbólico es

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

que tiene determinante no nulo, luego los planos hiperbólicos son subespacios no degenerados.

Si V es un espacio cuadrático/hermitiano, un subespacio $W \leq V$ se dice *isótropo/singular* si contiene vectores isótropos/singulares, *anisótropo/no singular* si no contiene vectores isótropos/singulares y *totalmente isótropo/totalmente singular* si todos sus vectores no nulos son isótropos/singulares. Por 8.24, un subespacio W es totalmente singular si y sólo si F se restringe a la forma nula sobre W.

Teorema 8.27 *Si V es un espacio cuadrático/unitario y $u_1, \ldots, u_r$ son una base de un subespacio de V totalmente singular, existen $v_1, \ldots, v_r \in V$ tales que*

$$\langle u_1, v_1 \rangle \perp \cdots \perp \langle u_r, v_r \rangle$$

y los pares (u_i, v_i) son hiperbólicos.

DEMOSTRACIÓN: Sea $X_1 = \langle u_1, \ldots, u_r\rangle$ y $X_2 = \langle u_2, \ldots, u_r\rangle$. Entonces $X_2 \leq X_1$, luego $X_1^\perp < X_2^\perp$, y la inclusión es estricta porque las dimensiones son $n - r < n - r + 1$, donde n es la dimensión de V. Por lo tanto, podemos tomar $v \in X_2^\perp \setminus X_1^\perp$, que necesariamente cumplirá $F(u_1, v) \neq 0$. Dividiendo v entre este valor podemos exigir que $F(u_1, v) = 1$.

Consideremos ahora un vector de la forma $v_1 = \alpha u_1 + v \in X_2^\perp$. Claramente $F(u_1, v_1) = 1$, y queremos elegir α para que $Q(v_1) = 0$. En el caso cuadrático tenemos

$$Q(v_1) = Q(\alpha u_1) + Q(v) + F(\alpha u_1, v) = Q(v) - \alpha = 0,$$

luego basta tomar $\alpha = -Q(v)$. En el caso unitario es

$$Q(v_1) = \mathrm{N}(v_1) = \alpha + \bar{\alpha} + \mathrm{N}(v) = 0,$$

que equivale a $\mathrm{Tr}(\alpha) - \mathrm{N}(v)$ y la traza es suprayectiva por 8.2, luego también podemos tomar $\alpha \in C$ de modo que $Q(v_1) = 0$.

En ambos casos $\langle u_1, v_1\rangle \leq X_2^\perp$ es un plano hiperbólico. Equivalentemente, tenemos que $X_2 \leq V_2 = \langle u_1, v_1\rangle^\perp$, y podemos repetir el argumento en V_2 para obtener otro plano hiperbólico $\langle u_2, v_2\rangle \leq V_2$ que forma una suma ortogonal $\langle u_1, v_1\rangle \perp \langle u_2, v_2\rangle$ y así, tras r pasos, llegamos a la suma ortogonal del enunciado. ∎

En particular, el teorema anterior para $r = 1$ afirma que si V es un espacio cuadrático/unitario y $u \in V$ es un vector singular, existe $v \in V$ tal que (u, v) es un par hiperbólico. Esto nos da a su vez el teorema siguiente:

Teorema 8.28 *Todo espacio cuadrático/unitario V se puede expresar en la forma*

$$V = H_1 \perp \cdots \perp H_m \perp W,$$

donde los H_i son planos hiperbólicos y W es un subespacio no singular.

DEMOSTRACIÓN: Si V no posee vectores singulares, basta tomar $m = 0$ y $W = V$. Si u_1 es un vector singular, por el teorema anterior existe $v_1 \in V$ tal que $H_1 = \langle u_1, v_1\rangle$ es un plano hiperbólico. En particular es no degenerado, luego $V = H_1 \perp H_1^\perp$. Ahora basta repetir el proceso con $H_1^\perp$ en lugar de V. ∎

Un resultado fundamental y que no es obvio en absoluto es que el número m que aparece en la descomposición del teorema anterior está unívocamente determinado por el espacio V, es decir, que un mismo espacio no puede admitir dos descomposiciones del tipo indicado en el teorema para distintos valores de m. Probaremos esto a partir de un resultado más general:

Teorema 8.29 (Witt) *Si V es un espacio cuadrático/unitario y $f : U_1 \longrightarrow U_2$ es una isometría entre dos subespacios de V, entonces f se extiende a una isometría $g : V \longrightarrow V$.*

DEMOSTRACIÓN: Notemos que no exigimos que los subespacios U_i sean no degenerados. Sea $n = \dim V$ y $d = \dim U_i$. Probaremos el teorema por inducción sobre d. Si $d = 0$ basta tomar como g la identidad en V.

Sea $H \leq U_1$ cualquier subespacio de dimensión $d-1$. Por hipótesis de inducción $f|_H$ se extiende a una isometría $h : V \longrightarrow V$. Sea $f^* = f \circ h^{-1} : U_1 \longrightarrow h^{-1}[U_2]$, que es una isometría entre dos subespacios de V. Si probamos que f^* se extiende a una isometría g^*, entonces $h \circ g$ será una isometría de V que extenderá a f, luego no perdemos generalidad si suponemos que $f|_H = 1|_H$.

En particular $f[H] = H$, luego $H \leq U_1 \cap U_2$. Si $f|_{U_1} = 1|_{U_1}$, basta tomar $g = 1_V$, luego podemos suponer que f no deja invariantes a todos los vectores de U_1. Así

$$U_1 = H \oplus \langle u_1 \rangle, \qquad U_2 = H \oplus \langle u_2 \rangle,$$

con $f(u_1) = u_2 \neq u_1$. Equivalentemente, si llamamos $P = \mathrm{Im}(f-1)$, tenemos que $P = \langle u_2 - u_1 \rangle$ tiene dimensión 1. Observemos ahora que si $u, v \in U_1$, se cumple

$$F(f(u), f(v) - v) = F(f(u), f(v)) - F(f(u), v) =$$
$$F(u, v) - F(f(u), v) = F(u - f(u), v).$$

En particular $H \leq P^\perp$, pues si $u \in H$, queda $F(u, f(v) - v) = 0$, donde $f(v) - v$ recorre P. Además, $U_1 \leq P^\perp$ si y sólo si $U_2 \leq P^\perp$, pues si $U_1 \leq P^\perp$ tenemos que $F(f(u), f(v) - v) = F(u - f(u), v) = 0$, donde $f(u)$ recorre U_2 y $f(v) - v$ recorre P, luego $U_2 \leq P^\perp$, e igualmente se prueba el recíproco.

Supongamos en primer lugar que $U_i \not\leq P^\perp$. Como $H \leq P^\perp$, esto implica que

$$U_1 \cap P^\perp = U_2 \cap P^\perp = H.$$

Tomemos W tal que $P^\perp = H \oplus W$ y veamos que $V = U_i \oplus W$. En efecto, por una parte, si $v \in U_1 \cap W \leq U_I \cap P^\perp = H$, resulta que $v \in H \cap W = 0$, de modo que $U_i \cap W = 0$ y $\dim W = \dim P^\perp - \dim H = n - 1 - (d-1)$, luego $\dim(U_1 \oplus W) = d + n - d = n$, luego $U_i \oplus W = V$.

Por otro lado, si $u \in U_1$ y $w \in W$, tenemos que $F(f(u) - u, w) = 0$, pues $f(u) - u \in P$ y $w \in W \leq P^\perp$, luego

$$F(f(u), w) = F(u, w).$$

De aquí se sigue que el isomorfismo $g : V \longrightarrow V$ que sobre U_1 coincide con f y sobre W es la identidad es una isometría, pues la matriz de F respecto de una base de V formada por una base de U_1 unida a una base de W es la misma que su matriz respecto de la imagen de dicha base.

A partir de aquí suponemos que $U_1, U_2 \leq P^\perp$. Recordemos que $P = \langle p \rangle$, donde $p = u_2 - u_1$, y ahora tenemos que p es isótropo, pues

$$F(p, p) = F(u_2, p) - F(u_1, p) = 0.$$

Más aún, en el caso cuadrático tenemos que

$$Q(f(u_1)) = Q(u_2) = Q(u_1) + Q(p) + F(u_1, p) = Q(u_1) + Q(p),$$

luego $Q(p) = 0$.

Supongamos que $U_1 \neq U_2$, de modo que, según teníamos,

$$U_1 = H \oplus \langle u_1 \rangle\,, \qquad U_2 = H \oplus \langle u_2 \rangle$$

y ahora $X = \langle u_1 + u_2 \rangle \neq 0$. Tenemos que

$$U_1 + U_2 = U_1 \oplus X = U_2 \oplus X,$$

pues si $u \in U_1 \cap X$, entonces $u = \alpha(u_1 + u_2)$, luego $u_2 \in U_1$ salvo si $\alpha = 0$, luego la suma $U_1 \oplus X$ es directa, y claramente contiene a U_1 y U_2, luego es $U_1 + U_2$, e igualmente se razona con U_2. Sea W tal que $P^\perp = (U_1 + U_2) \oplus W$ y llamemos $S = W + X$. Entonces

$$P^\perp = U_1 \oplus S = U_2 \oplus S.$$

En efecto, si $v \in U_i \cap S$, entonces $v = w + x \in U_i$, con $w \in W$, $x \in X$, luego $w \in (U_1 + U_2) \cap W = 0$, luego $v \in U_i \cap X = 0$. Por lo tanto la suma $U_i \oplus S$ es directa y, como contiene a U_1, U_2 y a W, tiene que ser $P^\perp$.

Por otra parte, si $s \in S$ y $u \in U_1$, tenemos que $u - f(u) \in P$, luego $F(u - f(u), s) = 0$, luego $F(f(u), s) = F(u, s)$ y, como antes, esto implica que podemos extender f a una isometría $f^* : P^\perp \longrightarrow P^\perp$.

El argumento se simplifica si $U_1 = U_2$, pues podemos descomponer directamente $P^\perp = U_1 \oplus S$ y sigue cumpliéndose que $F(f(u), s) = F(u, s)$, luego también tenemos la extensión a $P^\perp$.

Así pues, basta con probar que toda isometría de $P^\perp$ en sí mismo puede extenderse a V o, equivalentemente, no perdemos generalidad si suponemos que $U_1 = U_2 = P^\perp$ es un hiperplano de V (al que llamaremos U). Todo el razonamiento visto hasta aquí sigue siendo válido con esta hipótesis adicional. En particular tenemos que $P = \langle p \rangle$, con p singular.

Sea $l \in V \setminus U$ y sea $L = \langle p, l \rangle$, de modo que $F(p, l) \neq 0$, por lo que la matriz de F en la base p, l tiene determinante $-F(p, l)^2 \neq 0$, y así L es un subespacio de V no degenerado. Como $p \in L$ es singular, el teorema 8.27 nos da que existe $q \in L$ tal que (p, q) es un par hiperbólico, y $L = \langle p, q \rangle$ es un plano hiperbólico.

Por construcción L no está contenido en U, luego tiene que ser $q \notin U$, y así $V = U \oplus \langle q \rangle$.

Como $\langle p \rangle < L$, tenemos que $L^\perp$ es un hiperplano de $U = \langle p \rangle^\perp$. Como $\langle q \rangle$ no está contenido en U, resulta que $\langle q \rangle^\perp$ es un hiperplano de V que no contiene a U, luego $\langle q \rangle^\perp \cap U$ es un hiperplano de U que contiene a $L^\perp$, luego tiene que ser $\langle q \rangle^\perp \cap U = L^\perp$. Más aún, $U = L^\perp \oplus \langle p \rangle$, ya que $F(p, q) = 1$, luego $p \notin L^\perp$.

Como $q \notin U = f[U]$, en particular $q \notin f[L^\perp]$, luego $\langle q \rangle + f[L^\perp]$ es un hiperplano de V que no contiene a $f(p)$ (porque $p \notin L^\perp$, ya que $F(p, q) = 1$), luego $(\langle q \rangle + f[L^\perp])^\perp = \langle q' \rangle$, para cierto $q' \in V$, de modo que $\langle q \rangle + f[L^\perp] = \langle q' \rangle^\perp$, y a su vez $f[L^\perp] = \langle f(p), q' \rangle^\perp$, pues, como $p \in L$, tenemos que $L^\perp \leq \langle p \rangle$ y $f[L^\perp] \leq \langle f(p) \rangle^\perp$, luego de hecho $f[L^\perp] \leq \langle f(p), q' \rangle^\perp$, y ambos subespacios tienen dimensión $n - 2$.

Como $F(f(p), q') \neq 0$ y $f(p)$ es singular, tenemos que $\langle f(p), q' \rangle$ es no degenerado y, por el teorema 8.27, existe q'' tal que $\langle f(p), q' \rangle = \langle f(p), q'' \rangle$ y $(f(p), q'')$

es un par hiperbólico. En particular,

$$f[L^\perp] = \langle f(p), q'' \rangle .$$

Notemos que $q'' \notin U$, pues en tal caso

$$1 = F(f(p), q'') = F(p, f^{-1}(q'')) = 0,$$

ya que $U = \langle p \rangle^\perp$. Por lo tanto $V = U \oplus \langle q \rangle = U \oplus \langle q'' \rangle$, y tenemos la isometría $f : U \longrightarrow U$, así como la isometría $f^* : \langle q \rangle \longrightarrow \langle q'' \rangle$ dada por $g(q) = q''$ (ya que ambos vectores son singulares). Para probar que f y f^* determinan una isometría $g : V \longrightarrow V$, teniendo en cuenta que $U = L^\perp \oplus \langle p \rangle$, basta observar que

$$F(f(p), f^*(q)) = 1 = F(p, q),$$

así como que si $x \in L^\perp$, entonces

$$F(f(x), f^*(q)) = 0 = F(x, q).$$

Esto hace que F tenga la misma matriz en una base de V formada por una base de $L^\perp$ extendida con $\{p, q\}$ que en la imagen por g de dicha base. ∎

Definición 8.30 Si V es un espacio cuadrático/unitario, definimos el *índice de Witt* de V como la mayor dimensión m de un subespacio de V totalmente singular.

El teorema de Witt implica que todo subespacio totalmente singular U_1 de V puede extenderse a uno de dimensión m. En efecto, basta tomar un subespacio totalmente singular U de V de dimensión m y tomar un subespacio U_2 con $\dim U_2 = \dim U_1$, y así cualquier isomorfismo $f : U_1 \longrightarrow U_2$ es una isometría (pues F es idénticamente nula en ambos subespacios). Por el teorema de Witt podemos extenderla a una isometría $g : V \longrightarrow V$, de modo que $g^{-1}[U]$ es un subespacio totalmente singular de V que contiene a U_1.

En otras palabras, el índice de Witt es la dimensión de todos los subespacios de V totalmente singulares maximales para la inclusión.

Teorema 8.31 *En la condiciones del teorema* 8.28, el índice de Witt de V es precisamente m.

Demostración: Observemos en primer lugar que V no puede admitir dos descomposiciones en las condiciones del teorema 8.28 con diferentes valores de m. En efecto, si fuera

$$V = H_1 \perp \cdots \perp H_m \perp W = H'_1 \perp \cdots \perp H'_{m'} \perp W'$$

con $m < m'$, podemos definir una isometría

$$f : H_1 \perp \cdots \perp H_m \longrightarrow H'_1 \perp \cdots \perp H'_m$$

tal que $f[H_i] = H'_i$, la cual, por el teorema de Witt, se extiende a otra isometría $g : V \longrightarrow V$ tal que $g[H_i] = H'_i$, para $i = 1, \ldots, m$.

Entonces

$$g[W] = g[(H_1 \perp \cdots \perp H_m)^\perp] = (H'_1 \perp \cdots \perp H'_m)^\perp =$$

$$H'_{m+1} \perp \cdots \perp H'_{m'} \perp W',$$

luego W contiene vectores singulares (las antiimágenes de los vectores singulares de H'_m), y tenemos una contradicción.

A partir de una descomposición en las condiciones del teorema 8.28, tomando un vector singular de cada plano hiperbólico, obtenemos la base de un subespacio totalmente singular de dimensión m, luego m es menor o igual que el índice de Witt de V, pero el teorema 8.27 nos permite construir un subespacio

$$H_1 \perp \cdots \perp H_m \leq V,$$

donde m es el índice de Witt y cada H_i es un plano hiperbólico. Llamando W al complemento ortogonal de este subespacio, tenemos que

$$V = H_1 \perp \cdots \perp H_m \perp W,$$

y no puede suceder que W contenga vectores singulares, pues entonces podríamos obtener una descomposición de V en las condiciones del teorema 8.27 con más de m planos hiperbólicos, y ya hemos visto que eso no es posible. ∎

Planos cuadráticos no singulares En la sección siguiente veremos que, cuando el cuerpo de escalares es finito, todo plano unitario es un plano hiperbólico, mientras que existen planos cuadráticos sin vectores singulares, con lo que no son planos hiperbólicos. Vamos a describirlos aquí (sin suponer que el cuerpo de escalares sea finito).

Sea, pues, V un espacio cuadrático de dimensión 2 que no tenga vectores singulares. Tomemos $u \in V$ no nulo, de modo que $Q(u) = \alpha \neq 0$. Ahora observamos que $Q^* = \alpha^{-1}Q$ es también una forma cuadrática en V cuya forma bilineal asociada es $F^* = \alpha^{-1}F$. Equivalentemente, tenemos que $Q = \alpha Q^*$, donde $Q^*(u) = 1$. Vamos a describir Q^* o, equivalentemente, podemos suponer que $Q(u) = 1$.

Tomemos una base $V = \langle u, v\rangle$, donde podemos exigir que $F(u, v) = 1$. En efecto, si la característica del cuerpo C de escalares es 2, necesariamente $F(u, v) \neq 0$, pues se cumple $F(u, u) = F(v, v) = 0$ y en caso contrario F sería idénticamente nula, luego degenerada, y cambiando v por un múltiplo adecuado podemos exigir que $F(u, v) = 1$. Si la característica de C es distinta de 2, por 8.25 poemos tomar una base ortogonal u, w y usamos que

$$F(u, au + w) = aF(u, u) = 2a,$$

luego $v = (1/2)u + w$ cumple lo requerido. Así, cualquiera que sea la característica de C, tenemos que $V = \langle u, v\rangle$ de modo que

$$Q(xu + yv) = x^2 + xy + ay^2,$$

donde $a = Q(v)$. El polinomio $x^2 + x + a$ tiene que ser irreducible en $C[x]$, pues si ω fuera una raíz, $\omega u + v$ sería un vector singular en V. Sea K una extensión de C donde dicho polinomio tenga una raíz ω. Podemos suponer que $K = C[\omega]$. Si $\bar{\omega}$ es la otra raíz del polinomio, tenemos que

$$x^2 + x + a = (x - \omega)(x - \bar{\omega}) = x^2 - (\omega + \bar{\omega})x + \omega\bar{\omega}.$$

Por lo tanto, $\omega + \bar{\omega} = -1$, $\omega\bar{\omega} = a$. La primera igualdad implica que $\omega \neq \bar{\omega}$, pues de lo contrario $\omega = -1/2 \in C$. Por lo tanto, la extensión K/C tiene un C-automorfismo de orden 2 que podemos representar por $\xi \mapsto \bar{\xi}$, que determina una norma y una traza:

$$\mathrm{N} : K \longrightarrow C, \qquad \mathrm{Tr} : K \longrightarrow C.$$

Observemos que

$$\mathrm{N}(x + y\omega) = (x + y\omega)(x + y\bar{\omega}) = x^2 - xy + ay^2.$$

Por lo tanto, K es un C-espacio vectorial de dimensión 2, y el isomorfismo (de espacios vectoriales) $f : V \longrightarrow K$ dado por

$$f(u) = 1, \qquad f(v) = -\omega$$

hace corresponder la forma cuadrática Q se corresponde con la forma que sobre $\xi = x + y\omega$ actúa como

$$Q(f^{-1}(\xi)) = Q(xu - yv) = x^2 - xy + ay^2 = \mathrm{N}(\xi).$$

Notemos que, ciertamente, el cuerpo K no tiene vectores singulares, pues la norma sólo se anula en el vector nulo. Con esto hemos probado:

Teorema 8.32 *Todo plano cuadrático no singular sobre un cuerpo C es isométrico al espacio cuadrático determinado por un cuerpo $K = C(\omega)$, donde ω es raíz de un polinomio x^2+x+a irreducible en $C[x]$, dotado de la forma cuadrática $Q(\xi) = \alpha\,\mathrm{N}(\xi)$, para cierto $\alpha \in C$.*

Así, por ejemplo, si C es algebraicamente cerrado, no puede haber planos cuadráticos no singulares. Por el contrario, en la sección siguiente veremos que si C es un cuerpo finito existe, salvo isometría, un único plano cuadrático no singular.

Nota Observemos que, respecto de la base $1, \omega$ de K, la forma cuadrática viene dada explícitamente por

$$Q(x + y\omega) = \alpha(x^2 - xy + ay^2).$$

Por el contrario, en un plano hiperbólico, respecto de la base formada por un par hiperbólico (u, v), la forma cuadrática es

$$Q(xu + yv) = xy.$$

Obviamente, un plano hiperbólico y un plano no singular no son isométricos (como espacios cuadráticos), pero si la característica de C es 2, la matriz de la forma bilineal en las bases correspondientes es en ambos casos (tomando $\alpha = 1$)

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

por lo que tenemos así un ejemplo de dos espacios cuadráticos isométricos como espacios simplécticos que no lo son como espacios cuadráticos. ∎

8.4 Espacios sobre cuerpos finitos

Veamos ahora algunos resultados adicionales que podemos probar sobre los espacios cuadráticos y unitarios cuando el cuerpo de escalares C es finito. Empezamos con el caso unitario, que es más sencillo:

Espacios unitarios sobre cuerpos finitos Si C es el cuerpo de p^m elementos, todo automorfismo de C fija a su cuerpo primo P (el cuerpo de p elementos), luego $\mathrm{Aut}(C)$ es el grupo de Galois de la extensión C/P, que es de Galois por [Al 9.1] y, según este mismo teorema, el grupo es cíclico de orden m, luego C tendrá un (único) automorfismo de orden 2 si y sólo si $m = 2e$ es par. Tomémoslo así y llamemos R al cuerpo de $q = p^e$ elementos, de modo que $|C : R| = 2$ y R es el cuerpo fijado por el único automorfismo de orden 2 de C, al que representaremos por $\alpha \mapsto \bar{\alpha}$. Específicamente la conjugación es σ^e, donde σ es el automorfismo de Frobenius, luego $\bar{\alpha} = \alpha^{p^e} = \alpha^q$.

Vamos a usar a menudo el hecho siguiente, que es un caso particular del teorema [Al 9.3] (notemos que la norma de la extensión C/R es la dada por $\mathrm{N}(\alpha) = \alpha\bar{\alpha} = \alpha^{q+1}$):

Teorema 8.33 *Sea R el cuerpo de q elementos y C el de q^2 elementos. Entonces, para cada $\beta \in R^*$, existen exactamente $q+1$ elementos $\alpha \in C$ tales que $\alpha^{q+1} = \beta$.*

Demostración: Basta probar que el homomorfismo $C^* \longrightarrow R^*$ dado por $\alpha \mapsto \alpha^{q+1}$ es suprayectivo, pues entonces su núcleo tendrá $(q^2-1)/(q-1) = q+1$ elementos y cada elemento $\beta \in R^*$ tendrá $q+1$ antiimágenes.

En efecto, C^* es un grupo cíclico de orden q^2-1. Sea g un generador. Un $\alpha \in R^*$ será de la forma $\alpha = g^r$ y, por otra parte, $\alpha^q = \bar{\alpha} = \alpha$, luego $\alpha^{q-1} = 1$, luego $g^{r(q-1)} = 1$, luego $q^2 - 1 \mid r(q-1)$, luego $q+1 \mid r$, luego $r = s(q+1)$ y así $\alpha = (g^s)^{q+1}$. ∎

Si V es un espacio unitario sobre un cuerpo finito C y $v \in V$ tiene norma no nula, por 8.33 existe un $\alpha \in C^*$ tal que $\alpha\bar{\alpha} = \alpha^{q+1} = F(v,v)$, con lo que $w = \alpha^{-1}v$ cumple $\mathrm{N}(w) = \alpha^{-1}\bar{\alpha}^{-1}F(v,v) = 1$ y $v = \alpha w$.

Así pues: todo vector de norma no nula es múltiplo de un vector de norma 1. Más precisamente, cada vector v de norma 1 tiene q^2-1 múltiplos no nulos αv,

de modo que $\mathrm{N}(\alpha v) = \alpha^{q+1}$, y por 8.33 vemos que exactamente $q+1$ múltiplos tienen también norma 1.

Teorema 8.34 *Todo espacio unitario sobre un cuerpo finito admite una base ortonormal, luego todos los espacios unitarios de una misma dimensión son isométricos.*

Demostración: Si V_1 y V_2 son espacios unitarios de la misma dimensión, en una base ortogonal de cada uno de ellos podemos sustituir cada vector por un múltiplo de norma 1 y así obtenemos bases ortonormales, con lo que el isomorfismo que hace corresponder una base con la otra es una isometría. ∎

El teorema siguiente muestra que todo espacio unitario de dimensión mayor que 1 sobre un cuerpo finito contiene necesariamente vectores isótropos:

Teorema 8.35 *Un espacio unitario de dimensión n sobre el cuerpo de q^2 elementos contiene*

$$z_n = (q^n - (-1)^n)(q^{n-1} + (-1)^n)$$

vectores isótropos y

$$y_n = q^{n-1}(q^n - (-1)^n).$$

vectores de norma 1.

Demostración: Si llamamos y_n al número de elementos de V de norma 1, vemos que cada $q+1$ de ellos generan un mismo subespacio vectorial de dimensión 1, el cual contiene q^2-1 elementos no nulos (de norma no nula), luego hay un total de $y_n/(q+1)$ subespacios con un total de $(q-1)y_n$ vectores de norma no nula. Si llamamos z_n al número de vectores isótropos de V, resulta que

$$q^{2n} = 1 + z_n + (q-1)y_n. \tag{8.1}$$

Ahora razonamos por inducción sobre n. Sea V_{n+1} un espacio unitario de dimensión $n+1$, fijemos una base ortonormal $e_1, \ldots, e_{n+1}$ y llamamos V_n al subespacio generado por $e_1, \ldots, e_n$ con la restricción del producto escalar de V_{n+1}. Todas las coordenadas que vamos a considerar serán respecto de estas bases. Fijemos un vector isótropo de V_{n+1}, lo cual equivale a que sus coordenadas cumplen

$$x_1\bar{x}_1 + \cdots + x_n\bar{x}_n + x_{n+1}\bar{x}_{n+1} = 0.$$

Distinguimos dos casos: si el vector de V_n de coordenadas $(x_1, \ldots, x_n)$ tiene norma nula, entonces la única posibilidad es que $x_{n+1} = 0$, luego hay z_n vectores en V_{n+1} en estas condiciones.

Si el vector de coordenadas $(x_1, \ldots, x_n)$ tiene norma no nula α, entonces

$$\alpha + x_{n+1}\bar{x}_{n+1} = \alpha + x_{n+1}^{q+1} = 0$$

y, como el núcleo de $x \mapsto x^{q+1}$ tiene orden $q+1$, hay exactamente $q+1$ valores posibles para x_{n+1} para cada vector de V_n de norma no nula. Como hay $(q-1)y_n$

tales vectores, en V_{n+1} tenemos $(q^2-1)y_n$ vectores de norma nula de este tipo y, en total,

$$z_{n+1} = z_n + (q^2-1)y_n.$$

Multiplicando la ecuación (8.1) por $(q+1)$ y simplificando y_n queda que

$$z_{n+1} = (q^{2n}-1)(q+1) - qz_n.$$

Es obvio que si V tiene dimensión 1 no hay vectores no nulos de norma nula, luego $z_1 = 0$, luego esta fórmula vale también para $n = 0$ si entendemos que $z_0 = 0$. Ahora, una simple inducción prueba que

$$z_n = (q^n - (-1)^n)(q^{n-1} + (-1)^n),$$

y a partir de aquí (8.1) nos da

$$y_n = q^{n-1}(q^n - (-1)^n).$$

∎

Ahora podemos contar el número de bases ortonormales de V. Para construir una, podemos elegir como primer vector v_1 cualquiera de los y_n vectores de norma 1 de V. El segundo vector lo tenemos que elegir en $\langle v_1\rangle^\perp$, que es un subespacio no degenerado de dimensión $n-1$ y $V = \langle v_1\rangle \oplus \langle v_1\rangle^\perp$, luego tenemos y_{n-1} posibilidades para v_2. Igualmente, v_3 hay que elegirlo en $\langle v_1, v_2\rangle^\perp$ y tenemos y_{n-2} posibilidades. En conclusión:

Teorema 8.36 *En un espacio unitario sobre el cuerpo de q^2 elementos hay*

$$\prod_{i=1}^{n} q^{i-1}(q^i - (-1)^i) = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - (-1)^i)$$

bases ortonormales.

El teorema 8.35 implica que, en la descomposición del teorema 8.28, necesariamente $\dim W \leq 1$, luego, concretamente, $\dim W$ será 0 o 1 según si $\dim V$ es par o impar. A su vez esto implica que todo espacio unitario de dimensión 2 sobre un cuerpo finito es un plano hiperbólico.

Espacios cuadráticos sobre cuerpos finitos En el caso cuadrático el cuerpo de escalares C puede tener $q = p^m$ elementos, donde m es ahora arbitrario (no necesariamente par). Si p es impar, tenemos que $1 \neq -1$, por lo que el homomorfismo $C^* \longrightarrow C^*$ dado por $\alpha \mapsto \alpha^2$ tiene núcleo $\{\pm 1\}$ de orden 2, luego su imagen tiene $(q-1)/2$ elementos, es decir, que en C^*, la mitad de los elementos son cuadrados y la otra mitad no lo son. Contando al 0 como cuadrado, concluimos que C contiene $(q+1)/2$ cuadrados. Por el contrario, si p es par, entonces el homomorfismo tiene núcleo trivial y concluimos que todos los elementos de C^* son cuadrados.

Teorema 8.37 *Si C es el cuerpo de q elementos para todo $\alpha \in C$ y todos los $a, b \in C$ no nulos, existen $x, y \in C$ tales que $ax^2 + by^2 = \alpha$.*

DEMOSTRACIÓN: Si la característica de C es 2, acabamos de observar que todo elemento de C es un cuadrado y la conclusión es inmediata. En caso contrario, los conjuntos $\{ax^2 \mid x \in C\}$ y $\{\alpha - by^2 \mid y \in C\}$ tienen ambos $(q+1)/2$ elementos, luego no pueden ser disjuntos, luego existen $x, y \in C$ tales que $ax^2 = \alpha - by^2$. ∎

Como consecuencia:

Teorema 8.38 *Si V es un espacio cuadrático de dimensión ≥ 3 sobre un cuerpo finito, entonces V contiene vectores singulares.*

DEMOSTRACIÓN: Supongamos en primer lugar que el cuerpo de escalares C tiene característica 2 y tomemos $u \in V$ no nulo. Entonces $\langle u\rangle^\perp$ tiene dimensión al menos 2, luego podemos tomar $v \in \langle u\rangle^\perp \setminus \langle u\rangle$. Entonces

$$Q(au + bv) = a^2Q(u) + b^2Q(v).$$

Si $Q(u) = 0$ o $Q(v) = 0$, ya tenemos ejemplos de vectores singulares en V. En caso contrario, para que se cumpla $a^2Q(u) + b^2Q(v) = 0$, basta tomar $a = 1$ y $b^2 = Q(u)/Q(v) \neq 0$, lo cual es posible porque todo elemento de C es un cuadrado.

Si C tiene característica $\neq 2$, podemos tomar tres vectores $u, v, w \in V$ ortogonales dos a dos. Por el teorema anterior existen $x, y \in C$ tales que

$$x^2\,\mathrm{N}(u) + y^2\,\mathrm{N}(v) = -\,\mathrm{N}(w).$$

Entonces $\mathrm{N}(xu + yv + w) = 0$. ∎

En particular, ahora sabemos que en la descomposición del teorema 8.28 para un espacio cuadrático sobre un cuerpo finito se tiene que cumplir necesariamente que $\dim W \leq 2$.

Si el cuerpo de escalares tiene característica 2, el caso $\dim W = 1$ es imposible, pues W sería obviamente degenerado y V también. Por lo tanto, los espacios cuadráticos sobre cuerpos finitos de característica 2 tienen necesariamente dimensión par.

En cambio, el teorema 8.32 implica que existe, salvo isometría, un único plano cuadrático no singular sobre el cuerpo C de q elementos:

Teorema 8.39 *Si C es el cuerpo de q elementos, existe, salvo isometría, un único plano cuadrático no singular sobre C, que es el dado por el cuerpo K de q^2 elementos con la forma cuadrática determinada por la norma $\mathrm{N} : K \longrightarrow C$.*

DEMOSTRACIÓN: El cuerpo K de q^2 elementos cumple las condiciones del teorema 8.32, pues podemos tomar $\omega \in K$ de traza -1 (que existe por 8.2) y podemos exigir que $\omega \notin C$ (pues en C hay a lo sumo un elemento de traza -1 y en K hay q elementos de traza -1). Entonces su polinomio mínimo sobre C es de la forma $x^2 + x + a$, donde $a = \mathrm{N}(\omega)$. El teorema nos da entonces que K es un plano cuadrático no singular con la forma cuadrática dada por la norma $\mathrm{N} : K \longrightarrow C$.

Además K es único salvo isometría, pues si V es cualquier plano cuadrático no singular, observamos en primer lugar que existe un $u \in V$ tal que $Q(u) = 1$. En efecto, si la característica de C no es 2, tomamos una base ortogonal u, v de V respecto a la cual

$$Q(xu + yv) = x^2Q(u) + y^2Q(v),$$

y el teorema 8.37 nos da un $w = xu + yv$ que cumple $Q(w) = 1$, mientras que si C tiene característica 2, todo elemento de C es un cuadrado, luego si $Q(u) = \alpha^2$, cambiando u por $\alpha^{-1}u$ se cumple igualmente que $Q(u) = 1$.

La prueba del teorema 8.32 muestra entonces que V es isométrico a un plano cuadrático en las condiciones del teorema con $\alpha = 1$ (pues α se toma como $Q(u)$, para un $u \in V$ no nulo arbitrario), y así éste es necesariamente el cuerpo K de q^2 elementos (que es único salvo isomorfismo) con su norma como forma cuadrática. ∎

Teorema 8.40 *Si V es un espacio cuadrático de dimensión $n \geq 2$ sobre un cuerpo finito C, la forma cuadrática $Q : V \longrightarrow C$ es suprayectiva.*

Demostración: Basta probarlo si V tiene dimensión 2, pues todo espacio cuadrático contiene un subespacio (no degenerado) de dimensión 2. Si V es un plano hiperbólico es inmediato, pues podemos expresar $Q(xu + yv) = xy$ y es obvio que toma todos los valores en C. Si V es un plano no singular, en virtud del teorema 8.39 basta tener en cuenta que la norma $\mathrm{N} : K \longrightarrow C$ entre dos cuerpos finitos es suprayectiva, lo cual es cierto en general por [Al 9.3], o por el teorema 8.33. ∎

En particular, vemos que, sobre un cuerpo de característica $\neq 2$, en todo plano cuadrático y, por consiguiente, en todo espacio cuadrático V de dimensión ≥ 2, existen elementos de norma 1. De aquí deducimos lo siguiente:

Teorema 8.41 *Todo espacio ortogonal V sobre un cuerpo finito C de característica $\neq 2$ admite una base ortogonal $v_1, \ldots, v_n$ tal que $\mathrm{N}(v_i) = 1$ para $i = 1, \ldots, n-1$, mientras que, fijado $\alpha \in C$ que no sea un cuadrado, v_n puede tomarse de modo que $\mathrm{N}(v_n) = 1$ o bien $\mathrm{N}(v_n) = \alpha$.*

Demostración: Por la observación precedente podemos ir eligiendo vectores de norma 1: $v_1 \in V$, $v_2 \in \langle v_1 \rangle^\perp$, $v_3 \in \langle v_1, v_2 \rangle^\perp$, hasta llegar a

$$\langle v_1, \ldots, v_{n-1} \rangle^\perp = \langle v_n \rangle,$$

donde ya no podemos asegurar que haya vectores de norma 1. Como C^*/C^{*2} tiene orden 2, tendremos que $\mathrm{N}(v_n) = \beta^2$ o bien $\mathrm{N}(v_n) = \beta^2\alpha$, para cierto $\beta \in C^*$, y cambiando v_n por $\beta^{-1}v_n$ obtenemos $\mathrm{N}(v_n) = 1$ o bien $\mathrm{N}(v_n) = \alpha$. ∎

A su vez esto nos da:

Teorema 8.42 *Si V es un espacio vectorial sobre un cuerpo finito C de característica $\neq 2$, existen, salvo isometría, dos únicas estructuras de espacio cuadrático en V, que se diferencian en que una admite bases ortonormales y la otra no, o también en que el determinante de la forma bilineal en cualquier base es un cuadrado en el primer caso y no lo es en el segundo.*

DEMOSTRACIÓN: Por el teorema anterior, cualquier estructura de espacio cuadrático en V admite una base ortogonal en la que la matriz de la forma bilineal es, o bien la identidad, o bien la identidad salvo un valor α en la última posición. En el primer caso el determinante de la forma cuadrática en dicha base es 1, y en cualquier otra base será un cuadrado en C, mientras que en el segundo caso el determinante es α en dicha base y $\beta^2\alpha$ en cualquier otra, luego las dos estructuras no son isométricas y dos del mismo tipo sí que lo son. ∎

Si $\dim V = n$ es par, hay dos estructuras posibles de espacio cuadrático en V, tanto si la característica de C es par o impar. Una corresponde a la descomposición

$$V = H_1 \perp \cdots \perp H_m,$$

de modo que $n = 2m$, donde m es el índice de Witt de V, y la otra corresponde a la descomposición

$$V = H_1 \perp \cdots \perp H_m \perp W,$$

donde W es un plano no singular, con lo que $n = 2m + 2$.

En cambio, si n es impar y C es un cuerpo finito de característica 2, tras 8.38 hemos visto que no hay estructuras de espacio cuadrático sobre V. Cuando la característica es impar, tenemos necesariamente la descomposición

$$V = H_1 \perp \cdots \perp H_m \perp W,$$

de modo que $n = 2m + 1$ y donde $W = \langle w \rangle$ determinará una estructura u otra según si $\mathrm{N}(w)$ es o no un cuadrado.

Aunque no lo vamos a necesitar, en el caso de espacios sobre cuerpos finitos de característica impar, resulta natural plantearse cuál de las dos estructuras cuadráticas de un espacio vectorial es la que admite una base ortonormal. La respuesta es sutil. Empezamos considerando el caso de un plano V:

Fijado $\alpha \in C$ que no sea un cuadrado, el teorema 8.41 nos da una base v_1, v_2 de V respecto a la cual la matriz de F es la identidad o bien diagonal con $1, \alpha$ en la diagonal. En cualquier caso, la norma de un vector $v = xv_1 + yv_2$ es

$$\mathrm{N}(v) = x^2 + \lambda y^2,$$

donde $\lambda = 1$ si V admite una base ortonormal y $\lambda = \alpha$ en caso contrario. Para que v sea isótropo es necesario que $x, y \neq 0$, y que $x^2 + \lambda y^2 = 0$, luego $\lambda = -(x/y)^2$.

Ahora tenemos que distinguir dos casos, según si -1 es un cuadrado o no en el cuerpo C. Es fácil saber cuándo se da cada caso. Si $-1 = \beta^2$, entonces

β tiene orden 4 en el grupo C^*, que es cíclico por [Al 4.50] y, recíprocamente, si β es un elemento de orden 4, entonces β^2 tiene orden 2, luego tiene que ser $\beta^2 = -1$. En resumen, -1 es un cuadrado en C si y sólo si $4 \mid q-1$, es decir, si y sólo si $q \equiv 1$ (mód 4).

Así pues, si $-1 = \beta^2$, tenemos que en V habrá vectores isótropos si y sólo si $\lambda = (\beta x/y)^2$ es un cuadrado, es decir, si y sólo si $\lambda = 1$, si y sólo si V tiene bases ortonormales. En cambio, si -1 no es un cuadrado en C, la condición de que $-\lambda$ sea un cuadrado equivale a que λ no lo sea, luego $\lambda = \alpha$ y V no tiene bases ortonormales.

En otros términos, si $q \equiv 1$ (mód 4) son los planos hiperbólicos los que tienen bases ortonormales, mientras que si $q \equiv -1$ (mód 4) son los planos anisótropos los que las tienen. En general:

Teorema 8.43 *Sea V un espacio cuadrático de dimensión n sobre el cuerpo de q elementos, con q impar, y sea*

$$V = H_1 \perp \cdots \perp H_m \perp W$$

una descomposición en las condiciones del teorema 8.28.

1. *Si $q \equiv 1$ (mód 4), entonces V tiene una base ortonormal si y sólo si $W = 0$ o bien W está generado por un vector cuya norma es un cuadrado.*
2. *Si $q \equiv -1$ (mód 4), entonces V tiene una base ortonormal si y sólo si:*
   (a) *m es par y $W = 0$ o bien W está generado por un vector cuya norma es un cuadrado, o bien*
   (b) *m es impar y $\dim W = 2$ o bien W está generado por un vector cuya norma no es un cuadrado.*

Demostración: Si formamos una base de V uniendo bases de los H_i y de W, el determinante de la matriz de F en dicha base es el producto de los determinantes de las matrices de las restricciones de F a cada H_i y a W. Según 8.42, sabemos que V tendrá una base ortonormal si y sólo si dicho determinante es un cuadrado.

Si $q \equiv 1$ (mód 4), hemos visto que el determinante de cada H_i es un cuadrado, luego V admitirá una base ortonormal si y sólo si la admite W, lo cual se cumple en las condiciones de 1.

Si $q \equiv -1$ (mód 4), el determinante de cada H_i no es un cuadrado, luego, si m es par hará falta que el determinante de W sea un cuadrado, y si m es impar hará falta que no lo sea, que es lo que afirma 2). ∎

Grupos de isometrías Si V es un espacio unitario, llamaremos *transformaciones unitarias* a las isometrías de V en sí mismo, que claramente forman un grupo al que llamaremos *grupo unitario* de V y que representaremos por $\mathrm{U}(V)$.

Si J es la matriz de la forma hermitiana F de V respecto de una base dada, los elementos de $\mathrm{U}(V)$ son claramente los automorfismos cuya matriz M en dicha base cumplen

$$MJ\bar{M}^t = J.$$

Si V es un espacio cuadrático, las isometrías de V en sí mismo se llaman *transformaciones ortogonales,* y forman un grupo que recibe el nombre de *grupo ortogonal* y que se representa por $O(V)$.

Similarmente, si J es la matriz de la forma bilineal de V la matriz M de un elemento $f \in O(V)$ debe cumplir

$$MJM^t = J,$$

y esta condición es necesaria y suficiente para que f sea una transformación ortogonal cuando la característica del cuerpo C es impar, pero sólo es necesaria (y no suficiente) cuando la característica es 2, pues sólo garantiza que f conserva la forma bilineal F y no la forma cuadrática Q.

Si el cuerpo de escalares C es finito con q^2 elementos, el teorema 8.34 prueba que existe una única estructura de espacio unitario en cada espacio vectorial V de dimensión n, por lo que podemos llamar $U(n, q^2)$ al grupo unitario correspondiente, que es isomorfo al grupo de las matrices unitarias $n \times n$ con coeficientes en C.

Cada transformación unitaria está determinada por la imagen de una base ortonormal prefijada de V, que será otra base ortonormal de V, luego hay tantas transformaciones unitarias como bases ortonormales. Así pues, el teorema 8.36 se interpreta ahora como que

$$|U(n, q^2)| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - (-1)^i).$$

La situación en el caso cuadrático es más delicada. Si V es un espacio vectorial de dimensión $n = 2m + 1$ sobre un cuerpo C de q elementos, con q impar, tenemos dos estructuras de espacio cuadrático en V no isométricas entre sí, pero ambas tienen el mismo grupo de isometrías. Ello se debe a que si F es una forma bilineal en V que determina la estructura cuadrática que admite una base ortonormal, entonces su matriz en dicha base será la identidad I, y si $\alpha \in C$ no es un cuadrado, entonces αF es también una forma bilineal simétrica sobre V que, en la misma base, tiene por matriz αI, cuyo determinante es α^n, que no es un cuadrado en C, luego F y αF determinan las dos únicas estructuras cuadráticas que admite V, y es inmediato que un automorfismo de V es una transformación ortogonal respecto de F si y sólo si lo es respecto de αF, luego tenemos un único grupo ortogonal $O(n, q)$, para n y q impares.

La situación es completamente distinta si n es par (en cuyo caso q puede ser par o impar). Ahora tenemos dos estructuras cuadráticas mucho más diferentes entre sí. Si llamamos m al índice de Witt, en un caso $n = 2m$, y en el otro caso $n = 2m + 2$ y vamos a ver que los grupos ortogonales correspondientes ni siquiera tienen el mismo orden. Conviene introducir una definición:

Definición 8.44 Si V es un espacio cuadrático de dimensión n e índice de Witt m, llamaremos *signo* de V a $\epsilon = 2m + 1 - n$.

De este modo, si

$$V = V_1 \perp \cdots \perp V_m \perp W$$

es la descomposición dada por el teorema 8.28, tenemos que

$$\dim W = \begin{cases} 0 & \text{si } \epsilon = 1, \\ 1 & \text{si } \epsilon = 0, \\ 2 & \text{si } \epsilon = -1. \end{cases}$$

En efecto, si n es impar, necesariamente $n = 2m + 1$ y el signo es $\epsilon = 0$. En cambio, si n es par y $n = 2m$ (luego $W = 0$) el signo es $\epsilon = 1$ y si $n = 2m + 2$ (luego $\dim W = 2$) el signo es $\epsilon = -1$.

Llamaremos $O^\epsilon(n, q)$ al grupo ortogonal de cualquier espacio cuadrático sobre un espacio vectorial V de dimensión n sobre el cuerpo de q elementos de signo ϵ.

Cuando ϵ tome un valor concreto, escribiremos simplemente

$$O^+(n, q), \qquad O(n, q), \qquad O^-(n, q)$$

para los grupos ortogonales correspondientes. Notemos que hemos justificado más arriba que, cuando $\epsilon = 0$, el grupo $O(n, q)$ es independiente de la estructura ortogonal que consideremos.

Es inmediato comprobar que si $\dim V = 1$, entonces $\mathrm{O}(V) = \{\pm 1\}$ (aunque el cuerpo de escalares no sea finito). Vamos a determinar ahora la estructura de los grupos $\mathrm{O}(V)$ cuando $\dim V = 2$. De momento no exigimos tampoco que el cuerpo de escalares sea finito. Tenemos dos posibilidades, según si el espacio cuadrático V tiene o no vectores singulares.

Si V contiene vectores singulares, entonces es un plano hiperbólico, luego podemos tomar un par hiperbólico (u, v), respecto al cual la forma cuadrática viene dada por

$$Q(xu + yv) = xy.$$

De aquí se sigue que los únicos vectores singulares son los de $\langle u \rangle$ y los de $\langle v \rangle$, luego una transformación $f \in \mathrm{O}(V)$ debe cumplir $f(u) = au$, $f(v) = bv$, o bien $f(u) = av$, $f(v) = bu$, para ciertos $a, b \in C$. La condición $Q(f(z)) = Q(z)$ equivale en ambos casos a que $ab = 1$, luego la matriz de f en la base u, v tiene que ser de una de las dos formas

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \qquad \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}.$$

Si llamamos f_a y g_b a las transformaciones ortogonales que en la base u, v vienen dadas por estas matrices, es inmediato comprobar que las f_a forman un subgrupo N isomorfo a C^*, mientras que las g_b tienen todas orden 2, y además

$$f_a^{g_b} = f_a^{-1}, \qquad g_b g_c = f_{bc^{-1}}.$$

De la primera relación se sigue que todo elemento de $\mathrm{O}(V)$ se puede expresar en la forma f_a o bien $f_a g_b = f_a g_b g_1 g_1 = f_a f_b g_1 = f_{ab} g_1$, luego

$$\mathrm{O}(V) = \langle g_1 \rangle\, [N] \cong C_2[C^*],$$

donde la acción es la dada por $x^g = x^{-1}$. En el caso en que C es el cuerpo de q elementos, $C^* \cong C_{q-1}$, por lo que $\mathrm{O}(V) \cong D_{2(q-1)}$.

Consideremos ahora el caso en que V es no singular (y de nuevo no suponemos que C sea finito). Según el teorema 8.32 podemos suponer que $V = K$ es un cuerpo de grado 2 sobre C y que $Q : K \longrightarrow C$ es la norma. No perdemos generalidad si suponemos $\alpha = 1$, porque un automorfismo de K (como C-espacio vectorial) es una isometría respecto de una forma cuadrática Q si y sólo si lo es respecto de otra de la forma αQ, luego al cambiar Q por $\alpha^{-1}Q$ para suponer $\alpha = 1$ no estamos alterando el grupo $\mathrm{O}(V)$.

Según dicho teorema, tenemos que $K = C(\omega)$, donde ω es raíz del polinomio irreducible $x^2 + x + a$, con $a = \mathrm{N}(\omega)$. La conjugación $g : K \longrightarrow K$ dada por $g(\omega) = \bar{\omega} = -1-\omega$ es claramente una transformación ortogonal, y tiene orden 2.

Por otro lado, si $\alpha \in K$ cumple $\mathrm{N}(\alpha) = 1$, entonces $f_\alpha(\xi) = \alpha\xi$ es una isometría, pues claramente es un isomorfismo de C-espacios vectoriales y

$$\mathrm{N}(\alpha\xi) = \mathrm{N}(\alpha)\,\mathrm{N}(\xi) = \mathrm{N}(\xi).$$

Además

$$f_\alpha^g(\xi) = \overline{f_\alpha(\bar{\xi})} = \overline{\alpha\bar{\xi}} = \bar{\alpha}\xi = \alpha^{-1}\xi = f_{\alpha^{-1}}(\xi),$$

luego $f_\alpha^g = f_\alpha^{-1}$. Si llamamos N al subgrupo generado por las transformaciones f_α, vamos a probar que $\mathrm{O}(V) \cong \langle g \rangle\, [N]$, donde la acción es la dada por $f^g = f^{-1}$.

Notemos que $\langle g \rangle \cap N = 1$, pues si $f_\alpha \in \langle g \rangle$ entonces $f_\alpha(1) = \alpha = 1$, con lo que $f_\alpha = 1$. Sólo falta probar que todo elemento $h \in \mathrm{O}(V)$ se expresa en la forma $h = f_\alpha$ o bien $h = g f_\alpha$.

Ahora bien, como h es ortogonal, $\alpha = h(1)$ tiene norma 1, luego está definida la transformación $f_\alpha \in \mathrm{O(V)}$ y tenemos que $(h f_\alpha^{-1})(1) = 1$. Basta probar que $h f_\alpha^{-1} = 1, g$ o, equivalentemente, podemos suponer que $h(1) = 1$ y probar que $h = 1, g$. A su vez, para ello basta probar que $h(\omega) = \omega, \bar{\omega}$, pues entonces h coincidirá con la identidad 1 o con g en la base $1, \omega \in K$.

Por una parte, $h(\omega)\overline{h(\omega)} = \mathrm{N}(h(\omega)) = \mathrm{N}(\omega) = a$. Por otra parte, teniendo en cuenta que

$$\mathrm{N}(1 + h(\omega)) = \mathrm{N}(h(1 + \omega)) = \mathrm{N}(1 + \omega) = \mathrm{N}(-\omega) = a,$$

vemos que

$$a = \mathrm{N}(1 + h(\omega)) = (1 + h(\omega))(1 + \overline{h(\omega)}) = 1 + h(\omega) + \overline{h(\omega)} + h(\omega)\overline{h(\omega)} =$$
$$1 + h(\omega) + \overline{h(\omega)} + a,$$

luego $h(\omega) + \overline{g(\omega)} = -1$, luego

$$(t - h(\omega))(t - \overline{h(\omega)}) = t^2 + t + a,$$

luego $h(\omega)$ tiene el mismo polinomio mínimo que ω, por lo que es $h(\omega) = \omega$ o bien $h(\omega) = \bar{\omega}$.

Así pues, $\mathrm{O}(V) = C_2[N]$, donde N es el núcleo de la norma $\mathrm{N} : K^* \longrightarrow C^*$. Si C es el cuerpo de q elementos, K^* es cíclico de orden $q^2 - 1$ y la norma es un epimorfismo de grupos por el teorema 8.40, luego su núcleo es $N \cong C_{q+1}$, luego $\mathrm{O}(V) \cong D_{2(q+1)}$. El teorema siguiente resume lo que hemos obtenido:

Teorema 8.45 *Si $\epsilon = \pm 1$, entonces $\mathrm{O}^\epsilon(2, q) \cong D_{2(q-\epsilon)}$.*

Observemos que, en realidad hemos probado mucho más, pues hemos visto que, si V es un espacio cuadrático de dimensión 2 sobre un cuerpo arbitrario, entonces $\mathrm{O}(V) \cong C_2[N]$, para cierto grupo abeliano N, de modo que $\mathrm{O}(V)$ es un grupo resoluble, luego no podremos obtener de él ningún grupo simple no abeliano tomando subgrupos y cocientes.

Para calcular los órdenes de los demás grupos ortogonales empezamos probando lo siguiente:

Teorema 8.46 *Si H es un plano hiperbólico sobre el cuerpo de q elementos, entonces H contiene $2(q-1)$ vectores singulares y, para cada $\alpha \in C^*$, hay $q-1$ vectores $v \in H$ tales que $Q(v) = \alpha$.*

Demostración: Basta tener en cuenta que, si $u, v \in H$ forman un par hiperbólico, se cumple que $Q(xu + yv) = xy$, con lo que $xy = 0$ se cumple siempre que $x = 0$ o $y = 0$, lo que nos da $q - 1$ posibilidades en cada caso (excluyendo el caso $x = y = 0$, que no corresponde a un vector singular), luego hay $2(q - 1)$ vectores singulares. Por el contrario, si $\alpha \neq 0$, la ecuación $xy = \alpha$ tiene $q - 1$ soluciones, una para cada valor $x \in C^*$ posible, con $y = \alpha/x$. ∎

Teorema 8.47 *El número de vectores singulares de un espacio cuadrático V de índice de Witt m y signo ϵ sobre el cuerpo C de q elementos es*

$$z_m^\epsilon = (q^{m-\epsilon} + 1)(q^m - 1).$$

Demostración: Ante todo, observemos que si $\epsilon = 0$ el valor de z_m no depende de la estructura cuadrática que consideremos en V, pues podemos tomarlas de modo que sus formas bilineales sean F y αF, donde $\alpha \in C$ no es un cuadrado, y es evidente que F y αF determinan los mismos vectores singulares. Por lo tanto, z_m está bien definido.

Vamos a probar el teorema por inducción sobre $n = \dim V$. La fórmula incluye el caso trivial $n = 0$, correspondiente a $m = 0$, $\epsilon = 1$, para el que da $z_0^+ = 0$, que es correcto, porque un espacio nulo no tiene vectores singulares.

Si $n = 1$ tiene que ser $m = 0$, $\epsilon = 1$, y de nuevo es correcto el valor $z_0^+ = 0$, pues en la descomposición del teorema 8.28 tenemos $V = W$, luego V es no singular.

Si $n = 2$, o bien $m = 0$, $\epsilon = -1$, que corresponde de nuevo al caso $V = W$, en el que V es anisótropo (luego el valor $z_0^- = 0$ es correcto), o bien $m = 1$, $\epsilon = 1$, que corresponde al caso en que V es un plano hiperbólico, y el valor $z_1^+ = 2(q - 1)$ también es correcto según el teorema anterior.

Ahora suponemos que la fórmula es cierta para espacios de dimensión menor que $n \geq 3$ y vamos a probarla para n. Fijemos un espacio cuadrático V de dimensión n, correspondiente a unos valores m, ϵ tales que $n = 2m + 1 - \epsilon$. Podemos descomponerlo como $V = H \perp V'$, donde H es un plano hiperbólico y V' es un espacio de dimensión $n-2$ correspondiente a $m-1$ y ϵ, al que podemos aplicar la hipótesis de inducción.

Si $v \in V$ es singular, lo podemos expresar de forma única como $v = v_1 + v_2$, donde $v_1 \in H$ y $v_2 \in V'$. Entonces $Q(v) = Q(v_1) + Q(v_2) = 0$. Por el teorema anterior sabemos que H contiene al vector nulo, más $2q-2$ vectores singulares, más $q-1$ vectores de cada una de las $q-1$ normas posibles. Por otro lado, en V' tenemos el vector nulo más z^ϵ_{m-1} vectores singulares y $q^{n-2} - z^\epsilon_{m-1} - 1$ vectores no singulares.

Si $Q(v_1) = Q(v_2) = 0$, las posibilidades son $2q-1$ para v_1 y $1 + z^\epsilon_{m-1}$ para v_2, pero entre ellas estamos contando al vector nulo, luego en V hay un total de $(2q-1)(1+z^\epsilon_{m-1})-1$ vectores singulares que se descomponen en suma de vectores singulares de H y V'.

Si v_1 y v_2 son no singulares, entonces $Q(v_2) = -Q(v_1)$, luego si en V' hay v_λ vectores en los que Q toma el valor $-\lambda$, en total tenemos $(q-1)v_\lambda$ vectores singulares tales que $Q(v_1) = \lambda$, luego un total de

$$(q-1)\sum_{\lambda \in C^*} v_\lambda = (q-1)(q^{n-2} - z^\epsilon_{m-1} - 1)$$

vectores singulares que se descomponen en suma de vectores no singulares. En total

$$z^\epsilon_m = (2q-1)(1+z^\epsilon_{m-1}) - 1 + (q-1)(q^{n-2} - z^\epsilon_{m-1} - 1),$$

que equivale a

$$z^\epsilon_m = q z^\epsilon_{m-1} + (q-1)(q^{n-2}+1).$$

De aquí se sigue fácilmente la fórmula del enunciado:

$$z^\epsilon_m = q(q^{m-1-\epsilon}+1)(q^{m-1}-1) + (q-1)(q^{2m-1-\epsilon}+1) = (q^{m-\epsilon}+1)(q^m-1)$$

■

A continuación observamos que, en las condiciones del teorema anterior, V tiene exactamente $q^{n-2} z^\epsilon_m$ pares (ordenados) hiperbólicos (u, v).

En efecto, para formar un par hiperbólico podemos tomar como primera componente cualquier vector $u \in V$ de los z^ϵ_m vectores singulares que tiene V. Sea $v_0 \in V$ tal que (u, v_0) sea un par hiperbolico y sea $W = \langle u, v_0\rangle^\perp$, de modo que $V = \langle u, v_0\rangle \perp W$. Así, un vector arbitrario de V es de la forma $v = xu + yv_0 + w$, con $x, y \in C$, $w \in W$, y para que (u, v) sea un par hiperbólico tiene que cumplirse que $F(u, v) = y = 1$, y que $Q(v) = Q(w) + x = 0$, luego

$$v = -Q(w)u + v_0 + w,$$

para todo $w \in W$, luego tenemos $|W| = q^{n-2}$ posibilidades para v, y el número de pares es $q^{n-2} z^\epsilon_m$.

A continuación observamos que el número de pares hiperbólicos (u_i, v_i) en V que generan planos hiperbólicos ortogonales dos a dos es

$$q^{2m-1-\epsilon}z_m^\epsilon\, q^{2m-3-\epsilon}z_{m-1}^\epsilon\cdots q^{1-\epsilon}z_1^\epsilon = \prod_{i=1}^m q^{2m+1-2i-\epsilon}\prod_{i=1}^m (q^{i-\epsilon}+1)(q^i-1) =$$

$$q^{m(1-\epsilon)}q^{2\sum_{i=0}^{m-1} i}\prod_{i=1}^m (q^{i-\epsilon}+1)(q^i-1) = q^{m(m-\epsilon)}\prod_{i=1}^m (q^{i-\epsilon}+1)(q^i-1).$$

Ahora, si $V = \langle u_1, v_1\rangle \perp \cdots \perp \langle u_m, v_m\rangle \perp W$, una transformación ortogonal $f \in \mathrm{O}(V)$ transforma la sucesión $u_1, v_1, \ldots, u_m, v_m$ en otra sucesión $f(u_1), f(v_1), \ldots, f(u_m), f(v_m)$ de pares hiperbólicos en las mismas condiciones, la cual determina a su vez el subespacio

$$W' = \langle f(u_1), f(v_1), \ldots, f(u_m), f(v_m)\rangle^\perp,$$

de modo que tenemos una transformación f para cada sucesión posible

$$f(u_1), f(v_1), \ldots, f(u_m), f(v_m)$$

(para la cual tenemos las posibilidades que acabamos de calcular hace un momento) y cada isometría $f|_W : W \longrightarrow W'$. Fijada una isometría $i : W' \longrightarrow W$, vemos que $f|_W \mapsto f|_W \circ i$ biyecta las isometrías posibles $W \longrightarrow W'$ con las transformaciones de $\mathrm{O}(W)$. Por consiguiente,

$$|\mathrm{O}(V)| = |\mathrm{O}(W)|q^{m(m-\epsilon)}\prod_{i=1}^m (q^{i-\epsilon}+1)(q^i-1).$$

Es claro que si $\dim W = 1$, entonces $O(W) = \{\pm 1\}$, luego $|\mathrm{O}(W)| = 2$ si $\epsilon = 0$, $|\mathrm{O}(W)| = 2(q+1)$ si $\epsilon = -1$ (por 8.45) y $|\mathrm{O}(W)| = 1$ si $\epsilon = 1$ (pues entonces $W = 0$).

El teorema siguiente resume lo que hemos obtenido, incluyendo el caso de los grupos unitarios:

Teorema 8.48 *Los órdenes de los grupos unitarios y ortogonales sobre cuerpos finitos vienen dados por las fórmulas siguientes:*

$$\begin{aligned}
|U(n,q^2)| &= q^{n(n-1)/2}\prod_{i=1}^n (q^i-(-1)^i),\\
|\mathrm{O}(2m+1,q)| &= 2q^{m^2}\prod_{i=1}^m (q^{2i}-1), \quad \textit{para } q \textit{ impar},\\
|\mathrm{O}^\epsilon(2m,q)| &= 2q^{m(m-1)}(q^m-\epsilon)\prod_{i=1}^{m-1} (q^{2i}-1).
\end{aligned}$$

Notemos que, en la cuarta fórmula, el índice de Witt del espacio cuadrático de tipo negativo de orden $2m$ no es m, sino $m-1$.

En el capítulo siguiente estudiaremos estos grupos y veremos cómo a partir de ellos podemos obtener nuevas familias de grupos simples.

Capítulo IX

Los grupos unitarios y ortogonales

En este capítulo probaremos que los grupos unitarios y ortogonales introducidos en el capítulo anterior proporcionan las dos últimas familias de grupos simples clásicos que nos falta estudiar.

9.1 Los grupos unitarios

Vamos a estudiar el grupo $\mathrm{U}(V) \leq \mathrm{LG}(V)$ de las transformaciones unitarias de un espacio unitario V sobre un cuerpo C. Cuando C es el cuerpo finito de q^2 elementos se trata de los grupos $U(n, q^2)$ cuyo orden hemos calculado en el capítulo anterior.

El homomorfismo inducido por el determinante $\det : \mathrm{LG}(V) \longrightarrow C^*$ se restringe a un homomorfismo $\det : \mathrm{U}(V) \longrightarrow C^*$ cuyo núcleo recibe el nombre de *grupo unitario especial* de V, y lo representaremos por

$$\mathrm{UE}(V) = \mathrm{U}(V) \cap \mathrm{LE}(V) \trianglelefteq \mathrm{U}(V).$$

Si J es la matriz de de la forma hermitiana F en una base de V prefijada, las transformaciones unitarias son los automorfismos de V cuya matriz M en dicha base cumple

$$MJ\bar{M}^t = J.$$

Por el teorema 8.25, tomando una base ortogonal de V, podemos suponer que la matriz J es diagonal. Así, el determinante $\alpha = |M|$ cumple $\alpha\bar{\alpha} = 1$, es decir, $\mathrm{N}(\alpha) = 1$, donde $\mathrm{N} : C \longrightarrow R$ es la norma de la extensión C/R y, recíprocamente, todo $\alpha \in C^*$ que cumpla $\mathrm{N}(\alpha) = 1$ es el determinante de una transformación unitaria, por ejemplo de la determinada por la matriz diagonal M que tiene en su diagonal $\alpha, 1, \ldots, 1$, que claramente cumple la relación $MJ\bar{M}^t = J$ supuesto que J sea diagonal.

Así pues, la imagen del homomorfismo $\det : \mathrm{U}(V) \longrightarrow C^*$ es el núcleo de la norma $\mathrm{N} : C^* \longrightarrow R^*$.

En [Al 6.21] hemos visto que todo automorfismo distinto de la identidad de un espacio vectorial V que fije a un hiperplano es una transvección o una dilatación, y en [Al 6.22] hemos probado que $\mathrm{LE}(V)$ está generado por las transvecciones, mientras que $\mathrm{LG}(V)$ está generado por las dilataciones y las transvecciones. Vamos a probar resultados análogos para los espacios unitarios.

Transvecciones y dilataciones unitarias Sea V un espacio unitario y consideremos una transvección $T : V \longrightarrow V$, dada por

$$T(v) = v + f(v)a,$$

donde $f : V \longrightarrow C$ es una aplicación lineal cuyo núcleo es un hiperplano H y $a \in H$ no es nulo. En particular, T deja fijos a los vectores de H.

Si completamos una base de H hasta una base de V, la matriz de T en dicha base tiene unos en la diagonal y ceros en las demás posiciones excepto en una, por lo que las transvecciones tienen determinante 1. Vamos a ver qué tiene que cumplir una transvección para ser unitaria.

Completando una base de H hasta una base de V podemos descomponer $V = H \oplus \langle x \rangle$ y considerar la proyección $\pi : V \longrightarrow C$ que a cada $v \in V$ le hace corresponder el escalar que permite expresar $v = h + \pi(v)x$, con $h \in H$. El teorema 8.5 nos da un $u \in V$ tal que $\pi(v) = F(v, u)$, para todo $v \in V$. Como $\pi(x) = 1$, $u \neq 0$ y, como π se anula en H, tiene que ser $F(h, u) = 0$ para todo $h \in H$, luego $u \in H^\perp$. Como $\dim H = n - 1$, tenemos que $\dim H^\perp = 1$, luego $H^\perp = \langle u \rangle$.

Así, todo vector $v \in V$ se expresa en la forma $v = h + F(v, u)x$, con lo que

$$T(v) = T(h + F(v, u)x) = h + F(v, u)(x + f(x)a) = v + F(v, u)z,$$

donde $z = f(x)a \in H$ no es nulo, luego $F(z, u) = 0$. Esto vale para cualquier transvección. Que T sea unitaria significa que

$$F(v, w) = F(T(v), T(w)) = F(v + F(v, u)z, w + F(w, u)z) =$$

$$F(v, w) + F(v, u)F(z, w) + \overline{F(w, u)}F(v, z) + F(v, u)\overline{F(w, u)}F(z, z),$$

luego T es unitaria si y sólo si

$$F(v, u)F(z, w) + \overline{F(w, u)}F(v, z) + F(v, u)\overline{F(w, u)}F(z, z) = 0,$$

para todo par de vectores $v, w \in V$. En particular, haciendo $v = z$ obtenemos que

$$\overline{F(w, u)}F(z, z) = 0,$$

y como esto tiene que cumplirse para todo $w \in V$, tiene que ser $F(z, z) = 0$, es decir, que el vector z es necesariamente isótropo. Por lo tanto, la condición para que T sea unitaria se reduce a que $z \in H$ sea isótropo y, para todo $v, w \in V$,

$$F(v, u)F(z, w) + F(u, w)F(v, z) = 0.$$

En particular, podemos tomar $v \in V$ tal que $F(v,u) \neq 0$, y esto implica $F(v,z) \neq 0$, pues en caso contrario la relación anterior nos daría que $F(z,w) = 0$ para todo $w \in V$. Por lo tanto, podemos despejar

$$F(u,w) = -\frac{F(v,u)}{F(v,z)}F(z,w) = \alpha F(z,w),$$

para todo $w \in V$ y un $\alpha \in C$ fijo, lo cual equivale a que $F(u - \alpha z, w) = 0$ para todo w, que a su vez obliga a que $u = \alpha z$. Por lo tanto, $z \in H \cap H^\perp$ y $H^\perp = \langle z \rangle$. La expresión para T se reduce así a

$$T(v) = v + \bar{\alpha}\, F(v,z)z,$$

y la condición para que T sea unitaria se reduce a que $z \in H$ sea isótropo y

$$(\alpha + \bar{\alpha})F(v,z)F(z,w) = 0$$

para todo $v, w \in V$, lo cual equivale a que $\alpha + \bar{\alpha} = 0$. En resumen:

Teorema 9.1 *Si V es un espacio unitario, las transvecciones unitarias en V son los automorfismos de la forma*

$$T_{z,\alpha}(v) = v + \alpha F(v,z)z,$$

donde z es isótropo y $\bar{\alpha} = -\alpha$.

Recordemos ahora de [Al 6.20] que las dilataciones son los automorfismos $D : V \longrightarrow V$ que fijan un hiperplano H y que, sobre un vector $u \in V \setminus H$, actúan como $D(u) = \alpha u$, para cierto $\alpha \neq 0$.

Vamos a determinar las dilataciones unitarias. Podemos suponer que $\alpha \neq 1$, o de lo contrario D es la identidad, que obviamente es unitaria. Descomponemos $V = H \oplus \langle u \rangle$ y consideramos la proyección $\pi : V \longrightarrow C$ que a cada $v \in V$ le hace corresponder el escalar que permite expresar $v = h + \pi(v)u$, con $h \in H$. El teorema 8.5 nos da un $w \in V$ tal que $\pi(v) = F(v,w)$, para todo $v \in V$. Notemos que $F(u,w) = \pi(u) = 1$ y si $h \in H$ se cumple $F(h,w) = \pi(h) = 0$, luego $w \in H^\perp$, luego $H^\perp = \langle w \rangle$.

Así, todo vector $v \in V$ se expresa en la forma $v = h + F(v,w)u$, con lo que

$$D(v) = h + F(v,w)\alpha u = v - F(v,w)u + F(v,w)\alpha u = v + (\alpha - 1)F(v,w)u.$$

Que D sea unitaria significa que, para todo par de vectores $v_1, v_2 \in V$, se cumple que

$$F(v_1,v_2) = F(D(v_1),D(v_2)) = F(v_1,v_2) + (\alpha-1)F(v_1,w)F(u,v_2) +$$
$$(\bar{\alpha}-1)\overline{F(v,w)}F(v_1,u) + (\alpha-1)(\bar{\alpha}-1)F(v_1,w)\overline{F(v_2,w)}F(u,u),$$

o, equivalentemente,

$$(\alpha-1)F(v_1,w)F(u,v_2) + (\bar{\alpha}-1)\overline{F(v_2,w)}F(v_1,u) +$$
$$(\alpha-1)(\bar{\alpha}-1)F(v_1,w)\overline{F(v_2,w)}F(u,u) = 0.$$

En particular, haciendo $v_2 = u$ (y recordando que $F(u,w) = 1$) queda

$$(\alpha-1)F(v_1,w)F(u,u) + (\bar{\alpha}-1)F(v_1,u) + (\alpha-1)(\bar{\alpha}-1)F(v_1,w)F(u,u) = 0.$$

Si fuera $F(u,u)=0$, tendríamos que $F(v_1,u)=0$ para todo $v_1\in V$, con lo que $u=0$, lo cual es imposible. Así pues, $\mathrm{N}(u)\neq 0$.

Tomando v_1 tal que $F(v_1,w)\neq 0$ y $v_2=h\in H$ queda

$$(\alpha-1)F(v_1,w)F(u,h)=0,$$

de donde $F(u,h)=0$ para todo $h\in H$, luego $u\in H^\perp=\langle w\rangle$. Si $w=\beta u$, concluimos que $1=F(w,u)=\beta F(u,u)$, luego

$$w=\frac{1}{F(u,u)}u,$$

y esto nos lleva a la expresión siguiente para D:

$$D(v)=v+(\alpha-1)\frac{F(v,u)}{F(u,u)}\,u.$$

Más aún, $\mathrm{N}(u)=\mathrm{N}(D(u))=\alpha\bar\alpha\,\mathrm{N}(u)\neq 0$, luego $\alpha\bar\alpha=1$. Si introducimos esta relación y la expresión para w en la condición para que D sea unitaria ésta se reduce a

$$(\alpha-1)F(v_1,u)F(u,v_2)+(\bar\alpha-1)F(v_1,u)F(u,v_2)+$$

$$(2-\alpha-\bar\alpha)F(v_1,u)F(u,v_2)=0,$$

pero esto se cumple trivialmente, luego las condiciones necesarias que hemos encontrado son suficientes. Así pues:

Teorema 9.2 *Si V es un espacio unitario, las dilataciones unitarias en V son los automorfismos de la forma*

$$D_{u,\alpha}(v)=v+(\alpha-1)\frac{F(v,u)}{F(u,u)}\,u,$$

donde $u\in V$ no es isótropo y $\alpha\bar\alpha=1$.

Si completamos con u una base ortogonal de $\langle u\rangle^\perp$, la matriz de $D_{u,\alpha}$ en dicha base es la identidad salvo α en una posición en la diagonal, luego $\det D_{u,\alpha}=\alpha$.

Se comprueba trivialmente que si $f\in \mathrm{U}(V)$, entonces

$$T^f_{z,\alpha}=T_{f(z),\alpha},\qquad D^f_{u,\alpha}=D_{f(u),\alpha}.$$

En [Al 4.39] hemos visto que el centro de $\mathrm{LG}(V)$ está formado por las homotecias $\alpha\cdot 1$, es decir, por los automorfismos dados por $f(v)=\alpha v$, para un cierto $\alpha\in C$. Una homotecia será unitaria si y sólo si cumple

$$F(v,v)=F(\alpha v,\alpha v)=\alpha\bar\alpha F(v,v),$$

y si aplicamos esto a un vector no isótropo v, concluimos que $\mathrm{N}(\alpha)=\alpha\bar\alpha=1$, luego el grupo $\mathrm{ZU}(V)$ de las homotecias unitarias de V está formado por las homotecias cuya razón α tiene norma 1.

Teorema 9.3 *Si V es un espacio unitario, el centro $Z(\mathrm{U}(V))$ del grupo unitario es el subgrupo $\mathrm{ZU}(V)$ de las homotecias unitarias.*

DEMOSTRACIÓN: Si $f \in Z(\mathrm{U}(V))$, dado un vector no nulo $v \in V$, si v es isótropo se tiene que cumplir que $T_{v,\alpha} = T^f_{v,\alpha} = T_{f(v),\alpha}$, luego, igualando los subespacios de vectores fijados, resulta que $\langle v\rangle^\perp = \langle f(v)\rangle^\perp$, luego $\langle f(v)\rangle = \langle v\rangle$. Si v es anisótropo llegamos a la misma conclusión razonando con $D_{v,\alpha}$. Por lo tanto, para cada $v \in V$ no nulo existe un escalar α_v tal que $f(v) = \alpha_v v$. Fijada una base $v_1, \ldots, v_n$, tenemos que

$$\alpha_{v_i+v_j}(v_i + v_j) = \alpha_{v_i} v_i + \alpha_{v_j} v_j,$$

luego por la independencia lineal concluimos que $\alpha_{v_i} = \alpha_{v_i+v_j} = \alpha_{v_j}$, luego todos los α_{v_i} coinciden con un mismo α y así f es una homotecia. ∎

Los grupos unitarios proyectivos Fijada una base de V, el centro $Z(V)$ del grupo $\mathrm{LG}(V)$ se corresponde con el grupo $Z(n, C) \cong C^*$ de las matrices escalares αI, con $\alpha \in C^*$, luego $\mathrm{ZU}(V)$ se corresponde con el grupo $\mathrm{ZU}(n, C)$ de las matrices αI de las matrices escalares con $\mathrm{N}(\alpha) = 1$, por lo que es isomorfo al núcleo de la norma. Acabamos de probar que

$$\mathrm{ZU}(V) = Z(V) \cap \mathrm{U}(V).$$

Según vimos en la sección [G 8.2] el grupo $\mathrm{LGP}(V) = \mathrm{LG}(V)/Z(V)$ se identifica con el grupo de las homografías del espacio proyectivo $P(V)$, y ahora podemos considerar el *grupo unitario proyectivo*

$$\mathrm{UP}(V) = \mathrm{U}(V)/\mathrm{ZU}(V)$$

al que podemos ver como subgrupo de $\mathrm{LGP}(V)$, es decir, que podemos considerar también a sus elementos como (parte de las) homografías del espacio $P(V)$.

Si llamamos

$$\mathrm{ZUE}(V) = \mathrm{UE}(V) \cap Z(V), \qquad \mathrm{UEP}(V) = \mathrm{UE}(V)/\mathrm{ZUE}(V),$$

tenemos que $\mathrm{ZUE}(V)$ está formado por las homotecias de razón α que cumplen $\mathrm{N}(\alpha) = 1$ (para que sean unitarias) y $\alpha^n = 1$ (para que tengan determinante 1), y el *grupo unitario especial proyectivo* $\mathrm{UEP}(V)$ puede verse como subgrupo normal de $\mathrm{UP}(V)$.

En esta sección demostraremos que si el espacio V es isótropo (es decir, si tiene vectores isótropos, lo que, en particular, sucede siempre que el cuerpo C es finito y $\dim V \geq 2$) entonces $\mathrm{UEP}(V)$ es un grupo simple, salvo en unos pocos casos excepcionales.

Para ello usaremos el teorema de Iwasawa, pero para ello no podemos considerar la acción de $\mathrm{UEP}(V)$ sobre $P(V)$ porque no es transitiva (ni, en particular, primitiva). En efecto, en $P(V)$ podemos distinguir entre *puntos isótropos y no*

isótropos, según que sean subespacios $\langle v\rangle$ generados por un vector isótropo o no isótropo, y es obvio que toda homografía inducida por una transformación unitaria envía puntos isótropos a puntos isótropos y puntos no isótropos a puntos no isótropos, por lo que la acción tiene como mínimo dos órbitas. Lo que vamos a ver a continuación es que podemos restringirla a una de ellas, es decir, que vamos a considerar la acción de $\mathrm{UP}(V)$ sobre el conjunto

$$\Omega = \{\langle v\rangle \in P(V) \mid v \neq 0,\ \mathrm{N}(v) = 0\}$$

de los puntos isótropos de $P(V)$, y veremos que cumple los requisitos del teorema de Iwasawa.

Teorema 9.4 *Si V es un espacio unitario isótropo, entonces el núcleo de la acción $\mathrm{U}(V) \longrightarrow \Sigma_\Omega$ es $\mathrm{ZU}(V)$, por lo que $\mathrm{UP}(V)$ (y, por consiguiente, $\mathrm{UEP}(V)$) es un grupo de permutaciones sobre Ω.*

Demostración: Sea $f \in \mathrm{U}(V)$ una transformación que fije a todos los puntos de Ω, es decir, que cumpla $f[\langle v\rangle] = \langle v\rangle$ para todo $v \in V$ isótropo. Tenemos que probar que $f \in \mathrm{ZU}(V)$.

Para que V sea isótropo es necesario que $n = \dim V \geq 2$ y si $n = 2$ entonces V es un plano hiperbólico. Vamos a considerar este caso en primer lugar, para lo cual tomamos un par hiperbólico (u, v) en V. Como u, v son isótropos, por hipótesis existen escalares α y β tales que $f(u) = \alpha u$, $f(v) = \beta v$. Podemos tomar $s \in C$ no nulo tal que $s + \bar{s} = 0$, con lo que $\mathrm{N}(u + sv) = s + \bar{s} = 0$, luego existe un escalar γ tal que

$$\gamma(u + sv) = f(u + sv) = f(u) + sf(v) = \alpha u + s\beta v.$$

Por la independencia lineal tiene que ser $\alpha = \gamma = \beta$, luego $f \in \mathrm{ZU}(V)$.

Supongamos ahora que $n \geq 3$. Basta probar que $f[\langle v\rangle] = \langle v\rangle$ para todo vector $v \in V$ anisótropo, ya que entonces f fija a todos los puntos de $P(V)$ y esto implica que $f \in Z(V)$ (porque los elementos de $\mathrm{LGP}(V)$ se identifican con las homografías de $P(V)$ o, más directamente, por el mismo argumento que hemos empleado en la prueba del teorema 9.3), luego de hecho $f \in \mathrm{ZU}(V)$.

A su vez, para ello basta probar que si v es anisótropo no nulo, entonces $\langle v\rangle = H_1 \cap H_2$ es la intersección de dos planos hiperbólicos, pues cada plano hiperbólico se descompone como suma $H = P_1 + P_2$ de dos puntos isótropos, luego se cumple que $f[H] = H$, y si f fija a los dos planos H_1 y H_2, también fija a su intersección.

Por hipótesis podemos tomar un vector isótropo $w \in V$. Observemos ahora que podemos tomar

$$z \in V \setminus (\langle v\rangle^\perp \cup \langle w\rangle^\perp \cup \langle v, w\rangle).$$

Esto se debe a un hecho general: si un espacio vectorial V se expresa como unión $V = W_1 \cup W_2$ de dos subespacios, necesariamente[1] $W_1 \leq W_2$ o $W_2 \leq W_1$,

[1] En caso contrario podríamos tomar $w_1 \in W_1 \setminus W_2$ y $w_2 \in W_2 \setminus W_1$, pero $w_1 + w_2$ tendría que estar en un W_i, por ejemplo en W_1, y entonces $w_2 \in W_1$, en contra de lo supuesto.

luego $V = W_1$ o $V = W_2$, y a su vez esto implica que lo mismo vale para tres subespacios. Como ninguno de los tres subespacios $\langle v\rangle^\perp, \langle w\rangle^\perp, \langle v, w\rangle$ puede ser V (todos tienen dimensión menor) su unión no puede ser V.

Entonces $H = \langle w, z\rangle$ es no degenerado, pues la matriz de F en la base indicada tiene determinante no nulo, y contiene un vector isótropo, luego tiene que ser un plano hiperbólico y podemos tomar $w' \in H$ tal que (w, w') es un par hiperbólico. Tomemos $s \in C$ no nulo tal que $s + \bar{s} = 0$, con lo que el vector $u = w + sw' \in H$ es isótropo, y al menos dos de los tres vectores u, w, w' no están en $\langle v\rangle^\perp$, pues, como $z \in H$, tenemos que $v \notin H^\perp$, y si v fuera ortogonal a dos de ellos, estaría en $H^\perp$. Por lo tanto, dos de los planos $H_1 = \langle v, u\rangle$, $H_2 = \langle v, w\rangle$, $H_3 = \langle v, w'\rangle$ son hiperbólicos, y su intersección es $\langle v\rangle$ (en caso contrario, dos de ellos serían iguales a H y entonces $z \in \langle v, w\rangle$). ∎

De aquí deducimos a su vez:

Teorema 9.5 *Si V es un espacio unitario isótropo, el centro de* $\mathrm{UE}(V)$ *es el subgrupo* $\mathrm{ZUE}(V) = \mathrm{ZU}(V) \cap \mathrm{UE}(V)$.

Demostración: Si $f \in Z(\mathrm{UE}(V))$, para cada vector isótropo $v \in V$ y cada α tal que $\alpha + \bar{\alpha} = 0$ no nulo, se tiene que cumplir que

$$T_{v,\alpha} = T^f_{v,\alpha} = T_{f(v),\alpha},$$

y al igualar los subespacios de vectores fijos queda que $\langle v\rangle^\perp = \langle f(v)\rangle^\perp$, luego $\langle f(v)\rangle = \langle v\rangle$, y el teorema anterior implica que $f \in \mathrm{ZU}(V)$, luego de hecho $f \in \mathrm{ZUE}(V)$. ∎

Observemos ahora que los grupos unitarios especiales de los planos hiperbólicos no son "nuevos":

Teorema 9.6 *Si V es un plano hiperbólico unitario, entonces*

$$\mathrm{UE}(V) \cong \mathrm{LE}(2, R), \qquad \mathrm{UEP}(V) \cong \mathrm{LEP}(2, R).$$

Demostración: Sea (u, v) un par hiperbólico en V. Entonces los elementos de $\mathrm{UE}(V)$ son los automorfismos de V cuya matriz en la base u, v cumple

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

y además $ad - bc = 1$. Al desarrollar el producto, vemos que esto equivale a que

$$\bar{a}d + \bar{b}c = 1, \quad a\bar{b} + b\bar{a} = 0, \quad c\bar{d} + d\bar{c} = 0, \quad ad - bc = 1.$$

Multiplicamos la primera ecuación por a y sustituimos la segunda y luego la cuarta:

$$a\bar{a}d + a\bar{b}c = a, \quad \Rightarrow \quad a\bar{a}d - bc\bar{a} = a \quad \Rightarrow \quad a\bar{a}d - (ad - 1)\bar{a} = a,$$

con lo que obtenemos que $\bar{a} = a$. Similarmente, multiplicando la primera ecuación por d y sustituyendo la tercera y luego la cuarta obtenemos $\bar{d} = d$. En

cambio, si multiplicamos la primera por b y sustituimos la segunda y la cuarta, el resultado es $\bar{b} = -b$, e igualmente $\bar{c} = -c$. Con esto obtenemos las ecuaciones

$$\bar{a} = a, \quad \bar{d} = d, \quad \bar{b} = -b, \quad \bar{c} = -c, \quad ad - bc = 1,$$

que claramente implican las ecuaciones iniciales. Por 8.2 podemos fijar $s \in C$ tal que $\bar{s} = -s$, y entonces

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & sb \\ s^{-1}c & d \end{pmatrix}$$

define claramente una biyección $\mathrm{LE}(2, R) \longrightarrow \mathrm{UE}(V)$ y se comprueba inmediatamente que es un homomorfismo, luego un isomorfismo de grupos.

Claramente, el isomorfismo hace corresponder el subgrupo $\mathrm{ZE}(2, R)$ de las matrices diagonales de determinante 1 con el subgrupo $\mathrm{ZUE}(V)$, por lo que induce el segundo isomorfismo del enunciado. ∎

Observemos que el isomorfismo del teorema anterior hace corresponder las transvecciones de la forma

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix},$$

—que, según [Al 6.22], constituyen un generador de $\mathrm{LE}(2, q)$— con las transformaciones unitarias con matrices de la forma

$$\begin{pmatrix} 1 & sb \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ s^{-1}c & 1 \end{pmatrix},$$

que no son sino las matrices de las transvecciones $T_{v,sb}$ y $T_{u,c/s}$, que son, de hecho, todas las transvecciones de la forma $T_{u,\alpha}$ y $T_{v,\alpha}$, con $\bar{\alpha} = -\alpha$, pues si α cumple esto, entonces $b = \alpha/s$ o $c = s\alpha$ cumplen $\bar{b} = b$, $\bar{c} = c$, luego $b, c \in R$. Por lo tanto, tenemos probado el teorema siguiente:

Teorema 9.7 *Si V es un plano hiperbólico unitario, el grupo $\mathrm{UE}(V)$ está generado por las transvecciones unitarias.*

Más precisamente, hemos probado que $\mathrm{UE}(V)$ está generado por las transvecciones determinadas por los vectores u, v de un par hiperbólico fijo.

Probaremos que esto es válido para (casi) todo espacio unitario isótropo V, para lo cual conviene definir $\mathfrak{T}(V)$ como el subgrupo de $\mathrm{UE}(V)$ generado por las transvecciones unitarias, de modo que queremos probar que $\mathfrak{T}(V) = \mathrm{UE}(V)$. De momento observamos lo siguiente:

Teorema 9.8 *Si V es un espacio unitario isótropo, el grupo $\mathfrak{T}(V)$ actúa transitivamente sobre Ω.*

Demostración: Tomemos dos puntos $P = \langle u \rangle$, $Q = \langle w \rangle \in \Omega$ y supongamos en primer lugar que $F(u, v) \neq 0$. En tal caso, sustituyendo u por un múltiplo,

podemos suponer que $F(u,v) = 1$. Tomemos $\beta \in C$ no nulo tal que $\beta + \bar{\beta} = 0$. Sea $x = u + \beta v$, de modo que $\mathrm{N}(x) = \beta + \bar{\beta} = 0$. Sea $\alpha = -1/\bar{\beta}$, con lo que también $\alpha + \bar{\alpha} = 0$ y podemos considerar la transvección unitaria $T_{x,\alpha} \in \mathfrak{T}(V)$, que cumple

$$T_{x,\alpha}(u) = u + \alpha F(u,x)x = u - \frac{1}{\bar{\beta}}F(u,\beta v)(u+\beta v) = -\beta v,$$

luego $T_{x,\alpha}(P) = Q$.

Supongamos ahora que $F(u,v) = 0$. No puede ser $V = \langle u\rangle^\perp \cup \langle v\rangle^\perp$ pues, en general, un espacio vectorial nunca es unión de dos subespacios propios.[2] Por lo tanto, podemos tomar $y \in V$ tal que $F(u,y) \neq 0$, $F(v,y) \neq 0$. Cambiando u y v por múltiplos, podemos suponer que $F(u,y) = F(v,y) = 1$. Como antes, podemos elegir $\beta \in C$ tal que $z = y + \beta u$ cumpla $\mathrm{N}(z) = 0$, y además tenemos que $F(u,z) = F(v,z) = 1$, luego tanto (u,z) como (z,v) están en las condiciones del caso anterior, luego, por la parte ya probada, existe una transvección unitaria que cumple $T(P) = \langle z\rangle$ y otra que cumple $T'(\langle z\rangle) = Q$, luego $T \circ T' \in \mathfrak{T}(V)$ transforma P en Q. ∎

En el caso de los planos hiperbólicos podemos decir más:

Teorema 9.9 *Si V es un plano hiperbólico unitario, $\mathfrak{T}(V)$ es doblemente transitivo sobre Ω.*

Demostración: Sea (u,v) un par hiperbólico en V. Basta probar que si $\langle x\rangle, \langle y\rangle \in \Omega$, son puntos distintos, existe un $f \in \mathfrak{T}(V)$ tal que $f(\langle x\rangle) = \langle u\rangle$, $f(\langle y\rangle) = \langle v\rangle$. Por el teorema anterior podemos suponer que $\langle x\rangle = \langle u\rangle$, con lo que buscamos $f \in \mathfrak{T}(V)$ tal que $f(\langle u\rangle) = \langle u\rangle$, $f(\langle y\rangle) = \langle v\rangle$. Pongamos que $y = au + bv$, con lo que $\mathrm{N}(y) = a\bar{b} + \bar{a}b = 0$. Observemos que $b \neq 0$, porque estamos suponiendo que $\langle y\rangle \neq \langle x\rangle = \langle u\rangle$. Sea $c = -a/b$, con lo que $\bar{c} = -c$ y consideramos la transvección $T_{u,c}$, que cumple

$$T_{u,c}(y) = au + bv + cbu = au + bv - ab^{-1}bu = bv,$$

luego $T_{u,c}(\langle y\rangle) = \langle v\rangle$ y, naturalmente, $T_{u,c}(\langle u\rangle) = \langle u\rangle$. ∎

Grupos unitarios proyectivos sobre cuerpos finitos Calculamos ahora los órdenes de los grupos unitarios proyectivos finitos:

Si C es el cuerpo de q^2 elementos, como $\mathrm{ZU}(n,q^2)$ es isomorfo al núcleo de la norma $\mathrm{N} : C^* \longrightarrow R^*$, que es suprayectiva (teorema 8.33), resulta que $|\mathrm{ZU}(n,q^2)| = q+1$, luego, teniendo en cuenta 8.48,

$$|\mathrm{UP}(n,q^2)| = q^{n(n-1)/2}\prod_{i=1}^{n-1}(q^{i+1} - (-1)^{i+1}).$$

[2] Véase la nota al pie en la prueba del teorema 9.4.

Ahora, el subgrupo $\mathrm{ZE}(n,q^2)$ está formado por las matrices escalares αI tales que $\alpha^{q+1}=1$ y $\alpha^n=1$. Esto equivale a que el orden de α divida a $(n,q+1)$ y, teniendo en cuenta que C^* es cíclico de orden q^2-1, tiene un único subgrupo de orden $(n,q+1)$ que tiene contiene a todos los α en estas condiciones, luego $|\mathrm{ZUE}(n,q^2)|=(n,q+1)$, y en consecuencia

$$|\mathrm{UEP}(n,q^2)|=\frac{q^{n(n-1)/2}}{(n,q+1)}\prod_{i=1}^{n-1}(q^{i+1}-(-1)^{i+1}).$$

Los teoremas 9.6 y 7.17 nos dan que los grupos

$$\mathrm{UEP}(2,q^2)\cong\mathrm{LEP}(2,q)\cong\mathrm{SpP}(2,q)$$

son simples salvo $\mathrm{UEP}(2,4)$ y $\mathrm{UEP}(2,9)$. Puede probarse además que

$$\mathrm{UEP}(4,4)\cong\mathrm{SpP}(4,3),$$

y ya no hay más isomorfismos entre ambas familias de grupos simples.

Para $n\geq 3$, los órdenes crecen muy rápidamente:

q	2	3	4	5
$\lvert\mathrm{UEP}(3,q^2)\rvert$	72	6 048	62 400	126 000
$\lvert\mathrm{UEP}(4,q^2)\rvert$	25 920	3 265 920	$\cdots$	

Vemos aquí otra excepción, pues sabemos que no hay grupos simples de orden 72, así que $\mathrm{UEP}(3,4)$ tampoco puede ser simple. Pero ya no hay más excepciones. El grupo $\mathrm{UEP}(3,9)$ es el primero de los dos grupos simples que faltaban en nuestra lista de grupos de orden menor que 25 000 al final de la sección 7.2.

Teorema 9.10 $\mathrm{UEP}(4,4)\cong\mathrm{SpP}(4,3)$.

Demostración: Sea V un espacio unitario de dimensión 4 sobre el cuerpo C de 4 elementos. Notemos que la norma es una aplicación $\mathrm{N}:V\longrightarrow\{0,1\}$. Según el teorema 8.35, el espacio V contiene 120 vectores de norma 1, luego el espacio proyectivo $P(V)$ contiene 40 puntos no isótropos. Llamamos $\Omega\subset P(V)$ al conjunto de estos 40 puntos no isótropos.

Llamamos $\mathcal{L}_0$ a la familia de todos los conjuntos de la forma

$$L=\{\langle e_1\rangle,\langle e_2\rangle,\langle e_3\rangle,\langle e_4\rangle\}\subset\Omega,$$

donde e_1,e_2,e_3,e_4 es una base ortonormal de V.

Si $p=\langle u\rangle$, $q=\langle v\rangle$ son dos puntos de Ω tales que $p\perp q$, entonces $\langle p,q\rangle$ es un subespacio no degenerado, luego también lo es $\langle p,q\rangle^\perp$, que, de nuevo por 8.35, es una recta proyectiva que contiene exactamente 2 puntos no isótropos, r,s, de modo que $L=\{p,q,r,s\}$ es claramente el único elemento de $\mathcal{L}_0$ que contiene a p, q.

Por otro lado, si $p = \langle u\rangle$, $q = \langle v\rangle$ son dos puntos de Ω no ortogonales, el subespacio $\langle u, v\rangle$ es degenerado (pues la matriz de la forma bilineal tiene sus cuatro coeficientes iguales a 1). Se cumple que $\alpha u + \beta v$ es isótropo si y sólo si $\alpha = \beta$, pues

$$F(\alpha u + \beta v, \alpha u + \beta v) = \alpha\bar{\alpha} + \beta\bar{\beta} + \alpha\bar{\beta} + \beta\bar{\alpha} = 0$$

requiere que $\alpha \neq 0 \neq \beta$, con lo que $\alpha\bar{\alpha} = \beta\bar{\beta} = 1$ y entonces $\alpha\bar{\beta} = \beta\bar{\alpha}$, luego $\alpha\bar{\beta} \in R$, luego $\alpha\bar{\beta} = 1 = \beta\bar{\beta}$, luego $\alpha = \beta$.

Así pues, la recta proyectiva $\langle u, v\rangle$ contiene un único punto isótropo y otros cuatro puntos en Ω, que serán no ortogonales dos a dos, ya que si $\langle u, v\rangle$ contuviera dos puntos de norma 1 ortogonales sería un subespacio no degenerado.

Llamamos $\mathcal{L}_1$ a la familia de todos los conjuntos de la forma $L \cap \Omega$, donde L es una recta proyectiva que pasa por dos puntos no ortogonales. Acabamos de probar que cada elemento de $\mathcal{L}_1$ contiene cuatro puntos no ortogonales dos a dos, mientras que cada elemento de $\mathcal{L}_0$ consta de cuatro puntos ortogonales dos a dos.

También tenemos que dos puntos cualesquiera de Ω están en un único elemento de $\mathcal{L}_0$ o de $\mathcal{L}_1$, según si son ortogonales o no.

Para cada $p \in \Omega$, llamamos $p^\circ = \{p\} \cup (P(p^\perp) \cap \Omega)$ al conjunto formado por p y por todos los puntos de Ω ortogonales a p, y llamamos $\mathcal{P}$ a la familia de todos los conjuntos p°.

Vamos a probar que Ω se convierte en un espacio proyectivo (en el sentido de [G 8.10]) tomando como rectas los elementos de $\mathcal{L}_0 \cup \mathcal{L}_1$ y como planos a los elementos de $\mathcal{P}$.

Observemos que $p^\perp$ es un espacio unitario tridimensional que, de nuevo por el teorema 8.35, contiene 12 puntos no isótropos, luego cada plano p° consta de 13 puntos.

Ya hemos probado que por cada par de puntos pasa una única recta (P1) y obviamente toda recta contiene al menos tres puntos (P6), pues contiene cuatro. Como cada plano consta de 13 puntos, ciertamente contiene al menos tres puntos no colineales (P5).

Veamos ahora (P4) que si $q, r \in p^\circ$, la recta que pasa por q y r está contenida en p°. Si uno de los puntos dados es p, por ejemplo, $q = p$, entonces $q \perp r$, luego la recta L que pasa por q y r es de $\mathcal{L}_0$ y consta de puntos ortogonales entre sí, luego $L \subset p^\circ$.

Supongamos ahora que $q \neq p \neq r$, de modo que $q + r \leq p^\perp$. Si q y r no son ortogonales, la recta que pasa por ellos es $P(q + r) \cap \Omega \subset P(p^\perp) \cap \Omega \subset p^\circ$. Falta considerar el caso en que $q \perp r$. Entonces los dos puntos adicionales de la recta L que pasa por ellos son los dos puntos no isótropos de $(q + r)^\perp$, uno de los cuales es p, y sabemos que los cuatro puntos de L son ortogonales entre sí, luego $L \subset p^\circ$.

Veamos ahora (P3) que por tres puntos no colineales q, r, s pasa un único plano. Supongamos que estuvieran contenidos en dos planos p_1° y p_2°. Por el

axioma P_4 ya probado, ambos contendrían las rectas qr, qs, y podemos tomar dos puntos en qr, digamos q' y r' distintos de p_1, p_2. Igualmente tomamos s' en qs distinto de q, p_1, p_2, con lo que q', r', s' son tres puntos no colineales contenidos en ambos planos, pero, más concretamente, están contenidos en $P(p_1^\perp)$ y $P(p_2^\perp)$, luego los subespacios $p_1^\perp$ y $p_2^\perp$ contienen tres vectores linealmente independientes, luego $p_1^\perp = p_2^\perp$, luego $p_1 = p_2$.

Observemos ahora que los 40 puntos $p \in \Omega$ determinan 40 planos distintos, pues si $p_1^\circ = p_2^\circ$, entre los 11 puntos de este plano distintos de p_1 y p_2 tiene que haber tres no colineales (pues una recta sólo contiene 4 puntos), luego $p_1^\perp \cap p_2^\perp$ contiene tres vectores linealmente independientes, luego $p_1^\perp = p_2^\perp$, luego $p_1 = p_2$.

Ahora, en Ω hay $40 \cdot 39 \cdot 36/6 = 9\,360$ ternas de puntos no colineales, y en cada uno de los 40 planos de Ω hay $13 \cdot 12 \cdot 9/6 = 234$ ternas de puntos no colineales, lo que hace un total de $234 \cdot 40 = 9\,360$ ternas contenidas en planos, luego son todas.

Veamos por último el axioma P2, es decir, que dos rectas se cortan si y sólo si son coplanares. Ciertamente, si dos rectas distintas pq y pr se cortan en un punto p, tenemos que los puntos p, q, r no son colineales, luego están contenidos en un plano (por P3), en el cual están contenidas las dos rectas (por P4), luego éstas son coplanares.

Para probar el recíproco necesitamos analizar con más detalle la estructura de un plano p°. Al unir p con cada uno de los 12 puntos de $P(p^\perp) \cap \Omega$ obtenemos rectas de $\mathcal{L}_0$, cada una de las cuales consta de 3 puntos distintos de p, luego hay un total de 4 rectas en Π que pasan por p, y todas ellas son de $\mathcal{L}_0$. Si L es una de ellas, tenemos una base ortonormal e_1, e_2, e_3, e_4 de V tal que $p = \langle e_1 \rangle$, $L = \{\langle e_1 \rangle, \langle e_2 \rangle, \langle e_3 \rangle, \langle e_4 \rangle\}$. Todo punto $r = \langle u \rangle \in \Omega$ es de la forma

$$u = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4$$

con

$$1 = F(u,u) = \alpha_1\bar{\alpha}_1 + \alpha_2\bar{\alpha}_2 + \alpha_3\bar{\alpha}_3 + \alpha_4\bar{\alpha}_4,$$

donde cada sumando está en $R = \{0, 1\}$, luego, o bien hay un único α_i no nulo, en cuyo caso $r = \langle e_i \rangle \in L$, o bien hay tres α_i no nulos, lo que se traduce en que $F(u, e_i) = 0$ para un único índice i, que necesariamente será $i = 1$ si $r \in p^\perp$. Esto se traduce en que los puntos de $p^\circ \setminus L$ no son ortogonales a los puntos de L distintos de p o, equivalentemente, que las rectas de p° que no pasan por p están en $\mathcal{L}_1$.

Consideremos ahora dos rectas contenidas en p° y veamos que son secantes. Si ambas pasan por p la conclusión es obvia. Si una recta L no pasa por p, no puede pasar por dos puntos de una misma recta que pase por p (ya que entonces coincidiría con dicha recta y pasaría por p), luego los cuatro puntos de L pertenecen a cuatro rectas distintas que pasan por p, pero sólo hay cuatro rectas que pasan por p, luego L corta a todas las rectas que pasan por p.

Sólo nos falta probar que dos rectas en p° que no pasen por p son secantes. Ahora bien, se trata de dos rectas de $\mathcal{L}_1$, luego serán de la forma $L_1 \cap \Omega$ y $L_2 \cap \Omega$, donde L_1 y L_2 son planos contenidos en el espacio tridimensional $p^\perp$, luego $L_1 \cap L_2 = \langle u \rangle$, y sólo hay que observar que $q = \langle u \rangle \in \Omega$, pues en caso

contrario sería el único punto isótropo de las rectas L_1 y L_2, que es, de hecho $q = L_1 \cap L_1^\perp = L_2 \cap L_2^\perp$. En tal caso podríamos expresar $L_i = \langle u, v_i\rangle$, de modo que $p^\perp = \langle u, v_1, v_2\rangle$ sería degenerado, pues u sería ortogonal a todos sus elementos, pero $p^\perp$ no es degenerado.

Así pues Ω es un espacio proyectivo, obviamente de dimensión mayor que 2, luego cumple el teorema de Desargues [G 8.14], y en virtud de [G 8.34] existe una colineación entre Ω y un espacio proyectivo $P(W)$, para cierto espacio vectorial W sobre cierto anillo de división K, pero, como las rectas tienen cuatro puntos, K tiene que ser necesariamente el cuerpo de tres elementos. Como Ω tiene 40 puntos, $\dim W = 4$.

Más aún, en Ω tenemos definida una aplicación $p \mapsto p^\circ$ que a cada punto le hace corresponder un (hiper)plano. Si $L \in \mathcal{L}_0$ y $q, r \in L$, es fácil ver que $L^\circ = q^\circ \cap r^\circ = L$, mientras que si $L \in \mathcal{L}_1$ entonces $L^\circ = q^\circ \cap r^\circ = (q+r)^\perp \cap \Omega$, donde $q + r$ es la única recta proyectiva de $P(V)$ que contiene a L, por lo que la definición de L° no depende de la elección de los puntos q, r, y es una recta de $\mathcal{L}_1$ (pues está contenida en q° y no pasa por q). Notemos que $L^{\circ\circ} = L$.

Por último, es fácil ver que si definimos $p^{\circ\circ}$ como la intersección de todos los planos q° con $q \in p^\circ$ obtenemos simplemente $p^{\circ\circ} = p$.

Así hemos definido en Ω una correlación en el sentido de [G 8.37] y, como el cuerpo de tres elementos no tiene automorfismos no triviales, [G 8.47] nos da que se trata de una correlación proyectiva, lo que se traduce en que existe una forma bilineal no degenerada $G : W \times W \longrightarrow K$ tal que, para todo $w \in W$,

$$\langle w\rangle^\circ = P(\{v \in W \mid G(w, v) = 0\}).$$

Más aún, como $p \in p^\circ$ para todo punto p, tenemos que $G(w, w) = 0$ para todo $w \in W$, lo que significa que G es alternada, luego dota a W de estructura de espacio simpléctico y $\mathrm{Sp}(W) = \mathrm{Sp}(4, 3)$.

Más explícitamente, ahora tenemos que p° es lo mismo que $p^\perp$ respecto a la forma G (no respecto de F) y en particular dos puntos $p, q \in \Omega$ son ortogonales respecto a G si y sólo si $q \in p^\circ$.

Ahora basta observar que toda la estructura simpléctica de W ha sido definida a partir de la estructura unitaria de V, por lo que cada $f \in \mathrm{UP}(V)$, vista como homografía de $P(V)$, se restringe a una colineación, luego una homografía, de $P(W)$ (por el teorema fundamental de la geometría proyectiva [G 8.27], teniendo en cuenta una vez más que K no tiene automorfismos no triviales). Más aún, es una homografía que conserva la ortogonalidad respecto a G. Pongamos que $f|_\Omega$ está inducida por $f_0 : W \longrightarrow W$. Entonces

$$G(f_0(u), f_0(v)) = 0 \text{ si y sólo si } G(u, v) = 0,$$

luego $G(f_0(u), f_0(v)) = \epsilon_{uv} G(u, v)$ con $\epsilon = \pm 1$, si $G(u, v) \neq 0$. Si e_1, e_2, e_3, e_4 es una base de W tal que (e_1, e_2) y (e_3, e_4) sean pares hiperbólicos ortogonales,

$$G(\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4, \beta_1 e_1 + \beta_2 e_2 + \beta_3 e_3 + \beta_4 e_4) =$$

$$\alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_4 - \alpha_4\beta_3 = 0$$

si y sólo si

$$G(f_0(\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4), f_0(\beta_1 e_1 + \beta_2 e_2 + \beta_3 e_3 + \beta_4 e_4)) =$$

$$\epsilon_{12}\alpha_1\beta_2 - \epsilon_{21}\alpha_2\beta_1 + \epsilon_{34}\alpha_3\beta_4 - \epsilon_{43}\alpha_4\beta_3 = 0.$$

Tomando $\alpha_1 = \beta_1 = \alpha_2 = \beta_2 = 1$, $\alpha_3 = \alpha_4 = \beta_3 = \beta_4$ obtenemos que $\epsilon_{12} = \epsilon_{21}$, mientras que con $\alpha_1 = \alpha_3 = \beta_2 = 1$, $\beta_4 = -1$, $\alpha_2 = \alpha : 4 = \beta_1 = \beta_3 = 0$ obtenemos que $\epsilon_{12} = \epsilon_{34}$, e igualmente llegamos a que $\epsilon_{12} = \epsilon_{43}$. Llamando ϵ_f a este valor común, concluimos que

$$G(f_0(u), f_0(v)) = \epsilon_f G(u, v),$$

para todo $u, v \in W$. Por otra parte, la aplicación

$$\mathrm{UEP}(4,4) \longrightarrow \{\pm 1\}$$

dada por $f \mapsto \epsilon_f$ es claramente un homomorfismo de grupos, pero $\mathrm{UEP}(4,4)$ es simple, luego tiene que ser el homomorfismo trivial, es decir, $\epsilon_f = 1$ para todo f, y así $f_0 \in \mathrm{Sp}(W)$, con lo que $f|_\Omega \in \mathrm{SpP}(W)$. Tenemos así un homomorfismo de grupos

$$\mathrm{UEP}(4,4) \longrightarrow \mathrm{SpP}(4,3)$$

que tiene que ser inyectivo de nuevo porque $\mathrm{UEP}(4,4)$ es simple, y como ambos grupos tienen el mismo orden, se trata de un isomorfismo. ∎

La parametrización de Wall En esta apartado probaremos unos hechos generales sobre transformaciones unitarias que nos permitirán probar, entre otras cosas, que el grupo $\mathrm{U}(V)$ está generado por las dilataciones y las transvecciones unitarias.

Si V es un espacio unitario, para cada transformación $f \in \mathrm{U}(V)$ definimos $\hat{f} = 1 - f$ y $V_f = \operatorname{Im} \hat{f}$, de modo que $\hat{f} : V \longrightarrow V_f$ es un epimorfismo.

Es fácil comprobar (sin más que desarrollar ambos miembros) que

$$F(\hat{f}(x), \hat{f}(y)) = F(\hat{f}(x), y) + F(x, \hat{f}(y)).$$

Definimos $F_f : V_f \times V_f \longrightarrow C$ mediante

$$F_f(\hat{f}(x), \hat{f}(y)) = F(x, \hat{f}(y)).$$

La definición es correcta, pues si $\hat{f}(x) = \hat{f}(x')$, $\hat{f}(y) = \hat{f}(y')$, entonces

$$F(x, \hat{f}(y)) = F(x, \hat{f}(y')) = F(\hat{f}(x), \hat{f}(y')) - F(\hat{f}(x), y') =$$

$$F(\hat{f}(x'), \hat{f}(y')) - F(\hat{f}(x'), y') = F(x', \hat{f}(y')).$$

Es inmediato que F_f es una forma sesquilineal en V_f (respecto del mismo automorfismo que F), pero no es hermitiana, sino que cumple la relación

$$F_f(u,v) + \overline{F_f(v,u)} = F(u,v).$$

No obstante, F_f no es degenerada, pues si $F_f(u,v) = 0$ para todo $u \in V_f$, entonces, haciendo $u = \hat{f}(x)$, tenemos que $F(x,v) = 0$ para todo $x \in V$, luego $v = 0$.

Por consiguiente, si $\hat{B}_f$ es la matriz de F_f en una base $v_1, \ldots, v_r$ de V_f, su determinante es no nulo y podemos considerar su inversa $A = (a_{ij}) = \hat{B}_f^{-1}$.

Dado $x \in V$, podemos expresar $\hat{f}(x) = \lambda_1 v_1 + \cdots + \lambda_r v_r$, y entonces

$$F(x, v_j) = F_f(\hat{f}(x), v_j) = \sum_{i=1}^{r} \lambda_i F_f(v_i, v_j).$$

Así:

$$(F(x,v_1), \ldots, F(x,v_r)) = (\lambda_1, \ldots, \lambda_r)\hat{B}_f^{-1},$$

luego

$$(\lambda_1, \ldots, \lambda_r) = (F(x,v_1), \ldots, F(x,v_r))A$$

o, explícitamente,

$$\lambda_j = \sum_{i=1}^{r} F(x, v_i) a_{ij}.$$

Por lo tanto,

$$x - f(x) = \hat{f}(x) = \sum_{i,j=1}^{r} F(x, v_i) a_{ij} v_j,$$

y así concluimos que, para todo $x \in V$, la transformación unitaria f viene dada por

$$f(x) = x - \sum_{i,j=1}^{r} F(x, v_i) a_{ij} v_j.$$

En particular, f es la identidad en $V_f^\perp$.

Teorema 9.11 *Sea V un espacio unitario, sea $W \leq V$ y sea G una forma sesquilineal no degenerada en W tal que, para todo $u, v \in W$, se cumple*

$$G(u,v) + \overline{G(v,u)} = F(u,v).$$

Entonces existe una única $f \in \mathrm{U}(V)$ tal que $V_f = W$ y $F_f = G$.

Demostración: El razonamiento precedente prueba que si existe f, es única, pues, fijada una base $v_1, \ldots, v_r$ de W, tiene que venir dada por

$$f(x) = x - \sum_{i,j=1}^{r} F(x, v_i) a_{ij} v_j,$$

donde $A = (a_{ij})$ es la matriz inversa de la matriz B de G en la base dada. Por lo tanto, sólo tenemos que probar que f así definida cumple lo requerido.

Si $u, v \in W$ tienen coordenadas x, y, la relación del enunciado afirma que

$$xB\bar{y}^t + \overline{yB\bar{x}^t} = x(F(v_i, v_j))\bar{y}^t,$$

o también

$$xB\bar{y}^t + x\bar{B}^t\bar{y}^t = x(F(v_i, v_j))\bar{y}^t,$$

y, como esto vale para todo $x, y \in C^r$, tiene que ser $B + \bar{B}^t = (F(v_i, v_j))$, o también

$$A^{-1} + \overline{(A^t)^{-1}} = (F(v_i, v_j)),$$

luego

$$A(F(v_i, v_j))\bar{A}^t = A + \bar{A}^t.$$

Claramente f es una aplicación lineal. Además,

$$F(f(x), f(y)) = F(x, y) - \sum_{ij} F(x, v_i)a_{ij}F(v_j, y) - \sum_{kl} F(v_k, y)\bar{a}_{kl}F(x, v_l)$$

$$+ \sum_{ijkl} F(x, v_i)a_{ij}F(v_j, v_l)\bar{a}_{kl}F(v_k, y).$$

En el segundo sumatorio podemos cambiar los índices k, l por j, i, y en el tercero podemos cambiar los índices j y k. El resultado es

$$F(f(x), f(y)) = F(x, y) - \sum_{ij} F(x, v_i)a_{ij}F(v_j, y) - \sum_{ij} F(v_j, y)\bar{a}_{ji}F(x, v_i)$$

$$+ \sum_{ijkl} F(x, v_i)a_{ik}F(v_k, v_l)\bar{a}_{jl}F(v_j, y) =$$

$$F(x, y) - \sum_{ij} F(x, v_i)(a_{ij} + \bar{a}_{ji})F(v_j, y) + \sum_{ij} F(x, v_i)\sum_{kl}(a_{ik}F(v_k, v_l)\bar{a}_{jl})F(v_j, y)$$

y los dos últimos términos se anulan, por la relación que hemos probado para la matriz A. Esto implica que f es un monomorfismo (luego un automorfismo), pues si $f(x) = 0$, entonces $F(x, y) = F(0, f(y)) = 0$ para todo $y \in V$, luego $x = 0$. Así pues, $f \in \mathrm{U}(V)$. Además

$$\hat{f}(x) = \sum_{i,j=1}^{r} F(x, v_i)a_{ij}v_j \in W,$$

luego $V_f \leq W$. Por 8.5 podemos tomar $x_k \in V$ tal que $F(v_i, x_k) = G(v_i, v_k)$, y así también $F(x_k, v_i) = G(v_k, v_i)$, con lo que, llamando (δ_{kj}) a la matriz identidad I_r,

$$\hat{f}(x_k) = \sum_{j=1}^{r}\sum_{i=1}^{r} G(v_k, v_i)a_{ij}v_j = \sum_{j=1}^{r} \delta_{kj}v_j = v_k,$$

luego $V_f = W$. Por último,

$$F_f(v_k, v_i) = F(x_k, v_i) = G(v_k, v_i),$$

luego $F_f = G$. ∎

Definición 9.12 Llamaremos $f_{W,G}$ a la función dada por el teorema anterior.

Por ejemplo, si $W = \langle u\rangle$ y $\alpha = G(u,u)^{-1}$, la que debe cumplir G según el teorema anterior se traduce en que $\alpha^{-1} + \bar{\alpha}^{-1} = \mathrm{N}(u)$. Si u es isótropo, queda $\bar{\alpha} = -\alpha$, y

$$f_{W,G}(v) = x - \alpha F(x,u)u = T_{u,-\alpha}(v).$$

Si u es anisótropo, es $\alpha + \bar{\alpha} = \alpha\bar{\alpha} = \mathrm{N}(u)$ y

$$f_{W,G}(v) = x - \alpha F(x,u)u = x - \alpha\,\mathrm{N}(u)\frac{F(x,u)}{F(u,u)}u = D_{u,\beta}(x),$$

donde $\beta = 1 - \alpha\,\mathrm{N}(u)$ cumple $\beta\bar{\beta} = 1$.

Podemos decir que hemos parametrizado el grupo $\mathrm{U}(V)$ en términos de pares (W,G). Podría pensarse que los parámetros son más complicados que los objetos parametrizados, pero el teorema siguiente muestra la utilidad de expresar las transformaciones unitarias en términos de subespacios y formas hermitianas:

Teorema 9.13 *Sea V un espacio unitario, sea $f \in \mathrm{U}(V)$, sea $W_1 \leq V_f$ un subespacio no degenerado (respecto de F_f) y sea $W_2 = {}^{\perp}W_1$ y sean $f_1, f_2 \in \mathrm{U}(V)$ las transformaciones unitarias asociadas a $(W_i, F_f|_{W_i})$. Entonces $f = f_1 f_2$.*

Demostración: Que W_1 sea no degenerado equivale a que si $w_1 \in W_1$ cumple $F_f(w_1, w) = 0$ para todo $w \in W_1$ entonces $w_1 = 0$, lo cual equivale a que $W_1 \cap W_2 = 0$, luego $W = W_1 \oplus W_2$.

Formemos una base de W uniendo una base $u_1, \ldots, u_s$ de W_1 con otra $v_1, \ldots, v_t$ de W_2. Así, la matriz de F_f en dicha base es de la forma

$$B = \begin{pmatrix} L & N \\ 0 & M \end{pmatrix},$$

donde L y M son las matrices de las restricciones de F_f a W_1 y F_2, mientras que N tiene en posición (i,j) el coeficiente

$$F_f(u_i, v_j) = F(u_i, v_j) - \overline{F_f(v_j, u_i)} = F(u_i, v_j).$$

Llamemos $L^{-1} = (a_{ij})$, $M^{-1} = (b_{ij})$, con lo que

$$\begin{pmatrix} L & N \\ 0 & M \end{pmatrix}^{-1} = \begin{pmatrix} L^{-1} & -L^{-1}NM^{-1} \\ 0 & M^{-1} \end{pmatrix}.$$

Si $x \in V$, tenemos que

$$f_1(x) = x - \sum_{ij} F(x,u_i)a_{ij}u_j, \qquad f_2(x) = x - \sum_{kl} F(x,v_k)b_{kl}v_l,$$

luego

$$f_2(f_1(x)) = f_2\left(x - \sum_{ij} F(x,u_i)a_{ij}u_j\right) = x - \sum_{ij} F(x,u_i)a_{ij}u_j$$

$$- \sum_{kl} F(x,v_k)b_{kl}v_l + \sum_{ijkl} F(x,u_i)(a_{ij}F(u_j,v_k)b_{kl})v_k = f(x),$$

pues $\sum_{jk} a_{ij}F(u_j,v_k)b_{kl}$ es el término (i,l) de $L^{-1}NM^{-1}$. ∎

Como consecuencia:

Teorema 9.14 *Si V es un espacio unitario, todo $f \in \mathrm{U}(V)$, $f \neq 1$ se descompone como $f = f_1 \cdots f_r$, donde cada f_i es una transvección o una dilatación. Además, el vector u que determina f_1 puede elegirse arbitrariamente con tal de que $F_f(u,u) \neq 0$.*

Demostración: Observemos en general que si G es una forma sesquilineal en un espacio vectorial W (respecto de una conjugación de orden 2) y no es idénticamente nula, existe $w \in W$ tal que $G(w,w) \neq 0$. En efecto, en principio existen $u, v \in W$ tales que $G(u,v) \neq 0$, y podemos tomarlos con $G(u,v) = 1$. Si todos los vectores fueran isótropos,

$$0 = G(u + \alpha v, u + \alpha v) = \alpha G(v,u) + \bar{\alpha}.$$

Haciendo $\alpha = 1$ queda $G(v,u) = -1$, luego todo escalar α cumple $\bar{\alpha} = \alpha$, lo que contradice que la conjugación tiene orden 2.

Probamos el teorema por inducción sobre la dimensión de V_f. Si $V_f = 0$ es que $f = 1$ y no hay nada que probar. En otro caso tomamos cualquier vector $u \in V_f$ con $F_f(u,u) \neq 0$ y llamamos $W_1 = \langle u \rangle$, $W_2 = {}^{\perp}W_1$. Así $V_f = W_1 \oplus W_2$ y el teorema 9.13 nos da una descomposición $f = f_1 f'$, donde f_1 está asociada a W_1 y es, por consiguiente, una transvección o una dilatación según si u es isótropo o anisótropo, y f' está asociada a W_2, que tiene dimensión menor que la de V_f, luego por hipótesis de inducción es producto de transvecciones y dilataciones. ∎

Veamos otra aplicación de la parametrización de Wall:

Teorema 9.15 *Si V es un espacio unitario isótropo, entonces $\mathfrak{T}(V)$ actúa transitivamente sobre el conjunto de los planos hiperbólicos de V, salvo a lo sumo en el caso* $\dim V = 3$ *y* $|C| = 4$.

Demostración: Si V es un plano hiperbólico es trivial, así que podemos suponer que $\dim V = n \geq 3$. Consideremos dos planos hiperbólicos $H = \langle u, v \rangle$ y $H_1 = \langle u_1, v_1 \rangle$. Buscamos $f \in \mathfrak{T}(V)$ tal que $f[H_1] = H$. Por el teorema 9.8, no perdemos generalidad si suponemos que $u_1 = u$. Si $H_1 = H$ nos sirve $f = 1$, así que podemos suponer que $\dim(H + H_1) = 3$. Entonces $F(v_1, v) \neq 0$, pues en caso contrario el índice de Witt de $H + H_1$ sería $m \geq 2$ y la dimensión tendría que ser al menos 4. Por lo tanto, $H + H_1 = \langle u, v, w \rangle$, donde $w = au + v - v_1$, con $a = F(v_1, v)$. Es fácil ver que

$$w \perp u, \qquad w \perp v, \qquad F(v_1, w) = a + \bar{a}, \qquad F(w,w) = -(a + \bar{a}).$$

Llamemos $W = \langle u, w \rangle$ y consideramos la forma sesquilineal G en W que en la base u, w tiene matriz

$$B = \begin{pmatrix} 0 & 1 \\ -1 & -\bar{a} \end{pmatrix}.$$

Así

$$B + \bar{B}^t = \begin{pmatrix} 0 & 0 \\ 0 & -(a+\bar{a}) \end{pmatrix},$$

que coincide con la matriz de F en dicha base. El teorema 9.11 nos da la transformación $f = f_{W,G} \in \mathrm{U}(V)$. Explícitamente,

$$A = B^{-1} = \begin{pmatrix} -\bar{a} & -1 \\ 1 & 0 \end{pmatrix},$$

luego

$$f(x) = x + F(x,u)\bar{a}u + F(x,u)w - F(x,w)u.$$

En particular $f(u) = u$, $f(v_1) = v_1 + \bar{a}u + w - (a+\bar{a})u = v$, luego $f[H] = H_1$. Tenemos que demostrar que $f \in \mathfrak{T}(V)$.

Sea $W_1 = \langle w \rangle$ y $W_2 = {}^{\perp}W_1 = \langle \bar{a}u + w \rangle$, de modo que el teorema 9.13 nos da una descomposición $f = f_1 f_2$, donde cada f_i es una dilatación o una transvección según si los vectores w y $\bar{a}u + w$ son anisótropos o isótropos. Más precisamente, si w es isótropo, entonces W es totalmente isótropo, luego f_1, f_2 son transvecciones y el teorema queda probado. A partir de aquí suponemos, pues, que $F(w,w) = -(a+\bar{a}) \neq 0$, con lo que, según las observaciones tras la definición 9.12,

$$\alpha^{-1} = G(w,w) = -\bar{a}, \quad \mathrm{N}(w) = -(a+\bar{a}), \quad 1 - \alpha\,\mathrm{N}(w) = -a\bar{a}^{-1},$$

con lo que $f_1 = D_{w,-a\bar{a}^{-1}}$,

$$\alpha^{-1} = G(\bar{a}u+w, \bar{a}u+w) = -a, \ \mathrm{N}(\bar{a}u+w) = -(a+\bar{a}), \ 1-\alpha\,\mathrm{N}(\bar{a}u+w) = -a^{-1}\bar{a},$$

con lo que $f_2 = D_{\bar{a}u+w,-a^{-1}\bar{a}}$.

Para terminar la prueba vamos a encontrar $g \in \mathfrak{T}(V)$ tal que $f_2 = g^{-1}f_1^{-1}g$, con lo que $f = f_1 f_2 = f_1 g^{-1} f_1^{-1} g = (g^{-1})^{f_1^{-1}} g \in \mathfrak{T}(V)$.

En primer lugar suponemos que $|C| \neq 4$, con lo que $|R| \neq 2$ y podemos tomar $c \in R \setminus \{0,1\}$. Definimos

$$\beta = \frac{(1-c)a}{c(a+\bar{a})}$$

y tomamos $\alpha \in C$ tal que $\alpha + \bar{\alpha} = \beta\bar{\beta}(a+\bar{a})$. Sea $w_1 = \alpha u + v + \beta w$. Un cálculo rutinario muestra que (u, w_1) es un par hiperbólico. Consideremos en $H_2 = \langle u, w_1 \rangle$ la forma sesquilineal que en dicho par tiene matriz

$$G' = \begin{pmatrix} 0 & 1-c^{-1} \\ c^{-1} & 0 \end{pmatrix},$$

de modo que $G' + \bar{G}'^t$ es la matriz de F en (u, w_1). Por lo tanto, el teorema 9.11 nos da la transformación $g = f_{H_2,G'} \in \mathrm{U}(V)$. Como

$$A = G'^{-1} = \begin{pmatrix} 0 & c \\ c(c-1)^{-1} & 0 \end{pmatrix},$$

se cumple que

$$g(x) = x - F(x,u)cw_1 - F(x,w_1)\frac{c}{c-1}u.$$

En particular $g(u) = (1-c)^{-1}u$, $g(w_1) = (1-c)w_1$, y g fija a todos los vectores de $H_2^\perp$, luego el determinante de g respecto de la base u, w_1 completada con una base de $H_2^\perp$ vale 1, luego $g \in \mathrm{UE}(V)$. Más precisamente, $g|_{H_2} \in \mathrm{UE}(H_2)$, luego por 9.7 es composición de transvecciones de H_2, cada una de las cuales se extiende a una transvección de V que fija a los vectores de $H_2^\perp$, luego g es la composición de dichas extensiones, y así $g \in \mathfrak{T}(V)$. Además

$$g(w) = w - F(w,w_1)\frac{c}{c-1}u = w - F(w,\alpha u + v + \beta w)\frac{c}{c-1}u = \bar{a}u + w,$$

luego

$$(f_1^{-1})^g = (D_{w,-a^{-1}\bar{a}})^g = D_{g(w),-a^{-1}\bar{a}} = D_{\bar{a}u+w,-a^{-1}\bar{a}} = f_2,$$

y esto completa la prueba cuando $|C| \neq 4$.

Si $|C| = 4$ suponemos $n \geq 4$ y el índice de Witt cumple $n = 2m$ o bien $n = 2m+1$, luego en cualquier caso $m \geq 2$, por lo que $H^\perp$ es un espacio unitario isótropo de dimensión al menos 2. La relación $-(a+\bar{a}) \neq 0$ se reduce en este caso a $\bar{a} \neq a$.

Tenemos que $w \in H^\perp$ no es isótropo, pero en la prueba del teorema 9.4 hemos visto que $\langle w \rangle$ es intersección de dos planos hiperbólicos de $H^\perp$, luego en particular podemos tomar $u' \in H^\perp$ isótropo tal que $\langle w, u' \rangle$ sea un plano hiperbólico y, cambiándolo por un múltiplo, podemos exigir que $F(w,u') = \bar{a}$. Llamemos $v' = \bar{a}^{-1}(w - u')$, de modo que (u', v') es un par hiperbólico de modo que $w = u' + \bar{a}v'$. En este caso tomamos $g = T_{u+u',1}T_{u',1} \in \mathfrak{T}(V)$, de modo que

$$g(w) = T_{u',1}(w + F(w,u+u')(u+u')) = T_{u',1}(w + \bar{a}(u+u')) =$$

$$w + \bar{a}(u+u') + F(w+\bar{a}(u+u'),u')u' = w + \bar{a}u + \bar{a}u' + \bar{a}u' = \bar{a}u + w.$$

A partir de aquí concluimos igual que en el caso anterior. ∎

Combinando este teorema con 9.9 concluimos:

Teorema 9.16 *Si V es un espacio unitario isótropo, el grupo $\mathfrak{T}(V)$ actúa transitivamente sobre los pares hiperbólicos de V salvo a lo sumo en el caso en que $\dim V = 3$ y $|C| = 4$.*

Finalmente podemos probar:

Teorema 9.17 *Si V es un espacio unitario isótropo, el grupo $\mathrm{UE}(V)$ está generado por las transvecciones unitarias salvo a lo sumo en el caso de $\mathrm{UE}(3,4)$.*

Demostración: Vamos a razonar por inducción sobre $n = \dim V$ (que, al ser V isótropo, es $n \geq 2$), pero la excepción del teorema anterior nos obliga a tratar aparte el caso en que $\dim V = 4$ y $|C| = 4$. En este caso podemos descomponer $V = H_1 \perp H_2$, donde H_1 y H_2 son planos hiperbólicos. Dada

$f \in \mathrm{UE}(V)$, se cumplirá que $f[H_1]$ es un plano hiperbólico, luego, por el teorema anterior, existe $T \in \mathfrak{T}(V)$ tal que $T[f[H_1]] = H_1$. Basta probar que $f \circ T \in \mathfrak{T}(V)$, luego no perdemos generalidad si suponemos que $f[H_1] = H_1$, en cuyo caso, como f conserva la ortogonalidad,

$$f[H_2] = f[H_1^\perp] = H_1^\perp = H_2.$$

Por lo tanto, la transformación f se restringe a dos transformaciones unitarias $f|_{H_i} : H_i \longrightarrow H_i$. Por 9.7 cada una de ellas es producto de transvecciones, y cada transvección de H_i se extiende claramente a una transvección de V que fija a $H_i^\perp$, luego $f|_{H_i}$ se extiende a un elemento $T_i \in \mathfrak{T}(V_i)$ que fija a $H_i^\perp$, y entonces $f = T_1 \circ T_2 \in \mathfrak{T}(V)$, pues ambas transformaciones unitarias coinciden en H_1 y en H_2, luego en H.

Empezamos la inducción: Si $n = 2$ entonces V es un plano hiperbólico y el teorema 9.7 nos da la conclusión. Por lo tanto, podemos suponer que $n \geq 3$. Más aún, si $|C| = 4$ podemos suponer que $n \geq 5$, pues en el caso $n = 3$ no hay nada que probar y el caso $n = 4$ ya lo hemos demostrado.

Como V es isótropo, contiene un plano hiperbólico P. Como $n \geq 3$ podemos tomar $x \in P^\perp$ anisótropo no nulo. Así $\langle x\rangle^\perp$ es no degenerado e isótropo, pues contiene a P. En la prueba del teorema 9.4 hemos visto que si $n \geq 3$ todo subespacio $\langle x\rangle$ es intersección de dos planos hiperbólicos. Por lo tanto, podemos tomar un plano hiperbólico $H \leq V$ tal que $x \in H$.

Dado $f \in \mathrm{UE}(V)$, el teorema 9.15 nos da $g \in \mathfrak{T}(V)$ tal que $g[f[H]] = H$. Basta probar que $fg \in \mathfrak{T}(V)$, luego no perdemos generalidad si suponemos que $f[H] = H$. Por 9.8 existe $g \in \mathfrak{T}(H)$ que cumple $g(f(x)) = x$. Las transvecciones en que se descompone g se pueden extender a transvecciones de V que fijan a $H^\perp$, con lo que g se extiende a $g \in \mathfrak{T}(V)$ y $(fg)(x) = x$, $(fg)[H] = H$. Por lo tanto, no perdemos generalidad si suponemos que $f(x) = x$. Esto hace que $f|_{\langle x\rangle^\perp} \in \mathrm{UE}(\langle x\rangle^\perp)$ (pues la matriz de f en una base que extienda a x con vectores de $\langle x\rangle^\perp$ tiene ceros en su primera fila y columna, salvo un 1 en la posición $(1,1)$, luego el determinante de la restricción es el mismo que el de f).

Por hipótesis de inducción $f|_{\langle x\rangle^\perp}$ es producto de transvecciones de $\langle x\rangle^\perp$, cada una de las cuales se extiende a una transvección de V que fija a x, luego el producto de las extensiones es f. ∎

Es inmediato comprobar que si $f \in \mathrm{U}(V)$,

$$T_{\lambda z,\alpha} = T_{z,\lambda\bar{\lambda}\alpha}, \qquad T_{z,\alpha} \circ T_{z,\beta} = T_{z,\alpha+\beta}.$$

Esto implica que si $P = \langle z\rangle \in \Omega$, el conjunto

$$A_P = \{T_{z,\alpha} \mid \alpha \in C,\ \alpha + \bar{\alpha} = 0\}$$

no depende de la elección de z y es un subgrupo normal abeliano del estabilizador de P en $\mathrm{UE}(V)$ (es isomorfo al núcleo de la traza $\mathrm{Tr} : C \longrightarrow R$).

Si $P = \langle z\rangle \in \Omega$ y z' es cualquier vector isótropo de V, el teorema 9.8 nos da una transformación unitaria $f \in \mathrm{U(E)}$ tal que $f(z) = z'$, con lo que $T_{z,\alpha}^f = T_{z',\alpha}$,

y así los conjugados de A_P contienen todas las transvecciones, luego, salvo en el caso exceptuado en el teorema anterior, la envoltura normal de A_P en $\mathrm{UE}(V)$ es todo $\mathrm{UE}(V)$. Si llamamos $\bar{A}_P$ a la imagen de A_P en $\mathrm{UEP}(V)$, sigue siendo un subgrupo normal abeliano del estabilizador de P y su envoltura normal es $\mathrm{UEP}(V)$, como requiere el teorema de Iwasawa.

Subgrupos derivados Ya hemos visto que el centro de $\mathrm{UE}(V)$ es $\mathrm{ZE}(V)$, y ahora vamos a comprobar que, salvo en unos pocos casos excepcionales, su derivado es él mismo. Necesitamos tratar dos casos aparte:

Teorema 9.18 $\mathrm{UE}(3,9)' = \mathrm{UE}(3,9)$.

Demostración: Sea V un espacio unitario de dimensión 3 sobre el cuerpo C de 9 elementos y sea $T = T_{u,\alpha}$ una transvección. Podemos formar un plano hiperbólico $H = \langle u, v\rangle$ y entonces $V = H \perp \langle w\rangle$, donde podemos suponer que $\mathrm{N}(w) = 1$. La matriz de T en la base u, v, w es

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Tomemos $\beta \in C$ tal que $\beta\bar{\beta} = -1$, sea $\gamma = -\beta^{-2}$ y observemos que la matriz

$$\begin{pmatrix} \beta & 0 & 0 \\ 0 & -\beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$$

corresponde a una transformación $f \in \mathrm{UE}(V)$, pues

$$\begin{pmatrix} \beta & 0 & 0 \\ 0 & -\beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} \bar{\beta} & 0 & 0 \\ 0 & -\bar{\beta} & 0 \\ 0 & 0 & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Por otro lado calculamos el conmutador $[T_{u,-\alpha/2}, f]$, cuya matriz es

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha/2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} \beta^{-1} & 0 & 0 \\ 0 & -\beta^{-1} & 0 \\ 0 & 0 & \gamma^{-1} \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ -\alpha/2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} \beta & 0 & 0 \\ 0 & -\beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} =$$

$$\begin{pmatrix} \beta^{-1} & 0 & 0 \\ \alpha\beta^{-1}/2 & -\beta^{-1} & 0 \\ 0 & 0 & \gamma^{-1} \end{pmatrix}\begin{pmatrix} \beta & 0 & 0 \\ -\alpha\beta/2 & -\beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

luego $T_{u,\alpha} = [T_{u,-\alpha/2}, f] \in \mathrm{UE}(V)'$. Ahora basta tener en cuenta que las transvecciones generan $\mathrm{UE}(V)$ (teorema 9.17). ∎

Teorema 9.19 $\mathrm{UE}(4,4)' = \mathrm{UE}(4,4)$.

DEMOSTRACIÓN: Sea V un espacio unitario de dimensión 4 sobre el cuerpo de 4 elementos. Observemos que todas las transvecciones unitarias de V son de la forma $T_{u,1}$, para cierto vector isótropo u. Sea v otro vector isótropo tal que $H = \langle u, v\rangle$ sea un plano hiperbólico, sea $v_1 \in H$ un vector de norma 1. Sea $\lambda = F(u, v_1)$. Se cumple $\lambda \neq 0$, o de lo contrario la matriz de la forma hermitiana en la base u, v_1 tendría determinante 0. El vector λv_1 también tiene norma 1 y $F(u, \lambda v_1) = 1$, luego podemos suponer que $F(u, v_1) = 1$. Entonces $v_2 = u + v_1$ también tiene norma 1 y $F(v_1, v_2) = 0$. Completamos hasta una base ortonormal v_1, v_2, v_3, v_4, respecto a la cual $u = v_1 + v_2$ y la matriz de $T_{u,1}$ es

$$\begin{pmatrix} 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Basta probar que esta matriz está en $\mathrm{UE}(4,4)'$. Para ello, si $C = \{0, 1, \alpha, \beta\}$, donde $\beta = \alpha^2$, consideramos las matrices

$$P = \begin{pmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & \alpha & 0 & 0\\ \beta & 0 & 0 & 0 \end{pmatrix},$$

$$R = \begin{pmatrix} 0 & 0 & 0 & 1\\ 1 & \beta & 1 & 0\\ 1 & \alpha & \alpha & 0\\ \alpha & \alpha & 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & \beta & \beta & \beta\\ 1 & 0 & \alpha & \alpha\\ \beta & 1 & 0 & 1\\ 1 & \alpha & \alpha & 0 \end{pmatrix}.$$

Se comprueba que las cuatro son unitarias, así como que

$$[P, Q] = \begin{pmatrix} \beta & 0 & 0 & 0\\ 0 & \alpha & 0 & 0\\ 0 & 0 & \beta & 0\\ 0 & 0 & 0 & \alpha \end{pmatrix}, \quad [R, S] = \begin{pmatrix} 0 & \alpha & 0 & 0\\ \beta & 0 & 0 & 0\\ 0 & 0 & \alpha & 0\\ 0 & 0 & 0 & \beta \end{pmatrix},$$

de donde a su vez $[P, Q][R, S] \in \mathrm{UE}(4,4)'$ es la matriz de $T_{u,1}$.

Así, todas las transvecciones están en $\mathrm{UE}(V)'$ y, como éstas generan el grupo, se tiene la igualdad del enunciado. ∎

Teorema 9.20 *Si V es un espacio unitario isótropo,* $\mathrm{UE}(V)' = \mathrm{UE}(V)$ *salvo a lo sumo en los casos* $\mathrm{UE}(2,4)$, $\mathrm{UE}(2,9)$, $\mathrm{UE}(3,4)$.

DEMOSTRACIÓN: El caso $n = 2$ nos lo dan los teoremas 9.6 y 7.16. Para $n \geq 3$, en virtud del teorema 9.17, basta probar que toda transvección $T_{u,\alpha}$ está en $\mathrm{UE}(V)'$. Sea H un plano hiperbólico tal que $u \in H$. Si $|C| \neq 4, 9$, entonces $T_{u,\alpha}|_H \in \mathrm{UE}(H)'$, luego $T_{u,\alpha}|_H$ se descompone en producto de conmutadores, los cuales se extienden a conmutadores de $\mathrm{UE}(V)$ que fijan a los vectores de $H^\perp$, luego el producto de las extensiones es $T_{u,\alpha}$, y así $T_{u,\alpha} \in \mathrm{UE}(V)'$.

Si $|C| = 9$ suponemos $n \geq 3$, luego podemos tomar $W = H \perp \langle x\rangle$, donde x es anisótropo no nulo, y etonces $T_{u,\alpha}|_W \in \mathrm{UE}(W)'$ por el teorema 9.18 y, como antes, esto implica que $T_{u,\alpha} \in \mathrm{UE}(V)'$. Similarmente, si $|F| = 4$ entonces $n \geq 4$, luego podemos tomar un subespacio $W = H \perp H'$, donde H' es otro plano hiperbólico, y concluimos igualmente usando el teorema 9.19. ∎

Claramente, esto implica que $\mathrm{UEP}(V)' = \mathrm{UEP}(V)$ salvo en los tres casos exceptuados.

La simplicidad de UEP(V) Para completar la comprobación de las hipótesis del teorema de Iwasawa comprobamos ahora que la acción de $\mathrm{UEP}(V)$ sobre el conjunto Ω es primitiva. Necesitamos un hecho auxiliar:

Teorema 9.21 *Si V es un espacio unitario de dimensión $n \geq 3$ y $x, y \in V$ son vectores isótropos, existe otro $w \in V$ isótropo tal que $F(x,w) \neq 0 \neq F(y,w)$.*

Demostración: Si $F(x,y) \neq 0$ podemos suponer que $F(x,y) = 1$. Así $\langle x,y\rangle$ es un plano hiperbólico, luego $\langle x,y\rangle^\perp$ es no degenerado y no nulo (porque $n \geq 3$), luego podemos tomar $z \in \langle x,y\rangle^\perp$ tal que $F(z,z) \neq 0$. Tomemos $w = x + \alpha y + z$, donde $\alpha + \bar{\alpha} = -F(z,z)$. Así $F(w,w) = 0$, $F(x,w) = \bar{\alpha} \neq 0$, $F(y,w) = 1$.

Supongamos ahora que $F(x,y) = 0$, con lo que x, y son linealmente independientes. Por 8.5 existe un $u \in V$ tal que $F(x,u) = F(y,u) = 1$. Sea $w = u + \beta x$, donde $\beta + \bar{\beta} = -F(u,u)$. Así $F(w,w) = 0$ y $F(x,w) = F(y,w) = 1$. ∎

Teorema 9.22 *Si V es un espacio unitario isótropo, el grupo $\mathrm{UE}(V)$ actúa primitivamente sobre Ω salvo a lo sumo en el caso de $\mathrm{UE}(3,4)$.*

Demostración: Si $n = 2$ el teorema 9.9 implica que $\mathrm{UE}(V)$ es doblemente transitivo, luego primitivo. Por lo tanto podemos suponer que $n \geq 3$ (así como que si $|C| = 4$ entonces $n \geq 4$). Supongamos que $B \subset \Omega$ es un bloque no trivial.

Vamos a probar que existen $\langle u\rangle, \langle v\rangle \in B$ tales que (u,v) es un par hiperbólico. Para ello basta con que $F(u,v) \neq 0$, pues dividiendo u entre $F(u,v)$ conseguimos que $F(u,v) = 1$. Tomemos, $\langle x\rangle, \langle v\rangle \in B$ (que existen, porque B no es trivial) y supongamos que $F(x,v) = 0$.

Si fuera $\langle v\rangle^\perp \leq \langle x\rangle^\perp$, como ambos subespacios tienen la misma dimensión, sería $\langle v\rangle^\perp = \langle x\rangle^\perp$, luego $\langle v\rangle = \langle v\rangle^{\perp\perp} = \langle x\rangle^{\perp\perp} = \langle x\rangle$, lo cual es imposible. Por lo tanto podemos tomar $w \in \langle x\rangle^\perp \setminus \langle v\rangle^\perp$ y, cambiando w por un múltiplo, podemos exigir que $F(w,v) = 1$.

Si $F(w,w) = 0$, llamemos $u = w$ y, en caso contrario, sea $u = w + \alpha v \in \langle x\rangle^\perp$, donde $\alpha + \bar{\alpha} = -F(w,w)$. Así en ambos casos $H = \langle u,v\rangle$ es un plano hiperbólico y $x \in H^\perp$. Por 9.8 existe $f_0 \in \mathrm{UE}(H)$ tal que $f_0(\langle v\rangle) = \langle u\rangle$, y extendiéndola como la identidad en $H^\perp$ obtenemos una transformación $f \in \mathrm{UE}(V)$ tal que $f(\langle v\rangle) = \langle u\rangle$ y $f(\langle x\rangle) = \langle x\rangle$. Por consiguiente, $\langle x\rangle \in B \cap f[B]$ y, como B es un bloque, tiene que ser $f[B] = B$, luego $\langle u\rangle \in f[B]$.

Así pues, fijamos $\langle u\rangle, \langle v\rangle \in B$ de modo que (u, v) sea un par hiperbólico. Sea $\langle x\rangle \in \Omega$ distinto de $\langle u\rangle$. Por el teorema anterior existe $\langle y\rangle \in \Omega$ tal que $F(x, y) \neq 0$, $F(u, y) \neq 0$. Cambiando y por un múltiplo suyo podemos exigir que (u, y) sea un par hiperbólico, y luego cambiando x podemos exigir que (x, y) también lo sea. Por el teorema 9.16 existen $f, g \in \mathrm{UE}(V)$ tales que $f(u) = u$, $f(v) = y$, $g(u) = x$, $g(y) = y$. Así $\langle u\rangle = f(\langle u\rangle) \in B \cap f[B]$, luego $f[B] = B$ y entonces $\langle y\rangle = f(\langle v\rangle) \in f[B] = B$. Por último, $\langle y\rangle = g(\langle y\rangle) \in B \cap g[B]$, luego $g[B] = B$ y $\langle x\rangle = g(\langle u\rangle) \in g[B] = B$. Como $\langle x\rangle \in \Omega$ era arbitrario, concluimos que $B = \Omega$. ∎

Con esto tenemos demostradas todas las hipótesis del teorema de Iwasawa, que nos permiten concluir:

Teorema 9.23 *Si V es un espacio unitario isótropo, el grupo* $\mathrm{UEP}(V)$ *es simple salvo en los casos* $\mathrm{UEP}(2, 4)$, $\mathrm{UEP}(2, 9)$, $\mathrm{UEP}(3, 4)$.

Según el teorema 9.6, tenemos que

$$\mathrm{UEP}(2, 4) \cong \mathrm{LEP}(2, 2) \cong \Sigma_3, \qquad \mathrm{UEP}(2, 9) \cong \mathrm{LEP}(2, 3) \cong A_4.$$

El grupo UEP(3,4) Para estudiar la estructura del grupo $\mathrm{UEP}(3, 4)$ empezamos con una observación general sobre los grupos $\mathrm{UEP}(3, q^2)$. Si V es un espacio unitario de dimensión 3 sobre el cuerpo de q^2 elementos, el teorema 8.35 nos da que tiene $(q^3 + 1)(q^2 - 1)$ vectores isótropos y, como cada uno genera un subespacio con $q^2 - 1$ vectores isótropos, resulta que el conjunto Ω de los puntos isótropos de $P(V)$ tiene $|\Omega| = q^3 + 1$ elementos.

Si llamamos *rectas hiperbólicas* a las rectas de $P(V)$ determinadas por los planos hiperbólicos de V, por el mismo teorema, cada plano hiperbólico contiene $(q^2 - 1)(q + 1)$ vectores isótropos, luego cada recta hiperbólica contiene $q + 1$ puntos isótropos.

Además, si $P = \langle u\rangle$, $Q = \langle v\rangle$ son dos puntos isótropos distintos, necesariamente $P+Q = \langle u, v\rangle$ es un plano hiperbólico, pues no puede ser que $F(u, v) = 0$, ya que entonces el índice de Witt de $P + Q$ sería al menos 2 y $\dim(P + Q) \geq 4$, lo cual es absurdo. Así, $P + Q$ determina una recta hiperbólica H que pasa por P y Q, y es claramente la única.

Con esto hemos probado que el conjunto Ω junto con las rectas hiperbólicas (o, más precisamente, con los bloques formados por los $q^2 - 1$ puntos de cada recta hiperbólica) forma un sistema de Steiner de tipo $S(2, q^2 - 1, q^3 + 1)$.

Más aún, si P es un punto anisótropo, entonces $P^\perp$ es un plano hiperbólico y viceversa, luego cada recta hiperbólica está formada por los puntos ortogonales a un punto anisótropo, y en particular hay tantas rectas hiperbólicas en Ω como puntos anisótropos en $P(V)$.

Particularizando ya al caso que nos interesa, en el que $q = 2$, vemos que el conjunto Ω de los puntos isótropos es un sistema de Steiner de tipo $S(2, 3, 9)$, luego, según [G 8.81], se trata del plano afín sobre el cuerpo de 3 elementos, al que llamaremos W_9 siguiendo la notación introducida en la sección 7.3. Así, W_9 consta de 9 puntos (isótropos) y 12 rectas (hiperbólicas), que se corresponden con los 12 puntos anisótropos de $P(V)$.

Más aún, como $\dim V = 3$, es obvio que dos planos hiperbólicos se cortan necesariamente en un subespacio de dimensión 1, es decir, en un punto de $P(V)$, que puede ser isótropo o anisótropo. En el primer caso las rectas hiperbólicas correspondientes son secantes y en el segundo paralelas.

Observemos que cada recta hiperbólica contiene, además de sus tres puntos isótropos, otros dos puntos anisótropos, que son ortogonales (es decir, de la forma $\langle w\rangle, \langle z\rangle$ con $w \perp z$) pues un plano hiperbólico contiene 15 vectores no nulos que se dividen en 5 subespacios vectoriales de dimensión 1 (puntos de $P(V)$), y son ortogonales porque todo plano hiperbólico tiene que contener una base ortogonal.

Cada punto anisótropo pertenece exactamente a dos rectas hiperbólicas. En efecto, en la prueba del teorema 9.4 hemos visto que pertenece al menos a dos de ellas, y si perteneciera a tres, éstas formarían uno de los tres haces de rectas paralelas de W_9, pero, fijada una de ellas, poseería un segundo punto anisótropo por el que pasaría una cuarta recta paralela, lo cual es imposible. Por lo tanto, los 12 puntos anisótropos se corresponden con los 12 pares de rectas paralelas de W_9 (tres de cada uno de los 4 haces de rectas paralelas). A cada haz de rectas paralelas le corresponden tres puntos anisótropos ortogonales dos a dos, de modo que cada recta del par contiene dos de ellos, los correspondientes a los dos pares de paralelas de los que forma parte.

En particular vemos que los 12 puntos anisótropos se dividen en 4 clases de tres puntos anisótropos ortogonales dos a dos. (Cada punto anisótropo P está en un único conjunto de tres puntos anisótropos ortogonales, pues los otros dos tienen que ser necesariamente los contenidos en $P^\perp$).

Según 9.4, el grupo $\mathrm{UP}(3,4)$ es un grupo de permutaciones sobre W_9 y cada transformación unitaria transforma planos hiperbólicos en planos hiperbólicos, luego induce una colineación en W_9, por lo que tenemos un monomorfismo de grupos $\mathrm{UP}(3,4) \longrightarrow \mathrm{Aut}(W_9)$. Como $|\mathrm{UP}(3,4)| = 2^3 \cdot 3^3$, la imagen es un subgrupo de índice 2. Ahora bien, al estudiar el grupo de Mathieu M_9 en la sección 7.3 hemos visto que $\mathrm{Aut}(W_9)$ tiene un único subgrupo de índice 2, a saber:

$$\mathrm{UP}(3,4) = \mathrm{LE}(2,3)[C_3 \times C_3].$$

Ahora, $|\mathrm{UEP}(3,4)| = 2^3 \cdot 3^2$. Si llamamos N a este subgrupo, tenemos que $N \cap (C_3 \times C_3) \trianglelefteq \mathrm{UP}(3,4)$, pero $\mathrm{LE}(2,3)$ actúa transitivamente (por conjugación) sobre $C_3 \times C_3$, lo que se traduce en que ninguno de sus subgrupos propios es normal en $\mathrm{UP}(3,4)$, y no puede ser $N \cap (C_3 \times C_3) = 1$ (pues el producto tendría orden divisible entre 3^4), luego tiene que ser $C_3 \times C_3 \leq \mathrm{UEP}(3,4)$, y un 2-subgrupo de Sylow de $\mathrm{UEP}(3,4)$ tiene que serlo de $\mathrm{UP}(3,4)$, luego de $\mathrm{LE}(3,2)$. Según hemos visto en la sección 3.7, el grupo $\mathrm{LE}(3,2)$ tiene un único 2-subgrupo de Sylow isomorfo a Q_8, luego tenemos el producto semidirecto

$$\mathrm{UEP}(3,4) \cong Q_8[C_3 \times C_3],$$

donde la acción es la que resulta de considerar a $Q_8 \trianglelefteq \mathrm{LE}(2,3)$. Equivalentemente, comparando con los resultados de la sección 7.3, tenemos que

$$\mathrm{UEP}(2,4) \cong M_9.$$

Teniendo en cuenta que el único elemento no nulo de C que cumple $\alpha+\bar{\alpha}=0$ es $\alpha=1$, así como la relación $T_{\lambda u,\alpha}=T_{u,\lambda\bar{\lambda}\alpha}$, resulta que en $\mathrm{U}(3,4)$ hay exactamente 9 transvecciones, de la forma $T_P=T_u,1$, donde $P=\langle u\rangle$ recorre los puntos de W_9.

La transvección T_P fija los vectores de $\langle u\rangle^\perp=\langle u,w\rangle$, donde w es anisótropo, ya que $\langle u\rangle^\perp$ no puede ser totalmente isótropo, o V tendría índice de Witt $m\geq 2$ y entonces $\dim V\geq 4$. Así $\mathrm{N}(au,bw)=b\bar{b}\,\mathrm{N}(w)$, de donde se concluye que P es el único punto isótropo fijado por T_P, la cual fija además a otros cuatro puntos anisótropos, entre los que no puede haber dos ortogonales (pues entonces $\langle u\rangle^\perp$ sería no degenerado, y no es el caso), luego hay uno en cada una de las cuatro clases de puntos anisótropos ortogonales dos a dos.

Como T_P tiene que transformar cada una de estas clases en otra de ellas, el hecho de que fije a un punto de cada una se traduce en que T_P fija las cuatro clases, lo que a su vez se interpreta como que T_P fija a cada uno de los cuatro haces de rectas paralelas de W_9, es decir, que envía cada recta hiperbólica a otra paralela a ella misma.

Ahora bien, desde el punto de vista de la geometría de W_9, las únicas biyecciones afines que transforman cada recta en una paralela son las homotecias y las traslaciones [G 5.8], que admiten una expresión en coordenadas de la forma

$$f(x,y)=(\alpha x+a,\alpha y+b),$$

donde $\alpha=\pm 1$ y $a,b\in\{0,\pm 1\}$. Esto hace que haya exactamente 9 homotecias (de orden 2, correspondientes a $\alpha=-1$) y 9 traslaciones (de orden 3 salvo la identidad, correspondientes a $\alpha=1$).

Es fácil ver que las transvecciones tienen orden 2, luego las 9 transvecciones de $\mathrm{U}(3,4)$ inducen las 9 homotecias de W_9, y el subgrupo $\mathfrak{T}(3,4)$ que generan induce el grupo formado por las 18 homotecias y traslaciones. Así pues, el grupo

$$\mathfrak{TP}(3,4)=\mathfrak{T}(3,4)\mathrm{ZUE}(3,4)/\mathrm{ZUE}(3,4)$$

cumple $|\mathfrak{TP}(3,4)|=18$. Explícitamente, $\mathfrak{TP}(3,4)\cong C_2[C_3\times C_3]$, donde C_2 es el único subgrupo de Q_8 de orden 2. Vamos a ver que $\mathrm{ZUE}(3,4)\leq\mathfrak{T}(3,4)$, con lo que $|\mathfrak{T}(3,4)|=54$.

Para ello fijamos un par hiperbólico (u,v) y tomamos un vector $w\in\langle u,v\rangle^\perp$ de norma 1. Consideramos la base (u,w,v) de V, respecto a la cual las transvecciones T_u,T_v tienen por matrices las dos de la izquierda:

$$\begin{pmatrix}1&0&0\\0&1&0\\1&0&1\end{pmatrix}\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&0&1\\0&1&0\\1&0&0\end{pmatrix}.$$

El producto representa, pues, una traslación (de orden 3). Consideramos ahora otro vector isótropo, por ejemplo $z=\omega u+w+v$, donde $\omega\in C$ cumple las relaciones $\bar{\omega}=\omega^2=\omega+1$. Es fácil ver que su matriz en la base considerada es

la matriz de la izquierda:

$$\begin{pmatrix} \omega^2 & 1 & 1 \\ \omega & 0 & 1 \\ 1 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \omega & 1 & 1 \\ \omega^2 & 0 & 1 \\ \omega^2 & \omega^2 & \omega \end{pmatrix}.$$

Así tenemos otro producto de transvecciones que tiene que ser otra traslación (de orden 3). Ahora bien, una comprobación rutinaria muestra que las dos "traslaciones" que hemos obtenido no conmutan. Aunque el grupo de traslaciones es abeliano, esto no debe sorprendernos, pues sólo tienen que conmutar como elementos del cociente $\mathcal{TP}(3,4)$, no como elementos de $\mathcal{T}(3,4)$. El lector puede calcular el conmutador de ambas "traslaciones", pero en realidad podemos predecir el resultado sin necesidad de ningún cálculo:

Tenemos que $|\mathcal{TP}(3,2)\mathrm{ZUE}(3,4)| = 2\cdot 3^3$ y, si S es un 3-subgrupo de Sylow, entonces $S/\mathrm{ZUE}(3,4) \cong C_3 \times C_3$ es el único 3-subgrupo de Sylow (normal) de $\mathcal{TP}(3,2)\mathrm{ZUE}(3,4)/\mathrm{ZUE}(3,4)$, luego $S \trianglelefteq \mathcal{TP}(3,2)\mathrm{ZUE}(3,4)$ es el único 3-subgrupo de Sylow.

Por lo tanto, las dos "traslaciones" que hemos encontrado están en S, y el hecho de que no conmuten prueba que S no es abeliano, luego $S' = \mathrm{ZUE}(3,4)$, por lo que el conmutador de las dos "traslaciones" tiene que ser uno de los dos elementos no triviales de $\mathrm{ZUE}(3,4)$ (según en qué orden lo calculemos). Esto prueba que $\mathrm{ZUE}(3,4) \leq \mathcal{T}(3,4)$, pues sus elementos son productos de cuatro transvecciones. Así concluimos que $\mathcal{T}(3,4) = C_2[S] = \mathrm{UE}(3,4)'$. Un análisis un poco más detallado muestra que todos los elementos no triviales de S tienen orden 3, por lo que S es isomorfo al segundo grupo descrito en el teorema 3.22.

En realidad, $S/\mathrm{ZUE}(3,4) \trianglelefteq \mathrm{UE}(3,4)/\mathrm{ZUE}(3,4)$, por lo que $S \trianglelefteq \mathrm{UE}(3,4)$ y resulta que $\mathrm{UE}(3,4) = Q_8[S]$, donde la acción de Q_8 sobre S es la inducida por la acción sobre $S/\mathrm{ZUE}(3,4) \cong C_3 \times C_3$ fijando a todos los elementos de $\mathrm{ZUE}(3,4)$, que es el centro del grupo.

Sabemos que $\mathcal{TP}(3,4)$ está formado por todos los elementos de $\mathrm{UP}(3,4)$ que fijan los cuatro haces de rectas paralelas, por lo que tenemos un monomorfismo de grupos

$$\mathrm{UP}(3,4)/\mathcal{TP}(3,4) \longrightarrow \Sigma_4$$

cuya imagen tiene orden 12, luego dicha imagen es isomorfa a A_4. Por lo tanto,

$$\mathrm{UEP}(3,4)/\mathcal{TP}(3,4)$$

es isomorfo a un subgrupo de A_4 de orden 4, que es necesariamente V_4 (el grupo formado por los pares de transposiciones y el neutro), lo que significa que cada transformación unitaria fija los cuatro haces de rectas paralelas de W_9 o bien los intercambia por pares, y de aquí es fácil concluir que $\mathrm{UEP}(3,4)$ deja invariantes las tres clases de cuadriláteros $\mathcal{Q}_i$ definidas en 7.24, por lo que está contenindo en el grupo M_9 y, al tener el mismo orden, tenemos una prueba explícita de que $\mathrm{UEP}(3,4) = M_9$. ∎

9.2 Los grupos ortogonales

En esta sección estudiaremos el grupo $\mathrm{O}(V) \leq \mathrm{LG}(V)$ de las transformaciones ortogonales de un espacio cuadrático V sobre un cuerpo C. Cuando C es el cuerpo finito de q elementos se trata de los grupos $\mathrm{O}(2m+1,q)$, $\mathrm{O}^+(2m,q)$ y $\mathrm{O}^-(2m,q)$ cuyos órdenes hemos calculado en el teorema 8.48. (Recordemos que los grupos $\mathrm{O}(2m+1,q)$ sólo los tenemos definidos cuando q es impar).

El grupo $\mathrm{O}(V)$ actúa de forma natural sobre el espacio proyectivo $P(V)$, pero, como en el caso de los grupos unitarios, si V tiene puntos singulares la acción no es transitiva, por lo que necesitaremos restringirnos al conjunto de los puntos singulares:

Definición 9.24 Si V es un espacio cuadrático, llamaremos X_0 al conjunto de todos los vectores singulares de V y $X = \{\langle u\rangle \mid u \in X_0\} \subset P(V)$. Es claro que $\mathrm{O}(V)$ actúa sobre X_0 y sobre X.

Teorema 9.25 *Si V es un espacio cuadrático singular de dimensión ≥ 3, el núcleo de la acción de $\mathrm{O}(V)$ sobre X es $\{\pm 1\}$.*

Demostración: Llamemos N al núcleo de la acción y $Z = \{\pm 1\}$, de modo que obviamente $Z \leq N$. Tomemos $f \in K$. Sea $H = \langle u, v\rangle$ un plano hiperbólico y sea $w \in H^\perp$ un vector no singular no nulo. Entonces $x = w + v - Q(w)u$ es singular, luego $\langle x\rangle \in X$. Por lo tanto, existen escalares a, b, c tales que

$$f(u) = au, \qquad f(v) = bv, \qquad f(x) = cx.$$

Por lo tanto

$$cw + cv - Q(w)cu = cx = f(x) = f(w) + bv - Q(w)au.$$

Por la suma directa $V = H \perp H^\perp$, podemos concluir que $f(w) = cw$ así como que

$$cv - cQ(w)u = bv - Q(w)au,$$

luego, por la independencia lineal de u, v, también $b = c$, $a = c$. Esto significa que, fijados u, v, la constante c es independiente de w. Además, tenemos que $Q(w) = Q(f(w)) = c^2Q(w)$, luego $c^2 = 1$ y $c = \pm 1$.

Si el cuerpo de escalares tiene característica distinta de 2, podemos tomar una base ortogonal de $H^\perp$ y completarla con u, v hasta una base de V de modo que $f(z) = cz$ para todos los vectores de la base, luego para todo $z \in V$, y así $f = \pm 1$.

Si la característica es 2, entonces $c = 1$ y hemos probado que $f(u) = u$ para cualquier vector $u \in V$ singular. En particular, $f(z) = z$ para todo $z \in H^\perp$ singular, y también para todo $w \in H^\perp$ no singular, luego $f(z) = z$ para todo $z \in H^\perp$. Completando con u, v cualquier base de $H^\perp$ tenemos de nuevo que f fija a todos los vectores básicos, luego $f = 1$. ∎

Reflexiones Hemos visto —y aprovechado a fondo— que los grupos $\mathrm{UE}(V)$ están generados por las transvecciones. Sin embargo, ahora veremos que no hay transvecciones ortogonales, pero lo demostraremos a la vez que les encontramos un sustituto. Antes necesitamos algunos resultados técnicos:

Teorema 9.26 *Si V es un espacio cuadrático y $f \in \mathrm{O}(V)$, entonces*

$$\mathrm{N}(f-1) = \mathrm{Im}(f-1)^\perp.$$

Demostración: Si $v \in \mathrm{N}(f-1)$ y $w \in V$, entonces (teniendo en cuenta que $v = f(v)$):

$$F(v,(f-1)(w)) = F(v,f(w)) - F(v,w) = F(v,w) - F(v,w) = 0.$$

Por lo tanto, $\mathrm{N}(f-1) \leq \mathrm{Im}(f-1)^\perp$. Por otro lado, si $v \in \mathrm{Im}(f-1)^\perp$ y $w \in V$,

$$F((f-1)(v),f(w)) = F(f(v),f(w)) - F(v,f(w)) =$$

$$F(v,w) - F(v,f(w)) = -F(v,(f-1)(w)) = 0,$$

y como esto vale para todo $w \in V$, tiene que ser $(f-1)(v) = 0$ (porque F no es degenerada), luego $v \in \mathrm{N}(f-1)$. ∎

Teorema 9.27 *Si V es un espacio cuadrático y $f \in \mathrm{O}(V)$ fija todos los vectores de un hiperplano, o bien f es la identidad, o bien existe un vector no singular no nulo $v \in V$ tal que, para todo $w \in V$,*

$$f(w) = w - \frac{F(w,v)}{Q(v)}\,v.$$

Demostración: Suponemos que $f \neq 1$ y llamamos H al hiperplano formado por los vectores que fija. Entonces $V = H \oplus \langle v_0\rangle$, de modo que cada $w \in V$ se expresa de forma única como $w = h + g(w)v_0$, donde $g : V \longrightarrow C$ es una aplicación lineal. Por el teorema 8.5, existe un $u \in V$ tal que $g(w) = F(w,u)$, y por lo tanto $w = h + F(w,u)v_0$. A su vez,

$$f(w) = h + F(w,u)f(v_0) = w - F(w,u)v_0 + F(w,u)f(v_0) = w + F(w,u)v,$$

donde llamamos $v = f(v_0) - v_0$. Si $v = 0$, entonces f es la identidad. Supongamos, pues, que $v \neq 0$. Entonces, según 9.26,

$$\langle u\rangle^\perp = \mathrm{N}(f-1) = \mathrm{Im}(f-1)^\perp = \langle v\rangle^\perp,$$

luego $\langle v\rangle = \langle u\rangle$. Pongamos que $u = \alpha v$, con lo que

$$f(w) = w + \alpha F(w,v)v.$$

Notemos que $\alpha \neq 0$. Ahora, para todo $w \in V$, se cumple que

$$Q(w) = Q(f(w)) = Q(w) + \alpha^2 F(w,v)^2 Q(v) + \alpha F(w,v)^2,$$

luego

$$\alpha F(w,v)^2(1 + \alpha Q(v)) = 0.$$

Tomando w tal que $F(w,v) \neq 0$ concluimos que $1 + \alpha Q(v) = 0$, luego v es no singular y $\alpha = 1/Q(v)$. Con esto llegamos a que f tiene la forma indicada en el enunciado. ∎

Definición 9.28 Si V es un espacio cuadrático y $v \in V$ es un vector no singular no nulo, definimos la *reflexión* respecto al hiperplano $H = \langle v\rangle^\perp$ como la transformación $R_v \in \mathrm{O}(V)$ dada por

$$R_v(w) = w - \frac{F(w,v)}{Q(v)}\, v.$$

Es fácil comprobar que realmente es una transformación ortogonal. Hemos probado que las reflexiones son las únicas transformaciones ortogonales (además de la identidad) que fijan a todos los vectores de un hiperplano. Concretamente, tenemos que $R_v(w) = w$ si y sólo si $w \in \langle v\rangle^\perp$, mientras que $R_v(v) = -v$.

Si la característica del cuerpo de escalares no es 2, las reflexiones tienen determinante -1, pues tenemos que $V = \langle v\rangle \perp \langle v\rangle^\perp$ y completando con v una base de $\langle v\rangle^\perp$ obtenemos una base de V en la que la matriz de R_v es diagonal con toda la diagonal igual a 1 excepto un -1.

Por lo tanto, salvo que el cuerpo de escalares tenga característica 2, no son transvecciones, ya que las transvecciones tienen determinante 1 y, como cada transvección fija a los vectores de un hiperplano, concluimos que, salvo en característica 2, no hay transvecciones ortogonales.

Notemos que si $\alpha \neq 0$, entonces $R_{\alpha v} = R_v$. Más aún, si $R_v = R_w$, entonces $\langle v\rangle^\perp = \langle w\rangle^\perp$, luego $\langle v\rangle = \langle w\rangle$, luego $w = \alpha v$, para cierto escalar α.

Se cumple que $R_v^2 = 1$. En efecto:

$$R_v(R_v(w)) = R_v(w - \frac{F(w,v)}{Q(v)}v) = R_v(w) - \frac{F(w,v)}{Q(v)}R_v(v) =$$

$$w - \frac{F(w,v)}{Q(v)}v + \frac{F(w,v)}{Q(v)}v = w.$$

Una comprobación elemental muestra que si $f \in \mathrm{O}(V)$, entonces

$$f^{-1}R_v f = R_{f(v)}.$$

Usando las reflexiones podemos calcular el centro de $\mathrm{O}(V)$:

Teorema 9.29 *Si V es un espacio cuadrático, entonces $Z(\mathrm{O}(V)) = \{\pm 1\}$ salvo en el caso de $\mathrm{O}^+(2,3)$.*

Demostración: Sea $n = \dim V$. Si $n = 1$ es $\mathrm{O}(V) = \{\pm 1\}$, luego la conclusión es trivial. Supongamos que $n \geq 2$. Llamemos $Z = Z(\mathrm{O}(V))$ y sea $f \in Z$. Si $u \in V$ es un vector no singular no nulo, $R_u = R_u^f = R_{f(u)}$, luego $f(u) \in \langle u\rangle$. Pongamos que $f(u) = \alpha u$. Entonces

$$Q(u) = Q(f(u)) = Q(\alpha u) = \alpha^2 Q(u),$$

luego tiene que ser $\alpha^2 = 1$, luego $\alpha = \pm 1$.

Si la característica del cuerpo de escalares es 2, entonces $\alpha = 1$, luego concluimos que $f(u) = 1$ para todo vector no singular u, pero el teorema 8.28 implica que V tiene una base formada por vectores no singulares, luego $f = 1$.

Si la característica del cuerpo de escalares no es 2, por el teorema 8.25 nos da que V tiene una base ortogonal, digamos $u_1, \ldots, u_n$, y entonces $f(u_i) = \epsilon_i u_i$, para cierto $\epsilon_i = \pm 1$.

Dados dos índices $i \neq j$, si $u_i + u_j$ es no singular,

$$\pm(u_i + u_j) = f(u_i + u_j) = f(u_i) + f(u_j) = \epsilon_i u_i + \epsilon_j u_j,$$

de donde $\epsilon_i = \epsilon_j$. Si $u_i + u_j$ es singular y $n \geq 3$, tomemos un índice k distinto de i, j, de modo que

$$Q(u_i + u_j + u_k) = Q(u_i + u_j) + Q(u_k) = Q(u_k) \neq 0,$$

luego

$$\pm(u_i + u_j + u_k) = f(u_i + u_j + u_k) = \epsilon_i u_i + \epsilon_j u_j + \epsilon_k u_k,$$

de donde nuevamente $\epsilon_i = \epsilon_j$ y $f = \pm 1$.

Sólo falta considerar el caso en que el cuerpo de escalares C tiene característica distinta de 2, la dimensión de V es $n = 2$ y V tiene vectores singulares, es decir, el caso en que V es un plano hiperbólico. En la prueba del teorema 8.45 hemos visto que $\mathrm{O}(V) \cong C_2[C^*]$, donde, si $C_2 = \langle g \rangle$, su acción sobre C^* viene dada por $\alpha^g = \alpha^{-1}$. Por lo tanto, g sólo conmuta con los elementos de C^* de orden ≤ 2, luego, si C^* contiene elementos de orden > 2, el centro se reduce a los elementos de C^* de orden 2, que son ± 1. Si C^* no contiene elementos de orden > 2 es que $C^* = \{\pm 1\}$, luego $\mathrm{O}(V) = \mathrm{O}^+(2, 3) \cong D_4 \cong C_2 \times C_2$. ∎

La parametrización de Wall Vamos a probar que —salvo una excepción— el grupo $\mathrm{O}(V)$ está generado por las reflexiones, para lo cual presentamos la parametrización de Wall de $\mathrm{O}(V)$ análoga a la que hemos estudiado ya para los grupos unitarios.

Si V es un espacio cuadrático, para cada transformación $f \in \mathrm{O}(V)$ definimos $\hat{f} = 1 - f$ y $V_f = \operatorname{Im} \hat{f}$, de modo que $\hat{f} : V \longrightarrow V_f$ es un epimorfismo.

Como en el caso unitario se comprueba inmediatamente que

$$F(\hat{f}(x), \hat{f}(y)) = F(\hat{f}(x), y) + F(x, \hat{f}(y)).$$

Definimos $F_f : V_f \times V_f \longrightarrow C$ mediante

$$F_f(\hat{f}(x), \hat{f}(y)) = F(x, \hat{f}(y)).$$

Exactamente igual que en el caso unitario se comprueba que F_f está bien definida y es una forma bilineal en V_f no degenerada que cumple

$$F_f(u, v) + F_f(v, u) = F(u, v).$$

(las pruebas en el caso unitario no usan en ningún momento que la conjugación de la forma sesquilineal no sea la identidad, por lo que valen sin cambio alguno en este contexto). Más aún, si $x \in V$, tenemos que

$$Q(x) = Q(f(x)) = Q(x - \hat{f}(x)) = Q(x) + Q(\hat{f}(x)) - F(x, \hat{f}(x)),$$

luego $F_f(\hat{f}(x), \hat{f}(x)) = F(x, \hat{f}(x)) = Q(\hat{f}(x))$. En otras palabras, para todo $u \in V_f$ se cumple que $F_f(u, u) = Q(u)$. Recíprocamente:

Teorema 9.30 *Sea V un espacio cuadrático, sea $W \leq V$ y sea G una forma bilineal no degenerada en W tal que, para todo $u \in W$, se cumple*

$$G(u, u) = Q(u).$$

Entonces existe una única $f \in \mathrm{O}(V)$ tal que $V_f = W$ y $F_f = G$.

Demostración: Veamos en primer lugar la unicidad: si $f, g \in \mathrm{O}(V)$ cumplen $V_f = V_g$ y $F_f = F_g$, entonces, para todo $x \in V$ y todo $v \in V_f = V_g$, tenemos que

$$F_f(\hat{f}(x), v) = F(x, v) = F_g(\hat{g}(x), v) = F_f(\hat{g}(x), v),$$

luego $F_f(\hat{f}(x) - \hat{g}(x), v) = 0$ para todo $v \in V_f$. Como F_f no es degenerada, tiene que ser $\hat{f}(x) = \hat{g}(x)$ para todo $x \in V$, luego también $f(x) = g(x)$ para todo $x \in V$, y así $f = g$.

Dados W y G en las condiciones del enunciado, para cada $x \in V$ podemos considerar la aplicación lineal $W \longrightarrow C$ dada por $y \mapsto F(x, y)$. Como G no es degenerada, por la observación previa al teorema 8.5 tenemos un isomorfismo $\iota_i : W \longrightarrow W^*$ dado por $\iota_i(v)(y) = G(v, y)$, luego existe un único $\tilde{f}(x) \in W$ tal que

$$G(\tilde{f}(x), y) = F(x, y)$$

para todo $y \in W$. La unicidad implica que $\tilde{f} : V \longrightarrow W$ es una aplicación lineal. De hecho es suprayectiva, pues, dado $w \in W$, la aplicación lineal $y \mapsto G(w, y)$ se extiende a una aplicación lineal $V \longrightarrow C$, que a su vez puede expresarse en la forma $y \mapsto F(x, y)$, para cierto $x \in V$, de modo que $G(w, y) = F(x, y)$ para todo $y \in W$, luego $\tilde{f}(x) = w$.

Ahora consideramos $f : V \longrightarrow V$ dada por $f(x) = x - \tilde{f}(x)$. Así

$$Q(x - f(x)) = G(x - f(x), x - f(x)) = F(x, x - f(x)),$$

luego

$$Q(x) + Q(f(x)) - F(x, f(x)) = F(x, x) - F(x, f(x)) = 2Q(x) - F(x, f(x)),$$

luego $Q(f(x)) = Q(x)$, lo que significa que $f \in \mathrm{O}(V)$. Además, entonces $\tilde{f} = \hat{f}$ y $W = \operatorname{Im} \tilde{f} = V_f$. Por último,

$$F_f(\hat{f}(x), y) = F(x, y) = G(\hat{f}(x), y),$$

para todo $x \in V$, $y \in V_f$, luego $F_f = G$. ∎

Teorema 9.31 *Sea V un espacio cuadrático, sea $f \in \mathrm{O}(V)$, sea $W_1 \leq V_f$ un subespacio no degenerado (respecto de F_f) y sea $W_2 = {}^{\perp}W_1$ y sean $f_1, f_2 \in \mathrm{O}(V)$ las transformaciones cuadráticas asociadas a $(W_i, F_f|_{W_i})$. Entonces $f = f_1 f_2$.*

Demostración: Que W_1 sea no degenerado equivale a que si $w_1 \in W_1$ cumple $F_f(w_1, w) = 0$ para todo $w \in W_1$ entonces $w_1 = 0$, lo cual equivale a que $W_1 \cap W_2 = 0$, luego $W = W_1 \oplus W_2$.

Si $u_1 \in W_1$, $u_2 \in W_2$, entonces $F_f(u_2, u_1) = 0$, luego

$$F(u_1, u_2) = F_f(u_1, u_2) + F_f(u_2, u_1) = F_f(u_1, u_2).$$

Por definición de F_f tenemos que

$$F_f(\hat{f}_1(v), u_1) = F(v, u_1), \qquad F_f(\hat{f}_2(v), u_2) = F(v, u_2).$$

Por último observamos que

$$\widehat{f_1 f_2} = 1 - f_1 f_2 = f_1(1 - f_2) + (1 - f_1) = f_1 \hat{f}_2 + \hat{f}_1,$$

con lo que, para todo $v \in V$, $u_i \in W_i$,

$$F_f(\widehat{f_1 f_2}(v), u_1 + u_2) = F_f(\hat{f}_2(f_1(v)) + \hat{f}_1(v), u_1 + u_2) =$$

$$F_f(\hat{f}_2(f_1(v)), u_1) + F_f(\hat{f}_1(v), u_1) + F_f(\hat{f}_2(f_1(v)), u_2) + F_f(\hat{f}_1(v), u_2) =$$

$$0 + F(v, u_1) + F(f_1(v), u_2) + F(\hat{f}_1(v), u_2) = F(v, u_1 + u_2).$$

Como esto vale para todo $u_i \in W_i$, tenemos que

$$F_f(\widehat{f_1 f_2}(v), u) = F(v, u) = F_f(\hat{f}(v), u)$$

para todo $u \in W$, luego $\widehat{f_1 f_2} = \hat{f}$, luego $f_1 f_2 = f$. ∎

Según el teorema 9.27, una transformación ortogonal f es una reflexión si y sólo si fija un hiperplano, lo cual equivale claramente a que $\dim V_f \leq 1$ (el caso $V_f = 0$ corresponde a $f = 1$). Concretamente, $V_{R_u} = \langle u \rangle$. Más en general, tenemos el teorema siguiente:

Teorema 9.32 *Sea V un espacio cuadrático, $v \in V$ un vector no singular y sea $f \in \mathrm{O}(V)$. Entonces:*

1. *Si $v = \hat{f}(x) \in V_f$, entonces $V_{fR_v} = V_f \cap \langle x \rangle^{\perp}$.*
2. *Si $v \notin V_f$, entonces $V_{fR_v} = V_f \oplus \langle v \rangle$.*

Demostración: 1) Tenemos que $F(x, v) = F_f(v, v) = Q(v)$, luego

$$R_v(x) = x - \frac{F(x, v)}{Q(v)} v = x - v = f(x).$$

Por lo tanto

$$x - R_v(f(x)) = x - R_v(R_v(x)) = x - x = 0,$$

luego, teniendo en cuenta 9.26, tenemos que $x \in \mathrm{N}(1 - fR_v) = \mathrm{Im}(fR_v - 1)^\perp$, luego $V_{fR_v} \leq \langle x\rangle^\perp$.

Por otra parte, $1 - fR_v = f(1 - R_v) + (1 - f)$ y, como $v \in V_f$,

$$(1 - fR_v)(y) = f(y) - R_v(f(y)) + \hat{f}(y) = \frac{F(f(y), v)}{Q(v)}v + \hat{f}(y) \in V_f.$$

Por lo tanto $V_{fR_v} \leq V_f$ y, de hecho, $V_{fR_v} \leq V_f \cap \langle x\rangle^\perp$.

Si llamamos $W_1 = V_f \cap \langle x\rangle^\perp$, tenemos que $v \in V \setminus W_1$ (pues hemos visto que $F(x, v) = Q(v) \neq 0$), luego $V_f = W_1 \oplus \langle v\rangle$. Más aún, $\langle v\rangle = {}^\perp W_1$ (respecto a F_f), pues $F_f(v, w) = F(x, w) = 0$, luego el teorema 9.31 nos da que la transformación ortogonal g asociada a W_1 cumple $f = gR_v$, luego es $g = fR_v$, luego $V_{fR_v} = W_1$.

2) Se cumple que $w \in \mathrm{N}(1 - fR_v)$ si y sólo si $R_v(f(w)) = w$ o, equivalentemente, si y sólo si

$$f(w) = R_v(w) = w - \frac{F(w, v)}{Q(v)}v$$

o

$$\hat{f}(w) = \frac{F(w, v)}{Q(v)}v.$$

Pero $v \notin V_f = \mathrm{Im}\,\hat{f}$, luego la igualdad anterior sólo puede darse si ambos miembros son nulos. Por lo tanto, $\mathrm{N}(1 - fR_v) = \mathrm{N}(\hat{f}) \cap \langle v\rangle^\perp$. El teorema 9.26 nos da entonces que

$$V_{fR_v} = \mathrm{N}(1 - fR_v)^\perp = \mathrm{N}(\hat{f})^\perp \oplus \langle v\rangle = V_f \oplus \langle v\rangle\,. \qquad \blacksquare$$

Nota Observemos que, en las condiciones del caso 2) del teorema anterior, se cumple que $\langle v\rangle = {}^\perp V_f$ respecto a la forma bilineal F_{fR_v}, con lo que la restricción de F_{fR_v} a V_f es F_f, ya que la transformación g asociada a dicha restricción tiene que cumplir que $fR_v = gR_v$, luego es $g = f$, luego la restricción es F_f.

En efecto, por el teorema 8.5 podemos tomar $x \in V$ tal que $F(w, x) = 0$ para todo $w \in V_f$ y $F(v, x) = Q(v)$. La primera condición equivale a que $x \in V_f^\perp = \mathrm{N}(1 - f)$, luego $f(x) = x$, y así

$$f\hat{R}_v(x) = x - R_v(f(x)) = x - R_v(x) = \frac{F(x, v)}{Q(v)}v = v,$$

luego si $w \in V_f$, se cumple que $F_{fR_v}(v, w) = F(x, w) = 0$, luego $\langle v\rangle \leq {}^\perp V_f$ y se da la igualdad porque ambos espacios tienen la misma dimensión. $\blacksquare$

Vamos a usar este teorema para probar que, salvo una excepción, todo grupo $\mathrm{O}(V)$ está generado por las reflexiones. Lo que afirma en esencia el teorema anterior es que si f es un producto de reflexiones, al añadir una más, el espacio V_f disminuye o aumenta su dimensión en una unidad, según si la nueva reflexión se cancela o no con alguna de las que ya están en f. Necesitamos este resultado auxiliar:

Teorema 9.33 *Sea F una forma bilineal no degenerada sobre un espacio vectorial W sobre un cuerpo distinto del cuerpo de dos elementos, y supongamos que existe al menos un vector no isótropo. Entonces W tiene una base $w_1, \dots, w_m$ tal que $F(w_i, w_i) \neq 0$ y $F(w_i, w_j) = 0$ para $i > j$.*

DEMOSTRACIÓN: Razonamos por inducción sobre la dimensión m de W. Si $m = 1$ es inmediato, pues basta tomar como w_1 cualquier vector no isótropo. En general tomamos un vector no isótropo $u \in W$ y consideramos la descomposición $W = \langle u\rangle \oplus {}^{\perp}\langle u\rangle$. El subespacio ${}^{\perp}\langle u\rangle$ es no degenerado. Si tiene vectores no isótropos basta aplicar la hipótesis de inducción, así que podemos suponer que no los tiene. Tomemos $v \in {}^{\perp}\langle u\rangle$ no nulo, de modo que

$$F(u + av, u + av) = F(u, u) + aF(u, v)$$

no puede ser 0 para todo $a \neq 0$, pues entonces, tomando dos valores distintos para a (y aquí usamos que C tiene más de dos elementos) concluiríamos $F(u, v) = 0$ y, a su vez, $F(u, u) = 0$. Cambiando v por un av adecuado podemos suponer que $c = F(u + v, u + v) \neq 0$.

Como ${}^{\perp}\langle u\rangle$ es no degenerado, tiene que existir $w \in {}^{\perp}\langle u\rangle$ tal que $F(w, v) = 1$ (y v, w tienen que ser linealmente independientes, pues $F(v, v) = 0$). Entonces, para todo escalar b, se cumple que

$$F(u + bv - cw, u + v) = F(u, u) + F(u, v) - c =$$

$$F(u, u + v) - F(u + v, u + v) = -F(v, u + v) = -F(v, u) - F(v, v) = 0$$

y

$$F(u + bv - cw, u + bv - cw) = F(u, u) + bF(u, v) - cF(u, w),$$

donde faltarían dos sumandos $-bcF(v, w) - bcF(w, v) = 0$, como se sigue de desarrollar $F(v + w, v + w) = 0$ teniendo en cuenta que $F(v, v) = F(w, w) = 0$.

Si la expresión anterior no se anula para algún valor de b, entonces basta tomar $w_1 = u + v$, pues así $F(w_1, w_1) \neq 0$ y ${}^{\perp}\langle w_1\rangle$ es un espacio no degenerado que contiene el vector no isótropo $u + bv - cw$, lo que nos permite aplicar la hipótesis de inducción.

Por lo tanto, podemos suponer que $F(u, u) + bF(u, v) - cF(u, w) = 0$ para todo b. Haciendo $b = 0, 1$ concluimos que $F(u, v) = 0$, luego

$$c = F(u + v, u + v) = F(u, u),$$

luego $F(u, u) - F(u, u)F(u, w) = 0$, luego $F(u, w) = 1$. Esto significa que, cuando hemos elegido $v \in {}^{\perp}\langle u\rangle$ más arriba, podemos tomarlo tal que $F(u, v) = 1$ (tomando $v = w$), y reemplazando v por un múltiplo adecuado obtenemos $F(u + v, u + v) = 0$ con $F(u, v) \neq 0$, pero ahora el caso en que $F(u, u) + bF(u, v) - cF(u, w) = 0$ para todo valor de b no puede darse, ya que esto implica $F(u, v) = 0$, luego sólo se puede dar el caso que ya hemos visto que nos permite aplicar la hipótesis de inducción. ∎

Como consecuencia:

Teorema 9.34 *Si V es un espacio cuadrático sobre un cuerpo distinto del cuerpo de dos elementos, cada transformación ortogonal $f \in \mathrm{O}(V)$ se descompone en producto de $\dim V_f$ reflexiones salvo si V_f es totalmente singular, en cuyo caso se descompone en producto de $\dim V_f + 2 \leq \dim V$ reflexiones.*

DEMOSTRACIÓN: Si el subespacio $W = V_f$ contiene un vector no singular u, entonces $F_f(u,u) = Q(u) \neq 0$, luego (V_f, F_f) tiene al menos un vector no isótropo, luego podemos aplicar el teorema anterior, que nos da una base $w_1, \ldots, w_m$ de V_f tal que $F_f(w_i, w_i) = Q(w_i) \neq 0$ y $F_f(w_i, w_j) = 0$ siempre que $i > j$. Así

$$^{\perp}\langle w_1\rangle = \langle w_2 \ldots, w_m\rangle$$

y la transformación ortogonal asociada a $\langle w_1\rangle$ es R_{w_1}. Si llamamos f_1 a la asociada a $^{\perp}\langle w_1\rangle$, tenemos que $f = R_{w_1} f_1$, pero a su vez, en $W_1 = {}^{\perp}\langle w_1\rangle$ se cumple que

$$^{\perp}\langle w_2\rangle = \langle w_3 \ldots, w_m\rangle\,,$$

y razonando análogamente concluimos que $f = R_{w_1} R_{w_2} f_2$, y así, tras un número finito de pasos, llegamos a que f es producto de m reflexiones.

Si V_f es totalmente singular y $u \in V$ es un vector no singular, entonces tenemos que $u \notin V_f$, y el teorema 9.32 nos da que $V_{fR_u} = V_f \oplus \langle u\rangle$, que no es totalmente singular, luego el caso ya probado nos da que fR_u es producto de $m+1$ reflexiones, luego f es producto de $m+2$ reflexiones. ∎

Veamos ahora qué sucede cuando el cuerpo de escalares es el cuerpo de dos elementos. Para ello demostramos una versión débil del teorema 9.33:

Teorema 9.35 *Sea W un espacio vectorial sobre el cuerpo de dos elementos y F una forma bilineal en W simétrica y no degenerada y supongamos que existe al menos un vector no isótropo w tal que la restricción de F a $^{\perp}\langle w\rangle$ es totalmente isótropa. Entonces W tiene una base ortonormal.*

DEMOSTRACIÓN: Como la restricción de F a $\langle w\rangle^{\perp}$ es no degenerada, existen $u, v \in \langle w\rangle^{\perp}$ tales que $F(u,v) = 1$ (tienen que ser independientes, pues todos los vectores son isótropos). Sea $H = \langle u, v\rangle$, de modo que $\langle w\rangle^{\perp} = H \perp H'$, donde H' es el complemento ortogonal de H en $\langle w\rangle^{\perp}$. Si llamamos

$$w_1 = w + u, \quad w_2 = w + u + v,$$

entonces $F(w_i, w_i) = 1$ y $F(w_1, w_2) = 0$ y $\langle w_1, w_2\rangle^{\perp} = \langle w + v\rangle \oplus H'$, donde $w+v$ no es isótropo y la restricción de F a $H' = \langle w + v\rangle^{\perp}$ es totalmente isótropa. Razonando por inducción sobre la dimensión de W tenemos que $\langle w_1, w_2\rangle^{\perp}$ admite una base ortonormal, luego W también. ∎

Teorema 9.36 *Todo grupo ortogonal excepto $\mathrm{O}^+(4,2)$ está generado por las reflexiones.*

DEMOSTRACIÓN: Por el teorema 9.34 sólo necesitamos considerar el caso del grupo ortogonal $\mathrm{O}(V)$ de un espacio cuadrático V de dimensión n sobre el cuerpo de 2 elementos. Sea $f \in \mathrm{O}(V)$ y vamos a probar que es producto de reflexiones por inducción sobre $r = \dim V_f$.

Si $r = 0$ entonces $f = 1$ y la conclusión es trivial. Si existe $v \in V_f$ no singular, entonces el teorema 9.32 nos da que V_{fR_v} tiene dimensión $r-1$, luego por hipótesis de inducción fR_v es producto de reflexiones y f también. Por lo tanto, podemos suponer que V_f es totalmente singular.

En tal caso, la forma bilineal F_f es totalmente isótropa, pues se cumple que $F_f(v,v) = Q(v) = 0$. En particular esto implica que F_f es simétrica, pues

$$F_f(v+w, v+w) = F(v,w) + F(w,v) = 0,$$

luego $F(v,w) = F(w,v)$.

Si $u_1, \ldots, u_r$ es una base de $W = V_f$, por el teorema 8.27 existen $v_1, \ldots, v_r$ tales que los planos $\langle u_i, v_i\rangle$ son hiperbólicos y ortogonales dos a dos. El espacio $W' = \langle v_1, \ldots, v_r\rangle$ es totalmente singular y $V = W^\perp \oplus W'$, pues si $x \in W^\perp \cap W'$, entonces $x = \alpha_1 v_1 + \cdots + \alpha_r v_r$ y $\alpha_i = F(u_i, x) = 0$, luego $x = 0$, y entonces $\dim(W^\perp \oplus W') = n - r + r = n = \dim V$.

Supongamos en primer lugar que $n > 2r$, con lo que $W \oplus W'$ es un subespacio no degenerado (es suma ortogonal de planos hiperbólicos) de dimensión menor que n, luego $(W \oplus W')^\perp$ es un subespacio no degenerado no nulo, luego por 8.24 podemos tomar $w \in (W \oplus W')^\perp$ tal que $Q(w) = 1$. Entonces, por 9.32, tenemos que $V_{fR_w} = W \oplus \langle w\rangle$ y, por la nota posterior, la restricción a W de F_{fR_w} es F_f. Por consiguiente F_{fR_v} está en las condiciones del teorema anterior, luego $W \oplus \langle w\rangle$ tiene una base ortonormal $w_1, \ldots, w_{r+1}$ (respecto de F_{fR_v}), y el teorema 9.31 nos da entonces que $fR_v = R_{w_1} \cdots R_{w_{r+1}}$, luego f es producto de reflexiones.

Ahora suponemos que $n = 2r$. Si $r = 2$ entonces V es suma de dos planos hiperbólicos, luego $\mathrm{O}(V) = \mathrm{O}^+(4,2)$ es el caso exceptuado en el enunciado, así que suponemos $r \neq 2$. Como F_f es una forma bilineal simétrica no degenerada y totalmente isótropa en V_f, el espacio V_f tiene que ser suma de planos hiperbólicos (respecto a V_f), luego r es par. En efecto, si $u \in V_f$ es cualquier vector no nulo, tiene que existir $v \in V_f$ tal que $F_f(u,v) = 1$, y entonces (u,v) es un par hiperbólico,[3] luego $V_f = \langle u,v\rangle \perp \langle u,v\rangle^\perp$, y si $\langle u,v\rangle^\perp \neq 0$, en él podemos encontrar otro plano hiperbólico, de modo que, tras un número finito de pasos, tenemos una descomposición en suma de planos hiperbólicos.

En particular, si $H \leq V_f$ es un plano hiperbólico respecto de F_f, el teorema 9.31 nos da que $f = f_1 f_2$, donde $V_{f_1} = H$, $V_{f_2} = H^\perp$, y ni H ni $H^\perp$ es totalmente singular respecto de F_f (o, equivalentemente, respecto a V_{f_1} y V_{f_2}, respectivamente). Como estos espacios tienen dimensión $2 < r$ y $r - 2 < r$, respectivamente, por hipótesis de inducción f_1 y f_2 son productos de reflexiones, luego f también. ∎

[3] No podemos asegurar que F_f deriva de una forma cuadrática, luego, cuando hablamos de un par hiperbólico, suponemos únicamente que $\mathrm{N}(u) = \mathrm{N}(v) = 0$, $F_f(u,v) = 1$.)

El invariante de Dickson Si V es un espacio cuadrático y M es la matriz de su forma bilineal en una base prefijada, el grupo $\mathrm{O}(V)$ consta de los automorfismos de V cuya matriz en la base dada cumple $AMA^t = M$, y al tomar determinantes queda $|A|^2 = 1$, luego $|A| = \pm 1$. Así pues, la aplicación determinante es, en este caso, un homomorfismo de grupos

$$\det : \mathrm{O}(V) \longrightarrow \{\pm 1\}.$$

Es fácil ver que es suprayectivo, pues esto es trivialmente cierto si el cuerpo de escalares tiene característica 2, en cuyo caso $1 = -1$, y en caso contrario, las reflexiones son claramente transformaciones ortogonales de determinante -1. Así pues, si la característica del cuerpo de escalares no es 2, el núcleo de la aplicación determinante es un subgrupo de $\mathrm{O}(V)$ de índice 2. Vamos a ver que este subgrupo admite una definición alternativa que es válida también cuando el cuerpo de escalares tiene característica 2:

Definición 9.37 Si V es un espacio cuadrático, definimos el *invariante de Dickson* como la aplicación

$$D : \mathrm{O}(V) \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

dada por $D(f) = \dim V_f + 2\mathbb{Z}$.

Se trata de un epimorfismo de grupos, pues, salvo en el caso exceptuado en el teorema 9.36, todo elemento de $\mathrm{O}(V)$ es producto de reflexiones, $f = r_1 \cdots r_s$, y el teorema 9.32 implica que $D(f) = [s]$ (las reflexiones cumplen $\dim V_r = 1$ y, cada vez que componemos con una reflexión, la dimensión aumenta o disminuye una unidad, luego pasa de par a impar o viceversa).

En el caso de $\mathrm{O}^+(4,2)$, podemos verlo como subgrupo de $\mathrm{O}^+(4,4)$, pues si C es el cuerpo de 4 elementos y R el subcuerpo de 2 elementos, podemos considerar en $R^4 \subset C^4$ las formas cuadráticas dadas por

$$Q(x, y, z, w) = xy + zw.$$

Es claro que son ciertamente formas cuadráticas cuyas formas bilineales asociadas tienen, respecto a la base canónica, la matriz

$$J = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

de modo que $V = R^4$ o $V = C^2$ se descompone en suma ortogonal de dos planos hiperbólicos, por lo que es un espacio de tipo $\mathrm{O}^+(4,2)$ o $\mathrm{O}^+(4,4)$, respectivamente. Estos grupos se identifican con los grupos de las matrices M (con coeficientes en R o en C) que cumplen $MJM^t = J$, y a través de estas representaciones podemos considerar $\mathrm{O}^+(4,2) \leq \mathrm{O}^+(4,4)$.

Ahora, si $f \in \mathrm{O}^+(4,2)$ tiene matriz M respecto de la base canónica de $V = R^4$, entonces $V_f = \mathrm{Im}(1 - f) = \{x(I - M) \mid x \in R^4\}$, y su dimensión es el

rango de la matriz $I - M$, pero dicho rango es el mismo tanto si consideramos las matrices con coeficientes en R o en C (por ejemplo, porque coincide con el mayor número de filas de una submatriz cuadrada con determinante no nulo), luego $\dim V_f$ es la misma tanto si consideramos a f como elemento de $\mathrm{O}^+(4,2)$ o de $\mathrm{O}^+(4,4)$, luego $D : \mathrm{O}^+(4,2) \longrightarrow \mathbb{Z}/2\mathbb{Z}$ es la restricción del homomorfismo $D : \mathrm{O}^+(4,4) \longrightarrow \mathbb{Z}/2\mathbb{Z}$, luego es también un homomorfismo. De hecho es un epimorfismo, porque las reflexiones tienen invariante 1.

Tenemos, pues, que salvo en el caso de $\mathrm{O}^+(4,2)$, el invariante de Dickson $D(f)$ de una transformación ortogonal es 0 o 1 según si se puede expresar como composición de un número par o impar de reflexiones.

Definición 9.38 Si V es un espacio cuadrático, definimos el *grupo ortogonal especial* $\mathrm{OE}(V)$ como el núcleo del invariante de Dickson, que es un subgrupo de $\mathrm{O}(V)$ de índice 2.

Salvo en el caso de $\mathrm{O}^+(4,2)$, los elementos de $\mathrm{OE}(V)$ son las transformaciones ortogonales que se descomponen en un número par de reflexiones. Si la característica del cuerpo de escalares es distinta de 2, teniendo en cuenta que las reflexiones tienen determinante -1, es claro que los elementos de $\mathrm{OE}(V)$ son también las transformaciones ortogonales de determinante 1 o, dicho de otro modo, $\mathrm{OE}(V)$ es también el núcleo de la aplicación determinante.

Por ejemplo, si $\dim V = 2$, entonces $\mathrm{OE}(V)$ es el subgrupo de índice 2 construido en la prueba del teorema 8.45, de modo que $\mathrm{OE}(V) \cong C^*$ si V es un plano hiperbólico y $\mathrm{OE}(V)$ es isomorfo al núcleo de la norma $\mathrm{N} : K^* \longrightarrow C^*$ si V es no singular.

En efecto, si $V = \langle u, v\rangle$ es un plano hiperbólico, hemos visto que $\mathrm{O}(V)$ tiene un subgrupo N de índice 2 formado por las transformaciones dadas por $f_\alpha(u) = \alpha u$, $f_\alpha(v) = \alpha^{-1}v$, y entonces V_f está generado por $(1-\alpha)u$, $(1-\alpha^{-1})v$, luego $V_{f_\alpha} = \langle u, v\rangle$ salvo si $\alpha = 1$, en cuyo caso $V_{f_\alpha} = 0$, luego $D(f_\alpha) = 0$, y así $N \leq \mathrm{OE}(V)$, y como ambos subgrupos tienen índice 2 se da la igualdad.

En el caso en que $V = K$ es no singular, se razona igualmente con las transformaciones $f_\alpha(\xi) = \alpha\xi$, donde $\mathrm{N}(\alpha) = 1$ y obtenemos que $V_{f_\alpha} = \langle 1, \omega\rangle$ salvo si $\alpha = 1$.

En particular $\mathrm{OE}(V)$ es abeliano y $\mathrm{O}(V)$ es resoluble, por lo que nos interesará el caso en que $\dim V \geq 3$. El teorema siguiente resuelve el caso en que $\dim V = 3$. Recordemos que, según el teorema 8.38 la existencia de vectores isótropos está garantizada cuando el cuerpo de escalares es finito:

Teorema 9.39 *Si V es un espacio cuadrático singular tridimensional, entonces*

$$\mathrm{O}(V) \cong \{\pm 1\} \times \mathrm{OE}(V), \qquad \mathrm{OE}(V) \cong \mathrm{LGP}(2, C).$$

Demostración: Según 8.28, podemos descomponer $V = H_1 \perp W$, donde $H_1 = \langle u, v\rangle$ es un plano hiperbólico y $W = \langle w\rangle$ es un subespacio no singular. En particular, esto requiere que la característica del cuerpo C de escalares sea

impar (y esto hace el primer isomorfismo inmediato). El grupo de isometrías no se altera si cambiamos la forma cuadrática por un múltiplo no nulo, y así podemos exigir que $Q(w) = -1$. De este modo la matriz de F en la base (u, w, v) es

$$J = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Los vectores isótropos de V son los de la forma $xu + yw + zv$ con $y^2 = xz$. Si $z = 0$, necesariamente $y = 0$ y obtenemos los vectores de $\langle u \rangle$, mientras que si $z = 1$, $y = \alpha$ obtenemos los vectores de la forma

$$\alpha^2 u + \alpha w + v.$$

Por lo tanto, si llamamos $P_\infty = \langle u \rangle$ y $P_\alpha = \langle \alpha^2 u + \alpha w + v \rangle$, tenemos que

$$\Omega = \{P_\alpha \mid \alpha \in C\} \cup \{P_\infty\}$$

es el conjunto de todos los puntos isótropos del espacio proyectivo $P(V)$. El grupo $\mathrm{OE}(V)$ actúa sobre Ω, y vamos a probar que si identificamos a Ω con la recta proyectiva sobre C, esta acción se corresponde con la de $\mathrm{LGP}(2, C)$.

Para ello observamos en primer lugar que si un elemento $f \in \mathrm{OE}(V)$ fija a $P_\infty = \langle u \rangle$, también fija a $\langle u \rangle^\perp = \langle u, w \rangle$, luego su matriz tiene que ser de la forma

$$M = \begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & e & f \end{pmatrix}$$

con $acf = 1$. Para que f sea ortogonal tiene que cumplir $MJM^t = J$, lo que se traduce en que

$$af = 1, \qquad c^2 = 1, \qquad bf = 2ce, \qquad df = e^2$$

y, teniendo en cuenta que $acf = 1$, tiene que ser $c = 1$ y llegamos a que M es de la forma

$$M = \begin{pmatrix} a & 0 & 0 \\ 2ae & 1 & 0 \\ ae^2 & e & a^{-1} \end{pmatrix}.$$

Si definimos

$$T(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha^{-1} \end{pmatrix}, \qquad H(\beta) = \begin{pmatrix} 1 & 0 & 0 \\ 2\beta & 1 & 0 \\ \beta^2 & \beta & 1 \end{pmatrix},$$

que son las matrices que resultan de hacer $e = 0$ y $a = 1$, respectivamente, vemos que $M = H(e)T(a)$. Además, las transformaciones ortogonales con matriz $T(\alpha)$ son precisamente las que fijan a P_∞ y a P_0. Más precisamente:

$$P_x T(\alpha) = P_{\alpha x}, \qquad P_x H(\beta) = P_{x+\beta},$$

y a estas transformaciones añadimos la transformación S de matriz

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

que ciertamente es ortogonal y cumple $P_xS = P_{1/x}$, entendiendo que $1/0 = \infty$ y $1/\infty = 0$. Ahora ya es fácil extraer varias conclusiones:

1. $\mathrm{OE}(V)$ *actúa fielmente sobre* Ω*, con lo que tenemos un monomorfismo de grupos* $\mathrm{OE}(V) \longrightarrow \Sigma_\Omega$.

   En efecto, si $f \in \mathrm{OE}(V)$ fija a todos los puntos de Ω, en particular fija a P_∞, P_0, P_1. Hemos visto que si fija a los dos primeros puntos su matriz es $T(\alpha)$ y, el hecho de que fije a P_1 se traduce en que $\alpha = 1$, luego $f = 1$.

2. $\mathrm{OE}(V)$ *está generado por las transformaciones determinadas por las matrices* $T(\alpha), H(\beta), S$.

   En efecto, si $f \in \mathrm{OE}(V)$ y $f(P_\infty) = P_x$, con $x \in C$, entonces se cumple que $(fT(-x)S)(P_\infty) = P_\infty$, luego $fT(-x)S = H(\beta)T(\alpha)$, para ciertos α, β, luego f está en el subgrupo generado por las transformaciones indicadas.

3. $\mathrm{OE}(V)$ *es triplemente transitivo sobre* Ω.

   Dada cualquier terna de puntos (P, P', P'') distintos dos a dos, si $P = P_x$, con $x \neq \infty$, la transformación $f_1 = P_{-x}S$ cumple $f_1(P_x) = P_\infty$. Si $P = P_\infty$ tomamos $f_1 = 1$. En cualquier caso, $f_1(P) = P_\infty$. Sea $f_1(P') = P_y$, de modo que $f_2 = f_1H(-y)$ cumple $f_2(P) = P_\infty$, $f_2(P') = P_0$. Por último, sea $f_2(P'') = P_z$, con lo que $f_3 = f_2F(z^{-1})$ cumple $f_3(P) = P_\infty$, $f_3(P') = P_0$, $f_3(P'') = P_1$.

4. *La restricción a* Ω *es un isomorfismo* $\mathrm{OE}(V) \longrightarrow \mathrm{LGP}(\Omega) \cong \mathrm{LGP}(2, C)$.

   Basta tener en cuenta que las transformaciones ortogonales con matrices $T(\alpha)$, $H(\beta)$ o S se restringen a homografías de Ω, luego todas las demás también. Esto prueba que la restricción es un monomorfismo entre los grupos indicados. La suprayectividad se debe al punto precedente, pues una homografía de una recta proyectiva está completamente determinada por la imagen de tres puntos cualesquiera, por ejemplo, P_∞, P_0, P_1 y, como hay una homografía en la imagen de $\mathrm{OE}(V)$ que transforma estos tres puntos en otros tres cualesquiera, dicha imagen incluye todas las homografías de Ω. ∎

En particular, $\mathrm{OE}(3,3) \cong \mathrm{LGP}(2,3) \cong \Sigma_4$ es resoluble, pero

$$\mathrm{OE}'(3,q) \cong \mathrm{LEP}(2,q)$$

es un grupo simple salvo si $q = 3$ (teorema 7.17).

Vemos así que, a diferencia de lo que sucede con los grupos $\mathrm{LE}(V)$ y $\mathrm{UE}(V)$, los grupos $\mathrm{OE}(V)$ todavía contienen un subgrupo de índice 2 al que tenemos que restringirnos si queremos obtener un grupo simple. (Lo hemos probado cuando el espacio V tiene dimensión 3, pero vamos a ver que lo mismo vale en general.)

La norma espinorial Si F es una forma bilineal en un espacio vectorial V sobre un cuerpo C y M, N son las matrices de F respecto de dos bases de V, se cumple la relación $N = BMB^t$, donde B es la matriz de cambio de base (la que nos da las coordenadas xB respecto de la base asociada a M a partir de las coordenadas x respecto de la base asociada a N). Por consiguiente, $|N| = |B|^2|M|$.

Así pues, las matrices de F respecto de bases distintas son distintos, pero dos cualesquiera de ellos se diferencian en un cuadrado. Por ello podemos definir el *discriminante* de la forma F como

$$\operatorname{disc} F = |M|C^{*2} \in C/C^{*2},$$

donde M es la matriz de F respecto de cualquier base. Así, el discriminante de F nos dice si la matriz de F respecto de cualquier base es o no un cuadrado en C.

Definición 9.40 Si V es un espacio cuadrático, definimos la *norma espinorial* de V como la aplicacion $\theta : \mathrm{O}(V) \longrightarrow C/C^{*2}$ dada por $\theta(f) = \operatorname{disc} F_f$.

Por ejemplo, para una reflexión tenemos que $V_{R_v} = \langle v\rangle$, con lo que la norma espinorial es $\theta(R_v) = Q(v)C^{*2}$.

Vamos a probar que θ es un homomorfismo de grupos. Para ello consideramos una transformación $f \in \mathrm{O}(V)$ y una reflexión R_v, donde $v \in V$ es un vector no singular. Si $v \in V_f$, el teorema 9.31 nos da que $f = R_v f'$, donde f' es la transformación ortogonal asociada a $W_2 = {}^{\perp}\langle v\rangle$, con la forma $F_{f'}$ que resulta de restringir F_f a W_2. Completando con v una base de W_2 obtenemos una base de V_f en la cual la matriz de F_f es de la forma

$$M = \left(\begin{array}{c|c} Q(v) & * \\ \hline 0 & M' \end{array}\right),$$

donde M' es la matriz de $F_{f'}$. Por lo tanto, $|M| = Q(v)|M'|$ y, por consiguiente, $\theta(f) = \theta(R_v)\theta(f')$, pero $f' = fR_v$, luego $\theta(fR_v) = \theta(f)\theta(R_v)$.

Si $v \notin V_f$, el teorema 9.32 nos da que $V_{fR_v} = V_f \oplus \langle v\rangle$, y aplicando a fR_v el caso precedente concluimos que $\theta(fR_vR_v) = \theta(fR_v)\theta(R_v)$, que equivale a $\theta(fR_v) = \theta(f)\theta(R_v)$.

Por lo tanto, la igualdad se cumple en ambos casos, y, más en general, si $f = R_{v_1}\cdots R_{v_s}$ se descompone en producto de reflexiones, se cumple que $\theta(f) = \theta(R_{v_1})\cdots\theta(R_{v_s})$, y esto prueba que θ es es un homomorfismo de grupos siempre que $\mathrm{O}(V)$ está generado por las reflexiones, es decir, salvo a lo sumo en el caso de $\mathrm{O}^+(4,2)$. Pero en este caso $C^* = C^{*2}$, luego θ es constante y es trivialmente un homomorfismo.

Más aún, si V es singular, la norma espinorial es un epimorfismo incluso restringida a $\theta : \mathrm{OE}(V) \longrightarrow C^*/C^{*2}$.

En efecto, podemos tomar un par hiperbólico (u,v) en V y, si $a \in C^*$, los vectores $u+v$ y $u+av$ son no singulares. Entonces $f = R_{u+v}R_{u+av} \in \mathrm{OE}(V)$ (porque es producto de un número par de reflexiones) y

$$\theta(f) = \theta(R_{u+v})\theta(R_{u+av}) = Q(u+v)Q(u+av)C^{*2} = aC^{*2}.$$

Así pues, siempre que V es isótropo y $C^* \neq C^{*2}$, el grupo $\mathrm{OE}(V)$ posee un subgrupo normal de índice 2, el núcleo de la norma espinorial. Vamos a ver que se trata del subgrupo derivado de $\mathrm{O}(V)$.

Definición 9.41 Si V es un espacio cuadrático, llamaremos $\Omega(V) = \mathrm{O}(V)'$.

Necesitamos un hecho elemental:

Teorema 9.42 *Si un grupo G está generado por elementos de orden 2 entonces todo cuadrado en G está en G'.*

Demostración: Si $g \in G$, podemos expresarlo como $g = g_1 \cdots g_r$, con cada g_i de orden 2, y entonces $g^2G' = g_1 \cdots g_r g_1 \cdots g_r G' = g_1^2 \cdots g_r^2 G' = G'$ (porque G/G' es abeliano), luego $g^2 \in G'$. ∎

Teorema 9.43 *Si V es un espacio cuadrático singular de dimensión ≥ 2, entonces, salvo en el caso de $\Omega^+(4,2)$, se cumple que*

$$\Omega(V) = \{f \in \mathrm{OE}(V) \mid \theta(f) = C^{*2}\}.$$

Por lo tanto, $\mathrm{OE}(V)/\Omega(V) \cong C^*/C^{*2}$.

Demostración: Sea $H = \langle u, v\rangle$ un plano hiperbólico en V. Si $f \in \mathrm{O}(H)$ no es una reflexión, entonces $V_f = H$, con lo que $w = u + v \in V_f$ es un vector no singular, luego el teorema 9.31 nos permite descomponer $f = R_w f'$, donde $\dim V_{f'} = 1$, luego f' también es una reflexión, y así resulta que todo elemento de $\mathrm{O}(H)$ es la identidad, una reflexión o un producto de dos reflexiones, luego todo elemento de $\mathrm{OE}(H)$ es la identidad o un producto de dos reflexiones, una de las cuales puede tomarse igual a R_{u+v}, y la otra será de la forma R_{u+av} (pues los vectores no singulares de H son los de la forma $xu + yv$ con $xy \neq 0$, y $u + x^{-1}yv$ determina la misma reflexión).

En suma, si $f \in \mathrm{OE}(H)$, entonces $f = R_{u+v}R_{u+av}$, donde $\theta(f) = aC^{*2}$. Es fácil ver que $f(u) = a^{-1}u$, $f(v) = av$.

Supongamos ahora que $V = H$. Si $\theta(f) = C^{*2}$, entonces $a = b^2$, para cierto $b \in C^*$, y entonces $f = g^2$, donde $g = R_{u+v}R_{u+bv}$. Como $\mathrm{O}(V)$ está generado por las reflexiones, que tienen orden 2, el teorema anterior nos da que $f \in \Omega(V)$. Con esto hemos probado que

$$\mathrm{OE}(V) \cap \mathrm{N}(\theta) \leq \Omega(V),$$

pero el subgrupo de la izquierda es normal en $\mathrm{O}(V)$ y el cociente tiene a lo sumo orden 4, luego es abeliano, y eso nos da la inclusión opuesta.

Supongamos ahora que $V \neq H$. Dado $f \in \mathrm{O}(V)$, podemos descomponerlo como producto de reflexiones $f = R_{u_1} \cdots R_{u_s}$. Sea $v_i = u + Q(u_i)v \in H$, de modo que $Q(v_i) = Q(u_i)$. Por el teorema de Witt 8.29, existe $h_i \in \mathrm{O}(V)$ tal que $h_i(u_i) = v_i$, con lo que $R_{u_i}^{h_i} = R_{v_i}$ y, como $\Omega(V)$ determina un cociente abeliano, $R_{u_i} \equiv R_{v_i}$ (mód $\Omega(V)$), luego $f \equiv g$ (mód $\Omega(V)$), donde $g = R_{v_1} \cdots R_{v_s}$.

Supongamos que $f \in \mathrm{OE}(V)$ y que $\theta(f) = C^{*2}$ y vamos a ver que $g \in \Omega(V)$, lo que implica que $f \in \Omega(V)$. Claramente, $g|_H = R_{v_1} \cdots R_{v_s}$, donde ahora las reflexiones son las de $\mathrm{O}(H)$. Por lo tanto, $g|_H \in \mathrm{OE}(H)$ (porque s es par), y como $\theta(R_{v_i}) = Q(v_i) = Q(u_i) = \theta(R_{u_i})$, resulta que $\theta(g|_H) = C^{*2}$. Por el caso anterior, $g|_H \in \Omega(H)$, es decir, que $g|_H$ es producto de conmutadores $[p_i, q_i]$ con $p_i, q_i \in \mathrm{O}(H)$, pero claramente p_i, q_i se extienden a transformaciones $p_i, q_i \in \mathrm{O}(V)$ que dejan invariantes a los vectores de $H^\perp$, al igual que g, luego g es el producto de los conmutadores $[p_i, q_i]$ de las extensiones y así $g \in \Omega(V)$. Con esto hemos probado que

$$\mathrm{OE}(V) \cap \mathrm{N}(\theta) \leq \Omega(V)$$

y, como antes, tenemos la igualdad. ∎

Teorema 9.44 *Si V es un espacio cuadrático singular de dimensión $n \geq 3$, entonces $\Omega(V) = \mathrm{OE}'(V)$ excepto en el caso de $\Omega^+(4, 2)$.*

Demostración: Si u, v son vectores no singulares no nulos, tenemos que $[R_u, R_v] = (R_u R_v)^2$. Llamemos K al subgrupo generado por estos conmutatores, de modo que $K \leq \Omega(V)$.

Como $R_u^f = R_{f(u)}$, para todo $f \in \mathrm{O}(V)$, se cumple que $K \trianglelefteq \mathrm{O}(V)$. Por el teorema 9.36 tenemos que $\mathrm{O}(V)/K$ está generado por las clases de las reflexiones, y éstas conmutan, luego el cociente es un grupo abeliano, luego $\Omega(V) \leq K$, y así tenemos la igualdad $\Omega(V) = K$.

Consideremos un generador $[R_u, R_v]$. Podemos suponer que u y v son linealmente independientes o, de lo contrario, $R_u = R_v$ y el conmutador es trivial. Más aún, podemos suponer que $F(u, v) \neq 0$, pues en caso contrario es fácil ver que R_u y R_v conmutan, e igualmente el conmutador es trivial. Llamemos $U = \langle u, v \rangle$. Si $w \in U^\perp$ es no singular, entonces R_w conmuta con R_u y R_v, por lo que

$$[R_u, R_v] = [R_u R_w, R_v R_w] \in \mathrm{OE}'(V).$$

Si, por el contrario, $U^\perp$ es totalmente singular, el teorema 8.24 nos da que la forma bilineal es idénticamente nula en $U^\perp$, luego $U^\perp \leq U^{\perp\perp} = U$, pero no puede ser $U = U^\perp$, pues $F(u, v) \neq 0$, luego $n - 2 = \dim U^\perp \leq 1$, luego $n \leq 3$ y así $n = 3$ y estamos en las condiciones del teorema 9.39. Si la característica del cuerpo es 2, $\mathrm{O}(V) = \mathrm{OE}(V)$ y trivialmente $[R_u, R_v] \in \mathrm{OE}'(V)$, y en caso contrario $[R_u, R_v] = [-R_u, -R_v] \in \mathrm{OE}'(V)$.

Así pues, $\Omega(V) \leq \mathrm{OE}'(V)$, pero $\mathrm{OE}(V)/\Omega(V)$ es abeliano, luego tenemos también la inclusión opuesta, luego la igualdad. ∎

Transformaciones de Siegel Ahora vamos a encontrar unas transformaciones que generen $\Omega(V)$.

Definición 9.45 Sea V un espacio cuadrático, $u \in V$ un vector singular y $y \in \langle u\rangle^\perp$. Definimos la *transformación de Siegel* $\rho_{u,y} : V \longrightarrow V$ mediante

$$\rho_{u,y}(w) = w + F(w,y)u - F(w,u)y - Q(y)F(w,u)u.$$

Obviamente es lineal y un cálculo rutinario muestra que

$$F(\rho_{u,y}(w), \rho_{u,y}(w')) = F(w,w').$$

En efecto, al desarrollar el miembro izquierdo aparecen ocho sumandos, pero se cancelan todos menos $F(w,w')$. Esto implica que $\rho_{u,y}$ es inyectiva, pues si $\rho_{u,y}(w) = 0$, entonces $F(w,w') = F(0,\rho_{u,y}(w')) = 0$, para todo $w' \in V$, luego $w = 0$. Por lo tanto, $\rho_{u,y} \in \mathrm{O}(V)$.

Observemos que si $w \in \langle u\rangle^\perp$ la expresión se simplifica:

$$\rho_{u,y}(w) = w + F(w,y)u \in \langle u\rangle^\perp.$$

Teorema 9.46 *Si V es un espacio cuadrático, $u \in V$ es un vector singular y $y \in \langle u\rangle^\perp$, entonces $\rho_{u,y}$ es la única transformación ortogonal que, para todo $w \in \langle u\rangle^\perp$, cumple*

$$\rho_{u,y}(w) = w + F(w,y)u.$$

Demostración: Sea $f \in \mathrm{O}(V)$ otra transformación ortogonal que cumpla esta propiedad, de modo que $g = f^{-1}\rho_{u,y}$ cumple que $g|_{\langle u\rangle^\perp} = 1$. Sea $v \in V$ tal que $H = \langle u, v\rangle$ sea un plano hiperbólico. Entonces $H^\perp \leq \langle u\rangle^\perp$, luego $g|_{H^\perp} = 1$. Esto implica que $g[H] = g[H^{\perp\perp}] = g[H^\perp]^\perp = H^{\perp\perp} = H$. Además, $g(u) = u$. Pongamos que $g(v) = \alpha u + \beta v$. Entonces

$$1 = F(u,v) = F(u, \alpha u + \beta v) = \beta,$$

$$0 = Q(v) = Q(\alpha u + v) = \alpha,$$

luego $g(v) = v$, por lo que $g|_H = 1$ y, por consiguiente, $g = 1$. ∎

El teorema anterior permite probar fácilmente las relaciones siguientes (comprobando que la cumplen las restricciones a $\langle u\rangle^\perp$):

1. $\rho_{u,y+z} = \rho_{u,y}\rho_{u,z}$,
2. $\rho_{\alpha u,z} = \rho_{u,\alpha z}$,
3. $\rho_{u,y}^{-1} = \rho_{u,-y}$,
4. $\rho_{u,y} = 1$ si y sólo si $y \in \langle u\rangle$,
5. Si $f \in \mathrm{O}(V)$, entonces $f^{-1}\rho_{u,y}f = \rho_{f(u),f(y)}$.

Por ejemplo, para probar la última observamos que si $w \in \langle u\rangle^\perp$, entonces $f(w) \in \langle f(u)\rangle^\perp$, y

$$(f^{-1}\rho_{u,y}f)(f(w)) = f(\rho_{u,y}(w)) = f(w + F(w,y)u) =$$

$$f(w) + F(w,y)f(u) = f(w) + F(f(w),f(y))f(u) = \rho_{f(u),f(y)}(f(w)),$$

por lo que $f^{-1}\rho_{u,y}f$ y $\rho_{f(u),f(y)}$ coinciden sobre $\langle f(u)\rangle^\perp$, luego son iguales.

Así, si $u \in V$ es un vector singular, la aplicación $\langle u\rangle^\perp \longrightarrow O(V)_u$ dada por $y \mapsto \rho_{u,y}$ es un homomorfismo de grupos por 1, luego su imagen

$$A_u = \{\rho_{u,y} \mid y \in \langle u\rangle^\perp\},$$

es un subgrupo abeliano del estabilizador $O(V)_u$. De hecho, $A_u \trianglelefteq O(V)_u$ por la propiedad 5.

Teorema 9.47 *Si V es un espacio cuadrático y $u \in V$ es singular, el grupo A_u actúa regularmente sobre el conjunto de los puntos singulares de $P(V)$ no ortogonales a $\langle u\rangle$.*

Demostración: Sean $Q = \langle v\rangle$, $R = \langle w\rangle$ puntos singulares de $P(V)$ no ortogonales a $P = \langle u\rangle$. Podemos suponer que $F(u,v) = F(u,w) = 1$. Entonces $H = \langle u, v\rangle$ es un plano hiperbólico y $V = H \perp H^\perp$. Sea $w = au + bv + x$, con $x \in H^\perp$. La condición $F(u,w) = 1$ se traduce en que $b = 1$, mientras que $Q(w) = 0$ nos da que $a = -Q(x)$. Así pues, $w = -Q(x)u+v+x$ y $\rho_{u,-x}(v) = w$. Por lo tanto, A_u actúa transitivamente sobre el conjunto indicado.

Si $y \in \langle u\rangle^\perp$ tal que $\rho_{u,y}(Q) = Q$, es decir, $\rho_{u,y}(v) = \alpha v$, y desarrollando esta igualdad obtenemos que $y \in \langle u, v\rangle = H$. De hecho, tiene que ser $y \in \langle u\rangle$, pues en caso contrario $v \in \langle u, y\rangle \leq \langle u\rangle^\perp$, en contra de lo supuesto. Por lo tanto, $\rho_{u,y} = 1$ y los estabilizadores son triviales, luego la acción es regular. ∎

Teorema 9.48 *Si V es un espacio cuadrático de dimensión $n \geq 3$, el subgrupo generado por las transformaciones de Siegel actúa transitivamente sobre el conjunto X de los puntos singulares de $P(V)$.*

Demostración: Sean $P = \langle u\rangle$, $Q = \langle v\rangle \in X$. Si $F(u,v) = 0$, el teorema 8.27 nos da planos hiperbólicos ortogonales $\langle u, u'\rangle$, $\langle v, v'\rangle$, y llamando $w = u' + v'$ tenemos que w es singular y $F(u,w) = F(v,w) = 1$. El teorema anterior nos da un elemento de A_x que transforma P en Q.

Si $F(u,v) \neq 0$, podemos suponer que $F(u,v) = 1$ y $H = \langle u, v\rangle$ es un plano hiperbólico. Sea $w \in H^\perp$ no singular. Llamamos $x = u - Q(w)v + w$, con lo que x es singular, $F(u,x) = Q(w)$, $F(v,x) = 1$. El teorema anterior nos da un elemento de A_x que transforma P en Q. ∎

Vamos a probar que el subgrupo generado por las transformaciones de Siegel es precisamente $\Omega(V)$, pero aún necesitamos algunos resultados previos:

Teorema 9.49 *Las transformaciones de Siegel tienen norma espinorial trivial.*

DEMOSTRACIÓN: Sea V un espacio cuadrático y $\rho_{u,y}$ una transformación de Siegel. Si $\rho_{u,y} = 1$ la conclusión es trivial, así que podemos suponer que $\rho_{u,y} \neq 1$, lo que equivale a que $y \notin \langle u\rangle$.

Veamos que $V_{\rho_{u,y}} = \langle u, y\rangle$. En efecto, de la propia definición se sigue que $V_{\rho_{u,y}} \leq \langle u, y\rangle$. No puede ser que $\langle u\rangle^\perp \leq \langle y\rangle^\perp$, pues entonces $\langle y\rangle \leq \langle u\rangle$. Por lo tanto podemos tomar un vector $w \in \langle u\rangle^\perp \setminus \langle y\rangle^\perp$, y podemos exigir que $F(w, y) = 1$. Entonces $\rho_{u,y}(w) = w + u$, luego $u \in V_{\rho_{u,y}}$. Por otra parte, tomando $w \in V \setminus \langle u\rangle$ (y podemos exigir que $F(w, u) = 1$) tenemos que

$$\rho_{u,y}(w) = w + F(w, y)u - y - Q(y)F(w, u)u,$$

de donde $y \in V_{\rho_{u,y}}$. Esto nos da la igualdad $V_{\rho_{u,y}} = \langle u, y\rangle$. Por una parte tenemos que $F_{\rho_{u,y}}(u, u) = Q(u) = 0$ y, por otra parte, tenemos la relación

$$F_{\rho_{u,y}}(u, v) + F_{\rho_{u,y}}(v, u) = F(u, v) = 0,$$

luego la matriz de $F_{\rho_{u,y}}$ en la base u, v es

$$\begin{pmatrix} 0 & \alpha \\ -\alpha & \beta \end{pmatrix}$$

y su determinante es α^2, luego $\theta(\rho_{u,y}) = C^{*2}$. ∎

Teorema 9.50 *Todo espacio cuadrático V está generado por sus vectores no singulares excepto el plano hiperbólico sobre el cuerpo de dos elementos.*

DEMOSTRACIÓN: Supongamos que $u \in V$ es singular. Entonces $\dim V \geq 2$. Si $\dim V > 2$, entonces u está contenido en un plano hiperbólico H y $H^\perp$ contiene un vector no singular v. Entonces $u = (u + v) - v$ y ambos sumandos son no singulares. Si $\dim V = 2$, puesto que tiene un vector singular, V es un plano hiperbólico, digamos $V = \langle u, v\rangle$. Si $\alpha \neq 0, 1$, entonces

$$u = (\alpha u + v) + ((1 - \alpha)u - v),$$

donde los dos sumandos son no singulares (pero si el cuerpo de escalares es $C = \{0, 1\}$, entonces V tiene un único vector no singular no nulo, que obviamente no genera todo el plano). ∎

Como consecuencia:

Teorema 9.51 *Si V es un espacio cuadrático y $u \in V$ es un vector singular, el grupo A_u está generado por las transformaciones $\rho_{u,y}$, donde $y \in \langle u\rangle^\perp$ es no singular, excepto si V tiene dimensión 4 e índice de Witt 2 y el cuerpo de escalares tiene 2 elementos.*

DEMOSTRACIÓN: Si $\langle u\rangle^\perp$ no contiene vectores singulares la conclusión es obvia. Si, por el contrario, $y \in \langle u\rangle^\perp$ es singular, el teorema 8.27 nos da vectores singulares v, z tales que $\langle u, v\rangle \perp \langle y, z\rangle$ es una suma ortogonal de planos hiperbólicos. Si llamamos $H = \langle u, v\rangle$, tenemos que $y \in H^\perp$ y $V = H \perp H^\perp$. Por el teorema anterior tenemos que y se expresa como suma de vectores no singulares de $H^\perp$ salvo si $H^\perp$ es un plano hiperbólico sobre el cuerpo de 2 elementos, es decir, salvo si V está en el caso exceptuado en el enunciado. Por consiguiente, $\rho_{u,y}$ es composición de transformaciones de Siegel $\rho_{u,w}$, donde $w \in H^\perp$ es no singular. ∎

A su vez:

Teorema 9.52 *Si V es un espacio cuadrático y $u \in V$ es singular e $y \in \langle u\rangle^\perp$ es no singular, entonces*

$$\rho_{u,y} = R_{Q(y)u-y}R_y.$$

DEMOSTRACIÓN: Como $y \notin \langle u\rangle$, tenemos que $\rho_{u,y} \neq 1$, y en la prueba del teorema 9.49 hemos visto que $V_{\rho_{u,y}} = \langle u, y\rangle$. Tomemos $w \in V$ tal que $w - \rho_{u,y}(w) = y$. Esto equivale a que $F(w, u) = 1$ y $F(w, Q(y)u - y) = 0$. El teorema 9.32 nos da que

$$V_{\rho_{u,y}R_y} = \langle u, y\rangle \cap \langle w\rangle^\perp = \langle Q(y)u - y\rangle\,.$$

Por lo tanto, $\rho_{u,y}R_y = R_{Q(y)u-y}$ y tenemos la conclusión. ∎

Ahora ya podemos probar:

Teorema 9.53 *Si V es un espacio cuadrático singular de dimensión $n \geq 3$, entonces $\Omega(V)$ está generado por las transformaciones de Siegel salvo en el caso de $\Omega^+(4, 2)$.*

DEMOSTRACIÓN: Por el teorema 9.51, toda transformación de Siegel de V es producto de transformaciones $\rho_{u,y}$ con y no singular, las cuales están en $\mathrm{OE}(V)$ por el teorema anterior, luego todas las transformaciones de Siegel están en $\mathrm{OE}(V)$ y, de hecho, están en $\Omega(V)$ por los teoremas 9.43 y 9.49. Así pues, si llamamos N al subgrupo generado por las transformaciones de Siegel, tenemos que $N \leq \Omega(V)$.

Como V es singular, contiene un plano hiperbólico H. Si $u \in V$ es no singular, existe $u' \in H$ con $Q(u') = Q(u)$ y por el teorema de Witt 8.29 existe $f \in \mathrm{O}(V)$ tal que $f(u') = u$.

Si $H = \langle u_0, v_0\rangle$, por el teorema 9.48 existe $g_1 \in N$ tal que $g_1(\langle u_0\rangle) = \langle f(u_0)\rangle$ y por 9.47 existe $g_2 \in N$ tal que $g_2(\langle g_1(u_0)\rangle) = \langle g_1(u_0)\rangle$ y $g_2(\langle g_1(v_0)\rangle) = \langle f(v_0)\rangle$. Así $g = g_1g_2 \in N$ cumple $g[H] = f[H]$, luego llamando $w = g^{-1}(u) \in H$, tenemos que $R_u = R_w^g$. Como $N \trianglelefteq \mathrm{O}(V)$,

$$R_u = R_wR_w^{-1}(g^{-1}R_wg) = R_w(R_w^{-1}g^{-1}R_w)g \in \mathrm{O}(H)N,$$

donde identificamos $\mathrm{O}(H)$ con el subgrupo de las transformaciones de $\mathrm{O}(V)$ que se restringen a la identidad en $H^\perp$. Como $\mathrm{O}(V)$ está generado por las reflexiones, concluimos que $\mathrm{O}(H)N = \mathrm{O(V)}$.

Por otra parte, $N \leq \Omega(V) \leq \mathrm{OE}(V)$, luego $\mathrm{OE}(V) = \mathrm{OE}(H)N$, pues si $h \in \mathrm{OE}(V)$, se descompone como $h = h_1h_2$, con $h_1 \in \mathrm{O}(H)$ y $h_2 \in \mathrm{N}$, luego $D(h) = D(h_2) = 0$, luego $D(h_1) = 0$ y así $h_1 \in \mathrm{OE}(H)$. Por lo tanto

$$\mathrm{OE}(V)/N \cong \mathrm{OE}(H)/(\mathrm{OE}(H) \cap N),$$

pero $\mathrm{OE}(H)$ es abeliano (véanse las observaciones tras la definición 9.38), luego, teniendo en cuenta 9.44, concluimos que $\Omega(V) = \mathrm{OE}'(V) \leq N$ y tenemos la igualdad. ∎

El grupo $\Omega^+(4,2)$ Antes de seguir analizaremos el grupo $\Omega^+(4,2)$ que nos está apareciendo como excepción en los teoremas que hemos demostrado.

Consideremos un espacio cuadrático V de dimensión $n = 4$ e índice de Witt $m = 2$ sobre el cuerpo C de dos elementos. Consideremos en él dos vectores singulares arbitrarios u_1, u_2 linealmente independientes y ortogonales. El teorema 8.27 nos da vectores $v_1, v_2 \in V$ de modo que $V = \langle u_1, v_1\rangle \perp \langle u_2, v_2\rangle$ es una descomposición de V en suma ortogonal de planos hiperbólicos. Vamos a representar los vectores de V en términos de sus coordenadas (x, y, z, w) respecto de la base u_1, v_1, u_2, v_2. La matriz de la forma bilineal respecto a dicha base es

$$J = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

y la forma cuadrática es

$$Q(x, y, z, w) = xy + zw.$$

Es fácil ver entonces que en V hay exactamente 6 vectores no singulares no nulos, a saber,

$$a = (0,0,1,1), \quad b = (1,1,1,0), \quad c = (1,1,0,1),$$
$$a' = (1,0,1,1), \quad b' = (1,1,0,0), \quad c' = (0,1,1,1).$$

La notación no es casual, sino que, así distribuidos, estos vectores determinan dos subespacios no singulares

$$W_1 = \{0, a, b, c\}, \qquad W_2 = \{0, a', b', c'\},$$

que son los únicos posibles, pues si tratamos de emparejar cualquier vector no nulo de W_1 con cualquier vector no nulo de W_2 veremos que su suma es singular. Es fácil comprobar que ambos subespacios son no degenerados por lo que constituyen planos ortogonales no singulares. Más aún, $V = W_1 \perp W_2$.

Por el teorema 9.50 (o simplemente comprobando que los seis vectores no singulares contienen una base de V) tenemos que toda transformación $f \in \mathrm{O}(V)$

está determinada por su restricción al conjunto de los seis vectores no singulares, lo que nos da un monomorfismo de grupos

$$\mathrm{O}^+(4,2) \longrightarrow \Sigma_6.$$

Es evidente que toda $f \in \mathrm{O}(V)$ debe fijar los subespacios W_i o bien intercambiarlos. Las dos posibilidades suceden realmente, pues si consideramos la transformación de Siegel $\rho = \rho_{u_1,u_2}$, un cálculo rutinario muestra que

$$\rho(a) = a', \quad \rho(b) = b', \quad \rho(c) = c'$$

(hemos elegido la notación para que así sea). Equivalentemente, vista como permutación,

$$\rho = (a, a')(b, b')(c, c').$$

En particular $\rho[W_1] = W_2$. Las transformaciones ortogonales que fijan los subespacios W_i forman claramente un subgrupo $N \cong \mathrm{O}(W_1) \times \mathrm{O}(W_2)$. Según el teorema 8.45 tenemos que $\mathrm{O}(W_i) = \mathrm{O}^-(2,2) \cong \Sigma_3$, luego en definitiva,

$$N \cong \Sigma_3 \times \Sigma_3.$$

Pero si $f \in \mathrm{O}(V)$ no fija a los W_i, $f\rho$ sí que lo hace, lo cual prueba que $\mathrm{O}^+(4,2) = \langle\rho\rangle N$ y, más precisamente, que tenemos una descomposición en producto semidirecto

$$\mathrm{O}^+(4,2) \cong C_2[\Sigma_3 \times \Sigma_3].$$

donde $C_2 = \langle\rho\rangle$ actúa sobre $\Sigma_3 \times \Sigma_3$ mediante la acción dada por $(\sigma, \tau)^\rho = (\tau, \sigma)$.

Con esto tenemos, en particular, que $|\mathrm{O}^+(4,2)| = 72 = 2^3 \cdot 3^2$. A su vez, $\mathrm{OE}^+(4,2)$ tiene que ser un subgrupo de orden 36, pero vamos a ver que no es N.

Para ello observamos que la reflexión asociada, por ejemplo, al vector a tiene que fijar a los vectores de $\langle a\rangle^\perp$, lo que incluye al propio a y a los de W_2, luego, como permutación, tiene que ser $R_a = (b, c)$. En general, las seis reflexiones de V son las seis transposiciones

$$(a, b), \quad (a, c), \quad (b, c), \quad (a', b'), \quad (a', c'), \quad (b', c'),$$

todas las cuales están en N, pero no en $\mathrm{OE}^+(4,2)$. Como ambos grupos tienen orden 36 e índice 2 en $\mathrm{O}^+(4,2)$, concluimos que el subgrupo

$$W = N \cap \mathrm{OE}^+(4,2)$$

tiene orden 18. Además, ahora es inmediato que el subgrupo generado por las reflexiones es N y no $\mathrm{O}^+(4,2)$, lo que justifica la excepción del teorema 9.36.

Por otra parte, por el teorema 9.32, sí que tienen que estar en $\mathrm{OE}^+(4,2)$ (luego en W) los productos de dos reflexiones, y ello incluye los cuatro ciclos de longitud 3:

$$(a, b, c), \quad (c, b, a), \quad (a', b', c'), \quad (c', b', a')$$

que resultan de multiplicar pares de transposiciones del mismo "grupo" a, b, c o a', b', c', y los 9 productos "mixtos" de una transposición de cada grupo. Los ciclos de longitud 3 generan $A_3 \times A_3$ que, con los 9 pares de transposiciones "mixtas" obtenemos las 18 permutaciones que tiene que tener W.

Por lo tanto, si llamamos, por ejemplo, $z = (a, b)(a', b')$ a una cualquiera de las transposiciones "mixtas", resulta que $W = \langle z \rangle\, (A_3 \times A_3)$. Más precisamente, si llamamos $x = (a, b, c)$, $y = (a', b', c')$ a un generador de $A_3 \times A_3$, resulta que

$$W = \{x, y, z \mid x^3 = y^3 = z^2 = 1,\ xy = yx,\ x^z = x^{-1},\ y^z = y^{-1}\}$$

es el quinto grupo de la lista del teorema 3.44.

Para identificar $\mathrm{OE}^+(4, 2)$ basta recordar que en la prueba de 9.49 hemos visto que las transformaciones de Siegel no triviales cumplen $\dim V_\rho = 2$, por lo que $\rho \in \mathrm{OE}^+(4, 2)$, luego tiene que ser $\mathrm{OE}^+(4, 2) = \langle \rho \rangle\, W$. Vamos a determinar la estructura de este grupo. Para ello llamamos

$$\rho' = \rho z = (a, b')(b, a')(c, c') \in \mathrm{OE}^+(4, 2),$$

$$x' = (a, b, c)(a', b', c'), \qquad y' = (a, b, c)(c', b', a'),$$

y observamos que

$$N_1 = \langle x', y' \rangle\,, \quad \mathrm{OE}^+(4, 2) = \langle \rho \rangle\, W = \langle \rho' \rangle\, W,$$

así como que

$$x'^{\rho} = x'^{-1}, \qquad y'^{\rho} = y', \qquad x'^{\rho'} = x', \qquad y'^{\rho'} = y'^{-1}.$$

A partir de aquí es fácil ver que $S_1 = \langle x', \rho \rangle$ y $S_2 = \langle y', \rho' \rangle$ son subgrupos normales de $\mathrm{OE}^+(4, 2)$ isomorfos a Σ_3 con intersección trivial, por lo que

$$\mathrm{OE}^+(4, 2) = S_1 \times S_2 \cong \Sigma_3 \times \Sigma_3.$$

Así pues, $\mathrm{O}^+(4, 2)$ tiene dos subgrupos de índice 2 isomorfos a $\Sigma_3 \times \Sigma_3$, uno de los cuales es el grupo N generado por las reflexiones y el otro es $\mathrm{OE}^+(4, 2)$. Esto implica que el cociente $\mathrm{O}^+(4, 2)/W$ tiene dos subgrupos de orden 2, luego tiene que ser

$$\mathrm{O}^+(4, 2)/W \cong C_2 \times C_2$$

y tiene que tener un tercer subgrupo de orden 2, que se corresponde con un tercer subgrupo de índice 2 de $\mathrm{O}^+(4, 2)$. Un representante de la clase no trivial de N/W es, por ejemplo, (a, b) y un representante de la clase no trivial de $\mathrm{OE}^+(4, 2)/W$ es ρ, luego un representante de la clase no trivial del tercer subgrupo de índice 2 será

$$\tau = (a, b)\rho = (a', a, b', b)(c', c),$$

que tiene orden 4, luego el tercer subgrupo es

$$N_2 = \left\langle x, y, \tau \mid x^3 = y^3 = \tau^4 = 1,\ xy = yx,\ x^\tau = y^{-1},\ y^\tau = x \right\rangle,$$

que puede verse como un producto semidirecto $C_4[C_3 \times C_3]$ con la única acción fiel de C_4 en $C_3 \times C_3$.

Como los subgrupos de índice 2 dan cociente abeliano, resulta que

$$\Omega^+(4,2) = \mathrm{O}^+(4,2)' \leq N \cap \mathrm{O}^+(4,2) = W.$$

Pero $[z, x^{-1}] = x$, $[z, y^{-1}] = y$, $[\rho, \tau^{-1}] = z$, luego se da también la inclusión opuesta y concluimos que

$$\Omega^+(4,2) = \{x, y, z \mid x^3 = y^3 = z^2 = 1,\ xy = yx,\ x^z = x^{-1},\ y^z = y^{-1}\}$$

es un grupo de orden 18. En particular $\Omega^+(4,2) \leq N$, luego $\rho \notin \Omega^+(4,2)$ luego la excepción en el teorema 9.53 está justificada.[4] También lo está en 9.43, pues si el teorema fuera válido en el caso exceptuado sería $\Omega^+(4,2) = \mathrm{OE}^+(4,2)$, y no es el caso, así como en 9.44, pues no es difícil ver que[5]

$$\mathrm{OE}^+(4,2)' = A_3 \times A_3 \neq \Omega^+(4,2).$$

La simplicidad de $\Omega\mathrm{P}(V)$ En general no podemos aspirar a demostrar que los grupos $\Omega(V)$ son simples porque pueden contener el subgrupo normal $\{\pm 1\}$, pero vamos a ver que es el único inconveniente posible.

Definición 9.54 Si V es un espacio cuadrático y $Z = Z(\mathrm{O}(V)) = \{\pm 1\}$, definimos los *grupos ortogonales proyectivos*

$$\mathrm{OP}(V) = \mathrm{O}(V)/Z, \qquad \mathrm{OEP}(V) = \mathrm{OE}(V)Z/Z, \qquad \Omega\mathrm{P}(V) = \Omega(V)Z/Z.$$

Observemos que si la característica del cuerpo de escalares es 2, entonces $Z = 1$, con lo que estas definiciones son triviales, pero si la característica es distinta de 2 y $\dim V = n$, entonces $-1 \in \mathrm{O}(V)$ tiene determinante $(-1)^n$, luego si n es impar se cumple que $-1 \notin \mathrm{OE}(V)$, por lo que igualmente

$$\mathrm{OEP}(V) \cong \mathrm{OE}(V), \qquad \Omega\mathrm{P}(V) \cong \Omega(V).$$

En cambio, si n es par, tenemos que $-1 \in \mathrm{OE}(V)$, pero $-1 \in \Omega(V)$ si y sólo si $\theta(-1) = 1$, y se cumple que $\theta(-1) = \operatorname{disc} F$.

En efecto, es fácil ver que $V_{-1} = V$ y, puesto que $x - (-1)(x) = 2x$,

$$F_{-1}(u, v) = F(u/2, v) = \frac{1}{2}F(u, v),$$

Luego la matriz de F_f en una base coincide con la de $1/2F$, luego

$$\theta(-1) = \operatorname{disc}\frac{1}{2}F = \frac{1}{2^n}\operatorname{disc} F = \operatorname{disc} F,$$

pues, como n es par, $1/2^n$ es un cuadrado en C^*.

[4]Notemos que ρ es una transformación de Siegel ρ_{u_1,u_2} donde u_1 y u_2 son arbitrarios salvo por la exigencia de que u_2 sea no singular, luego ninguna de ellas está en $\Omega^+(4,2)$. En cambio, las transformaciones de Siegel con u_2 regular se corresponden con los productos de transposiciones mixtas, que sí que están en $\Omega^+(4,2)$.

[5]Notemos, no obstante, que si hubiéramos definido $\Omega(V) = \mathrm{OE}(V)'$, en virtud del teorema 9.44, la definición sería equivalente a la que hemos dado en todos los casos, salvo por que así sería $\Omega^+(4,2) = A_3 \times A_3$, y no hay razón por la que una opción sea preferible a la otra.

Si V es un espacio cuadrático singular de dimensión ≥ 3, el teorema 9.25 nos permite considerar a $\mathrm{OP}(V)$ y, por consiguiente a sus subgrupos $\mathrm{OEP}(V)$ y $\Omega\mathrm{P}(V)$, como grupos de permutaciones sobre el conjunto X de los puntos singulares de $P(V)$. El teorema siguiente lo tenemos prácticamente demostrado:

Teorema 9.55 *Si V es un espacio cuadrático de índice de Witt 1 y dimensión $n \geq 3$, entonces $\Omega(V)$ es doblemente transitivo sobre el conjunto X de los puntos singulares de $P(V)$.*

Demostración: Como $\mathrm{O}^+(4,2)$ tiene índice de Witt 2, el teorema 9.53 nos da que $\Omega(V)$ es el grupo generado por las transformaciones de Siegel, luego 9.48 implica que es transitivo sobre X.

Sean P, Q y P', Q' dos pares de puntos distintos en X. Entonces existe $g \in \Omega(X)$ tal que $g(P) = P'$. Sea $g(Q) = Q''$. El hecho de que el índice de Witt sea 1 implica que V no puede contener dos vectores singulares ortogonales linealmente independientes, luego P y Q no son ortogonales, luego tampoco lo son P' y Q'', y tampoco lo son P' y Q'. Si $P' = \langle u\rangle$, el teorema 9.47 nos da que existe $g' \in A_u \leq \Omega(V)$ tal que $g'(Q'') = Q'$ y, naturalmente, $g'(P') = P'$, luego $gg' \in \Omega(V)$ transforma (P, Q) en (P', Q'). ∎

Teorema 9.56 *Si V es un espacio cuadrático singular de dimensión $n \geq 3$, entonces $\Omega\mathrm{P}(V)$ es primitivo sobre el conjunto X de los puntos singulares del espacio proyectivo $P(V)$ excepto si $n = 4$ y el índice de Witt es 2.*

Demostración: Si el índice de Witt es $m = 1$, el teorema anterior nos da que $\Omega\mathrm{P}(V)$ es doblemente transitivo, luego primitivo. Por lo tanto, podemos suponer que $m \geq 2$, luego $n \geq 4$. Si $n = 4$, entonces necesariamente $m = 2$, y estamos en el caso exceptuado en el enunciado, luego podemos suponer que $n \geq 5$.

Supongamos que $B \subset X$ es un bloque con $|B| > 1$ y sea $P \in B$. Supongamos en primer lugar que existe $Q \in B$ no ortogonal a P. Entonces B contiene todos los puntos de X no ortogonales a P, pues si R es uno de ellos, el teorema 9.47 nos da $g \in \Omega(V)$ tal que $g(P) = P$ y $g(Q) = R$, luego $P \in B \cap g[B]$, luego $R \in g[B] = B$.

Veamos ahora que B contiene también los puntos ortogonales a P, con lo que será $B = X$. Supongamos que $R \in P^\perp$, $R \neq P$. Si $P = \langle u\rangle$, $R = \langle u'\rangle$, con $u \perp u'$, el teorema 8.27 nos da planos hiperbólicos ortogonales $\langle u, v\rangle$, $\langle u', v'\rangle$, y tomando $w = v + v'$ y llamando $Q = \langle w\rangle$, tenemos que $Q \in X$ no es ortogonal ni a P ni a R, luego en particular $Q \in B$. Ahora aplicamos el caso anterior: tenemos $Q \in B$ y B contiene un punto P no ortogonal a Q, luego hemos probado que contiene a todos los puntos no ortogonales a Q, en particular $R \in B$.

Esto termina la prueba en el caso en que B contiene un punto no ortogonal a P. Supongamos ahora que B contiene un punto Q ortogonal a P (distinto de P) y vamos a probar que B contiene todos los puntos de X ortogonales a P. Admitiendo esto, es fácil concluir que B contiene también todos los puntos no

ortogonales a P, pues si R es uno de ellos, entonces $H = P + R$ es un plano hiperbólico y, como $m \geq 2$, tiene que haber otro plano hiperbólico $H' \leq H^\perp$, y podemos tomar un punto singular $Q \in H' \leq H^\perp$, luego $Q \in B$ y R es ortogonal a Q. Por la parte que tenemos pendiente probar, resulta que $R \in B$.

Así pues, sólo tenemos que probar que si B contiene un punto Q ortogonal a P, entonces contiene a cualquier otro punto R ortogonal a P. A su vez, para ello basta encontrar $f \in \Omega(V)$ tal que $f(P) = P$ y $f(Q) = R$. Así $R \in f[B] = B$.

Si Q y R no son ortogonales, entonces $H = Q + R$ es un plano hiperbólico, y $P \leq H^\perp$, luego podemos formar otro plano hiperbólico tal que $P \leq H' \leq H^\perp$. Así $H \leq H'^\perp$. Como $\dim H'^\perp \geq 3$, el teorema 9.48 nos da $g \in \mathrm{O}(H'^\perp)$ que es producto de trasformaciones de Siegel y cumple $g(Q) = R$. Ahora bien, toda transformación de Siegel de $H'^\perp$ se extiende a una transformación de Siegel de V que fija a H', en particular a P, luego g se extiende a $f \in \Omega(V)$ que cumple lo requerido.

Si $Q = \langle u_1 \rangle$ es ortogonal a $R = \langle u_2 \rangle$ (y ambos son ortogonales a $P = \langle u_3 \rangle$), por 8.27 podemos formar planos hiperbólicos ortogonales

$$\langle u_1, v_1 \rangle \perp \langle u_2, v_2 \rangle \perp \langle u_3, v_3 \rangle$$

y, como antes, podemos tomar $g \in \mathrm{O}(\langle u_3, v_3 \rangle^\perp)$ que sea producto de transformaciones de Siegel y que cumpla $g(Q) = R$, la cual se extiende a $f \in \Omega(V)$ que fija los vectores de $\langle u_3, v_3 \rangle$ y cumple lo requerido. ∎

Teorema 9.57 *Si V es un espacio cuadrático singular de dimensión $n \geq 3$, entonces $\Omega(V)' = \Omega(V)$ salvo en los casos $\Omega(3,3)$, $\Omega^+(4,2)$ y $\Omega^+(4,3)$.*

Demostración: Sea $\rho_{u,y}$ una transformación de Siegel y vamos a probar que $\rho_{u,y} \in \Omega(V)'$. El teorema 9.53 nos da entonces la conclusión.

Si y es singular, como $u \perp v$, el teorema 8.27 nos da planos hiperbólicos $\langle u, v \rangle \perp \langle y, y' \rangle$, con lo que $H = \langle u, v \rangle \leq \langle y \rangle^\perp$. Si y es no singular, entonces $\langle y \rangle^\perp$ es un espacio cuadrático e igualmente podemos tomar un plano hiperbólico $H = \langle u, v \rangle \leq \langle y \rangle^\perp$.

Para cada $a \in C^*$ podemos considerar la transformación $g \in \mathrm{O}(H)$ dada por $g(u) = au$, $g(v) = a^{-1}v$ (véase la prueba del teorema 8.45), y podemos extenderla a $g \in \mathrm{O}(V)$ de modo que $g|_{H^\perp} = 1$. El teorema 9.42 nos da que $g^2 \in \Omega(V)$. Si $|C^*| > 3$, podemos elegir a de modo que $a^2 \neq 1$, y entonces

$$[g^2, \rho_{u,(1-a^2)^{-1}y}] = g^{-2}\rho_{u,-(1-a^2)^{-1}y}g^2\,\rho_{u,(1-a^2)^{-1}y} =$$

$$\rho_{a^2u,-(1-a^2)^{-1}y}\,\rho_{u,(1-a^2)^{-1}y} = \rho_{u,-a^2(1-a^2)^{-1}y}\,\rho_{u,(1-a^2)^{-1}y} = \rho_{u,y},$$

luego $\rho_{u,y} \in \Omega(V)'$. Por lo tanto, a partir de aquí podemos suponer que $|C| \leq 3$. Por el teorema 9.51 podemos suponer que y es no singular.

Si C es el cuerpo de 2 elementos, entonces $H^\perp$ no puede ser un plano hiperbólico, pues entonces estaríamos en el caso de $\Omega^+(4,2)$. El teorema 9.50 nos da

que $H^\perp$ está generado por sus vectores no singulares. Si todos ellos estuvieran en $\langle y\rangle^\perp$, tendríamos que $H^\perp \le \langle y\rangle^\perp$, luego $y \in H$, lo cual no es cierto, por lo que podemos tomar $x \in H^\perp \setminus \langle y\rangle^\perp$ no singular. Así $W = \langle x, y\rangle$ es un subespacio no degenerado no singular, pues

$$Q(ax + by) = a^2 + ab + b^2$$

y a, b sólo pueden tomar los valores $0, 1$. Definimos una transformación $g \in \mathrm{O}(V)$ mediante $g(x) = x + y$, $g(y) = x$ y $g|_{W^\perp} = 1$. Entonces $g^3 = 1$, luego 9.42 nos da de nuevo que $g = (g^{-1})^2 \in \Omega(V)$ y

$$[g, \rho_{u,x}] = g^{-1}\rho_{u,x}g\rho_{u,x} = \rho_{u,x+y}\rho_{u,x} = \rho_{u,y} \in \Omega(V)'.$$

Supongamos finalmente que C es el cuerpo de 3 elementos, en cuyo caso las excepciones del enunciado nos dan que $n \ge 4$ y que si $n = 4$ el índice de Witt es $m = 1$, lo que se traduce en que $H^\perp$ es un plano no singular.

Vamos a probar que existe $x \in H^\perp \cap \langle y\rangle^\perp$ tal que $Q(x) = Q(y)$. Si $n = 4$, entonces $H^\perp$ admite una base ortogonal x, y, donde necesariamente se cumple $Q(x) = Q(y)$, porque en caso contrario sería $Q(x) = -Q(y)$, y entonces tendríamos que $Q(x + y) = 0$ en contra de que $H^\perp$ es no singular.

Si $n > 4$ tenemos una base ortonormal $H^\perp = \langle y, x_1, x_2, \ldots, x_r\rangle$, con $r \ge 2$. O bien $Q(y) = Q(x_1)$, o bien $Q(y) = Q(x_2)$, o bien $Q(x_1) = Q(x_2) = -Q(y)$, en cuyo caso $x = x_1 + x_2$ cumple $Q(x) = Q(y)$.

Ahora tomamos $g \in \mathrm{O}(V)$ dada por $g(x) = -y$, $g(y) = x$ y que fije a todos los vectores de $\langle x, y\rangle^\perp$. Entonces $g^2 \in \Omega(V)$ y

$$[g^2, \rho_{u,-y}] = g^{-2}\rho_{u,y}g^2\rho_{u,-y} = \rho_{u,-y}\rho_{u,-y} = \rho_{u,y} \in \Omega(V)'. \qquad \blacksquare$$

Ahora ya es inmediato el teorema que pretendíamos demostrar:

Teorema 9.58 *Si V es un espacio cuadrático singular de dimensión $n \ge 3$, el grupo $\Omega\mathrm{P}(V)$ es simple, salvo en el caso de $\Omega\mathrm{P}(3, 3)$ y cuando $n = 4$ y el índice de Witt es $m = 2$.*

Demostración: Sólo tenemos que aplicar el teorema de Iwasawa: con las excepciones recogidas en el enunciado, hemos probado (teormema 9.25) que $\Omega\mathrm{P}(V)$ es un grupo de permutaciones sobre el conjunto X de los puntos singulares de $P(V)$, que es primitivo (teorema 9.56), que coincide con su derivado (teorema 9.57) y, si $P = \langle u\rangle \in X$, el estabilizador $\Omega\mathrm{P}(V)_P$ contiene el subgrupo normal abeliano $A_u Z/Z$ cuya envoltura normal en $\Omega\mathrm{P}(V)$ contiene todas las transformaciones de Siegel (por 9.48), luego es todo $\Omega\mathrm{P}(V)$. El teorema de Iwasawa implica entonces que $\Omega\mathrm{P}(V)$ es simple. $\blacksquare$

El teorema 9.39 nos da el isomorfismo $\Omega\mathrm{P}(3, q) \cong \mathrm{LEP}(2, q)$, lo que en particular justifica la excepción $\Omega\mathrm{P}(3, 3) \cong \mathrm{LEP}(2, 3) \cong A_4$ en el teorema anterior. El teorema 9.56 nos ha introducido una familia infinita de excepciones más allá del grupo $\mathrm{O}^+(4, 2)$, que ya sabíamos que no es simple. El teorema siguiente muestra que todas ellas están justificadas:

Teorema 9.59 *Si V es un espacio cuadrático de dimensión $n = 4$ e índice de Witt $m = 2$ sobre un cuerpo C con $|C| > 3$, entonces*

$$\Omega\mathrm{P}(V) \cong \mathrm{LEP}(2, C) \times \mathrm{LEP}(2, C).$$

DEMOSTRACIÓN: Llamemos V al espacio vectorial de las matrices 2×2 con coeficientes en C, que ciertamente es un espacio vectorial de dimensión 4, y consideremos la forma cuadrática $Q : V \longrightarrow C$ dada por el determinante:

$$Q\begin{pmatrix} x & z \\ w & y \end{pmatrix} = xy - zw.$$

Es claro que se trata ciertamente de una forma cuadrática en V respecto a la cual $V = H_1 \perp H_2$ se descompone en suma ortogonal de dos planos hiperbólicos, a saber, los formados por las matrices de la forma

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \qquad \begin{pmatrix} 0 & z \\ w & 0 \end{pmatrix},$$

respectivamente. Por lo tanto, V tiene índice de Witt 2, y cualquier otro espacio cuadrático en las condiciones del enunciado es isométrico a V, luego basta probar el teorema para V. Observemos que la forma bilineal asociada a Q es

$$F\left(\begin{pmatrix} x & z \\ w & y \end{pmatrix}, \begin{pmatrix} x' & z' \\ w' & y' \end{pmatrix}\right) = xy' + x'y - (zw' + z'w).$$

Consideremos la aplicación

$$\rho : \mathrm{LG}(2, C) \times \mathrm{LG}(2, C) \longrightarrow \mathrm{LG}(V)$$

dada por

$$\rho(A, B)(X) = A^{-1}XB.$$

Claramente es un homomorfismo de grupos, y $\rho(A, B) \in \mathrm{O}(V)$ si y sólo si, para todo $X \in V$ se cumple que $|A|^{-1}|X||B| = |X|$, lo que equivale a que $|A| = |B|$. Así pues, llamamos

$$G = \{(A, B) \in \mathrm{LG}(2, C) \times \mathrm{LG}(2, C) \mid |A| = |B|\},$$

de modo que tenemos un homomorfismo $\rho : G \longrightarrow \mathrm{O}(V)$. Igualando coeficientes en la relación $A^{-1}XB = X$ o, equivalentemente, $AX = XB$, se concluye sin dificultad que el núcleo es

$$N = \{(\lambda I, \lambda I) \in \mathrm{LG}(2, C) \times \mathrm{LG}(2, C) \mid \lambda \in C^*\}.$$

Así pues, si llamamos $\tilde{G} = \rho[G] \leq \mathrm{O}(V)$, tenemos que $\tilde{G} \cong G/N$. Otra transformación ortogonal $T : V \longrightarrow V$ es obviamente la dada por $T(X) = X^t$.

Igualando coeficientes en la relación $\rho(A^{-1}, B)(X) = X^t$ se ve que es imposible, de modo que $T \notin \tilde{G}$. Por otro lado, si

$$U = \begin{pmatrix} p & r \\ s & q \end{pmatrix}$$

es una matriz no singular, se comprueba que la reflexión R_U puede expresarse como $R_U = \rho(A, B)T$, donde

$$A = \begin{pmatrix} -r & p \\ -q & s \end{pmatrix}, \qquad B = \begin{pmatrix} -r & -q \\ p & s \end{pmatrix}.$$

El teorema 9.36 nos da que $\tilde{G}$ y T generan $\mathrm{O(V)}$. Más aún, tomando

$$U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

obtenemos $A = B = I$, luego $T = R_U$ es una reflexión. También es fácil ver que

$$\rho(A, B)^T = \rho(B^{-1t}, A^{-1t}),$$

lo que implica que $\tilde{G} \trianglelefteq \mathrm{O}(V)$, así como que $\tilde{G}$ contiene a todos los productos de dos reflexiones, pues

$$R_U R_{U'} = \rho(A, B)T\rho(A', B')T = \rho(A, B)\rho(A', B')^T \in \tilde{G}.$$

Por lo tanto, puesto que los productos de reflexiones generan $\mathrm{OE}(V)$, tenemos que $\mathrm{OE}(V) \leq \tilde{G} < \mathrm{O}(V)$ y, como el grupo ortogonal especial tiene índice 2, tiene que ser $\tilde{G} = \mathrm{OE}(V)$. Equivalentemente, tenemos un isomorfismo

$$G/N \cong \mathrm{OE}(V).$$

Ahora llamamos

$$M(\alpha) = \left(\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \right),$$

de modo que $K = \{M(\alpha) \mid \alpha \in C^*\}$ forma un subgrupo de G isomorfo a C^*. Si $(A, B) \in G$ cumple $|A| = |B| = \alpha$, entonces

$$(A, B) = (A, B)M(\alpha^{-1})M(\alpha),$$

donde $(A, B)M(\alpha^{-1}) \in \mathrm{LE}(2, C) \times \mathrm{LE}(2, C)$, con lo que

$$G = (\mathrm{LE}(2, C) \times \mathrm{LE}(2, C))K.$$

El producto es normal en G, porque lo es en $\mathrm{LG}(2, C) \times \mathrm{LG}(2, C)$ y los dos factores tienen intersección trivial. Ahora,

$$K^2 = \{M(\alpha^2) \mid \alpha \in C^*\}$$

es un subgrupo isomorfo a C^{*2} y

$$G_0 = (\mathrm{LE}(2, C) \times \mathrm{LE}(2, C))K^2$$

es un subgrupo de G tal que $G/G_0 \cong K/K^2$ es abeliano, luego $G' \leq G_0$. Además

$$G_0 = (\mathrm{LE}(2, C) \times \mathrm{LE}(2, C))N,$$

pues

$$M(\alpha^2) = (M(\alpha^2)(\alpha^{-1}I, \alpha^{-1}I))(\alpha I, \alpha I) \in (\mathrm{LE}(2,C) \times \mathrm{LE}(2,C))N,$$

luego $G_0 \leq (\mathrm{LE}(2,C) \times \mathrm{LE}(2,C))N$. Recíprocamente,

$$(\lambda I, \lambda I) = \left(\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}\right) M(\lambda^2) \in G_0.$$

Por lo tanto, $(G/N)' \leq G_0/N$, luego, teniendo en cuenta el teorema 7.16,

$$\Omega(V) \leq \rho[G_0/N] = \rho[\mathrm{LE}(2,C) \times \mathrm{LE}(2,C)] = \rho[\mathrm{LE}(2,C)' \times \mathrm{LE}(2,C)'] \leq \Omega(V).$$

Concluimos que ρ induce un isomorfismo $G_0/N \cong \Omega(V)$. Más aún,

$$\Omega(V) \cong G_0/N \cong (\mathrm{LE}(2,C) \times \mathrm{LE}(2,C))/Z_0,$$

donde $Z_0 = (\mathrm{LE}(2,C) \times \mathrm{LE}(2,C)) \cap N = \{(I,I),(-I,-I)\}$. Finalmente, $Z(\Omega(V)) = \{\pm 1\}$, que es un subgrupo de orden 1 o 2 según si C tiene o no característica 2. Si llamamos

$$Z = \{(I,I),(I,-I),(-I,I),(-I,-I)\},$$

tenemos que $|Z/Z_0| = |Z(\Omega(V))|$ y Z/Z_0 está claramente contenido en el centro de $(\mathrm{LE}(2,C) \times \mathrm{LE}(2,C))/Z_0$, luego tiene que ser exactamente dicho centro, y así

$$\Omega\mathrm{P}(V) = \Omega(V)/Z(\Omega(V)) \cong (\mathrm{LE}(2,C) \times \mathrm{LE}(2,C))/Z =$$

$$(\mathrm{LE}(2,C) \times \mathrm{LE}(2,C))/(\{\pm I\} \times \{\pm I\}) \cong$$

$$(\mathrm{LE}(2,C)/\{\pm I\}) \times (\mathrm{LE}(2,C)/\{\pm I\}) = \mathrm{LEP}(2,C) \times \mathrm{LEP}(2,C).$$

∎

Los órdenes de los grupos $\Omega\mathrm{P}^\epsilon(n,q)$ Hemos probado la simplicidad de los grupos finitos $\Omega\mathrm{P}^\epsilon(n,q)$ excepto los casos $\Omega\mathrm{P}(3,3)$ y $\Omega\mathrm{P}^+(4,q)$, pero no hemos calculado sus órdenes.

El teorema 8.48 nos da los órdenes de los grupos $\mathrm{O}^\epsilon(n,q)$, y $\mathrm{OE}^\epsilon(n,q)$ es un subgrupo de índice 2, luego:

$$\begin{aligned} |\mathrm{OE}(2m+1,q)| &= q^{m^2} \prod_{i=1}^{m} (q^{2i}-1), \quad \text{para } q \text{ impar}, \\ |\mathrm{OE}^\epsilon(2m,q)| &= q^{m(m-1)}(q^m - \epsilon) \prod_{i=1}^{m-1} (q^{2i}-1). \end{aligned}$$

Por otra parte, el teorema 9.43 implica que si q es par, como $C^* = C^{*2}$, se cumple que $\Omega^\epsilon(n,q) = \mathrm{OE}^\epsilon(n,q)$ salvo para $\Omega^+(4,2)$, y si q es impar, entonces

$\Omega^\epsilon(n,q)$ tiene índice 2 en $\mathrm{OE}^\epsilon(n,q)$. Por lo tanto (salvo para $\Omega^+(4,2)$, que tiene orden 18):

$$\begin{aligned} |\Omega(2m+1,q)| &= \frac{1}{2}q^{m^2}\prod_{i=1}^{m}(q^{2i}-1), \quad \text{para } q \text{ impar},\\ |\Omega^\epsilon(2m,q)| &= \frac{q^{m(m-1)}(q^m-\epsilon)}{(2,q+1)}\prod_{i=1}^{m-1}(q^{2i}-1). \end{aligned}$$

Finalmente, tras la definición 9.54 hemos visto que $\Omega\mathrm{P}^\epsilon(n,q) = \Omega^\epsilon(n,q)$ siempre que q es par o si n y q son ambos impares. En el caso en que n es par y q es impar tenemos que $-1 \in \Omega^\epsilon(2m,q)$ si y sólo si el discriminante de la forma bilineal es trivial. En tal caso, si V es un espacio cuadrático de dimensión $n = 2m$ sobre C, tenemos que

$$V = V_1 \perp \cdots \perp V_m,$$

donde cada V_i es un plano hiperbólico salvo a lo sumo V_m, que lo será si $\epsilon = +1$ y será un plano no singular si $\epsilon = -1$. Si formamos una base de V uniendo bases de los planos V_i, el determinante de la forma cuadrática de F es el producto de los determinantes de sus restricciones a cada plano.

El determinante de la matriz de la forma bilineal de un plano hiperbólico respecto de un par hiperbólico es -1, que es un cuadrado en C^* si y sólo si C^* contiene elementos de orden 4, si y sólo si $q \equiv 1 \pmod 4$.

Por lo tanto, si $\epsilon = +1$, el espacio V admite una base en la que el determinante de la forma cuadrática es $(-1)^m$, que es un cuadrado en C^* si y sólo si $q^m \equiv 1 \pmod 4$.

En efecto, si $q \equiv 1 \pmod 4$, entonces 1 y -1 son cuadrados en C^*, luego $(-1)^m$ es siempre un cuadrado en C^* y $q^m \equiv 1 \pmod 4$ se cumple para todo m. En cambio, si $q \equiv -1 \pmod 4$, entonces ambas condiciones se cumplen si y sólo si m es par.

En la prueba del teorema 8.32 hemos visto que la forma cuadrática de un plano no singular en la base adecuada es de la forma $Q(x+y\omega) = x^2 - xy + ay^2$ (en la prueba del teorema 8.39 se razona que podemos tomar $\alpha = 1$). De aquí se sigue que la matriz de la forma bilineal en dicha base es

$$\begin{pmatrix} 2 & -1 \\ -1 & 2a \end{pmatrix}$$

cuyo determinante es $4a-1$, pero el polinomio x^2+x+a es irreducible en $C[x]$, lo que exige que $d = 1-4a \notin C^{*2}$, luego el determinante $-d$ es un cuadrado si y sólo si no lo es -1, es decir, sí y sólo si $q \equiv -1 \pmod 4$.

Por lo tanto, si $\epsilon = -1$, el determinante de la matriz de la forma cuadrática será un cuadrado si y sólo si se cumple $q \equiv -1 \pmod q$ y $q^{m-1} \equiv 1 \pmod 4$ o bien $q \equiv 1 \pmod 4$ y $q^{m-1} \equiv -1 \pmod 4$. Ambos casos equivalen a que $q^m \equiv -1 \pmod 4$.

En conclusión, para q impar, $-1 \in \Omega^\epsilon(2m,q)$ si y sólo si $q^m \equiv \epsilon \pmod 4$, luego el orden del grupo proyectivo $\Omega\mathrm{P}^\epsilon(2m,q)$ es la mitad que el de $\Omega^\epsilon(2m,q)$

si y sólo si $(q^m - \epsilon, 4) = 4$. Esto nos da las fórmulas

$$\begin{aligned} |\Omega\mathrm{P}(2m+1,q)| &= \frac{1}{2}q^{m^2}\prod_{i=1}^{m}(q^{2i}-1), \quad \text{para } q \text{ impar},\\ |\Omega\mathrm{P}^\epsilon(2m,q)| &= \frac{q^{m(m-1)}(q^m-\epsilon)}{(q^m-\epsilon,4)}\prod_{i=1}^{m-1}(q^{2i}-1), \end{aligned}$$

siempre con la excepción de $\Omega\mathrm{P}^+(4,2)$, que tiene orden 18 y no 36.

En dimensión 3, el teorema 9.39 implica que $\Omega\mathrm{P}(3,q) \cong \mathrm{LEP}(2,q)$, mientras que en dimensión 4, hemos visto que los grupos $\Omega\mathrm{P}^+(4,q)$ no son simples y, por otra parte:

Teorema 9.60 $\Omega\mathrm{P}^-(4,q) \cong \mathrm{LEP}(2,q^2)$.

Demostración: Sea C el cuerpo de q elementos y K el cuerpo de q^2 elementos, de modo que C es el cuerpo fijado en K por la conjugación $\bar{\alpha} = \alpha^q$. Según hemos visto en la prueba del teorema 8.39, $K = C(\omega)$, donde el polinomio mínimo de ω es de la forma $x^2 + x + a$.

Sea V el C-espacio vectorial formado por las matrices $X \in \mathrm{Mat}_2(K)$ tales que $\bar{X}^t = X$. Explícitamente, son las matrices de la forma

$$X = \begin{pmatrix} x & \xi \\ \bar{\xi} & y \end{pmatrix},$$

donde $x, y \in C$, $\xi \in K$. Si $K = C(\omega)$, teniendo en cuenta que podemos expresar $\xi = z + w\,\omega$, con $z, w \in C$, es claro que $\dim V = 4$. Además, podemos definir $Q : V \longrightarrow C$ mediante

$$Q(X) = |X| = xy - \xi\bar{\xi},$$

que es una forma cuadrática. Más precisamente, $V = H \perp W$, donde H es el subespacio vectorial formado por las matrices diagonales (que cumplen $\xi = 0$), y es un plano hiperbólico, y W es el subespacio formado por las matrices que cumplen $x = y = 0$, que es isomorfo a K y la restricción de Q a W se corresponde con la norma $\mathrm{N} : K \longrightarrow C$ cambiada de signo, por lo que W es no singular y $\mathrm{O}(V) = \mathrm{O}^-(4,q)$.

Ahora definimos $\rho : \mathrm{LE}(2,K) \longrightarrow \Omega(V)$ mediante

$$\rho(P)(X) = \bar{P}^t X P.$$

Notemos que, en efecto, $\rho(P) \in \mathrm{LG}(V)$ y ρ es un homomorfismo de grupos. Además $|\rho(P)(X)| = |X|$, por lo que, de hecho, $\rho(P) \in \mathrm{O}(V)$, pero 7.16 nos da que $\mathrm{LE}(2,K) = \mathrm{LE}(2,K)'$, de donde la imagen de ρ tiene que estar en $\mathrm{O}(V)' = \Omega(V)$. A su vez, ρ induce un homomorfismo

$$\bar{\rho} : \mathrm{LE}(2,K) \longrightarrow \Omega\mathrm{P}(V).$$

Vamos a calcular su núcleo, que estará formado por las matrices $P \in \mathrm{LE}(2,K)$ que cumplen $\rho(P)(X) = \epsilon X$, para todo $X \in V$, donde $\epsilon = 1$ si $-1 \notin \Omega(P)$ o bien $\epsilon = \pm 1$ si $-1 \in \Omega(P)$. Para ello expresamos

$$P = \begin{pmatrix} \alpha & \gamma \\ \delta & \beta \end{pmatrix}$$

y desarrollamos la igualdad $\bar{P}^t X P = P$:

$$\begin{pmatrix} \alpha\bar{\alpha}x + \delta\bar{\delta}y + \delta\bar{\alpha}\xi + \alpha\bar{\delta}\bar{\xi} & \bar{\alpha}\gamma x + \bar{\delta}\beta y + \bar{\alpha}\beta\xi + \bar{\delta}\gamma\bar{\xi} \\ \alpha\bar{\gamma}x + \delta\bar{\beta}y + \delta\bar{\gamma}\xi + \alpha\bar{\beta}\bar{\xi} & \gamma\bar{\gamma}x + \beta\bar{\beta}y + \beta\bar{\gamma}\xi + \gamma\bar{\beta}\bar{\xi} \end{pmatrix} = \begin{pmatrix} \epsilon x & \epsilon\xi \\ \epsilon\bar{\xi} & \epsilon y \end{pmatrix}.$$

Al igualar las coordenadas $(1,1)$ obtenemos $\alpha\bar{\alpha} = \epsilon$, $\delta\bar{\delta} = 0$, de donde $\delta = 0$. Igualmente, las coordenadas $(2,2)$ nos dan que $\beta\bar{\beta} = \epsilon$, $\gamma\bar{\gamma} = 0$, luego $\gamma = 0$, y las otras dos coordenadas nos dan además que $\bar{\alpha}\beta = \epsilon$. Además, como $|P| = 1$, tiene que ser $\alpha\beta = 1$. Como $\alpha\bar{\alpha} = \beta\bar{\alpha}$, tiene que ser $\alpha = \beta$ y entonces $\alpha^2 = 1$, luego $\alpha = \pm 1$, pero entonces $\epsilon = 1$, es decir, que -1 no está en la imagen de ρ aunque esté en $\Omega(V)$. Así pues, el núcleo de $\bar{\rho}$ está formado por las matrices $\pm I$, con lo que tenemos un monomorfismo

$$\mathrm{LEP}(2,K) \longrightarrow \Omega\mathrm{P}(V)$$

y, como ambos grupos tienen el mismo orden, tiene que ser un isomorfismo. ∎

En dimensión 5 y 6 tampoco obtenemos grupos nuevos:

Teorema 9.61 *Se cumple*

$$\Omega\mathrm{P}(5,q) \cong \mathrm{SpP}(4,q), \quad \Omega\mathrm{P}^+(6,q) \cong \mathrm{LEP}(4,q), \quad \Omega\mathrm{P}^-(6,q) \cong \mathrm{UEP}(4,q^2).$$

Demostración: Sea V el espacio de las matrices de la forma

$$X = \begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{pmatrix}$$

con coeficientes en el cuerpo C de q elementos.[6] Claramente se trata de un espacio vectorial de dimensión 6. Una comprobación rutinaria muestra que

$$|X| = (af - be + cd)^2.$$

Es inmediato comprobar que la aplicación $Q : V \longrightarrow C$ dada por

$$Q(X) = af - be + cd$$

[6]Si la característica de C es distinta de 2 el espacio V es el espacio de las matrices antisimétricas, pero si la característica es 2 tenemos que exigir explícitamente que los coeficientes de la diagonal sean nulos.

es una forma cuadrática en V, respecto a la cual V se descompone en suma ortogonal de tres planos hiperbólicos. Concretamente,

$$V = H_1 \perp H_2 \perp H_3,$$

donde H_i está formado, respectivamente, por las matrices

$$M_1(a,f) = \begin{pmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & f \\ 0 & 0 & -f & 0 \end{pmatrix}, \quad M_2(b,e) = \begin{pmatrix} 0 & 0 & b & 0 \\ 0 & 0 & 0 & e \\ -b & 0 & 0 & 0 \\ 0 & -e & 0 & 0 \end{pmatrix},$$

$$M_3(c,d) = \begin{pmatrix} 0 & 0 & 0 & c \\ 0 & 0 & d & 0 \\ 0 & -d & 0 & 0 \\ -c & 0 & 0 & 0 \end{pmatrix}.$$

Por consiguiente, $\mathrm{O}(V) = \mathrm{O}^+(6,q)$. Consideramos ahora la aplicación

$$\rho : \mathrm{LG}(4,q) \longrightarrow \mathrm{LG}(V)$$

dada por

$$\rho(P)(X) = P^t X P.$$

Es fácil comprobar que, ciertamente, $P^t X P \in V$, y es claro que ρ es un homomorfismo de grupos. Más laborioso es comprobar que, si $\alpha \neq 0$, entonces $\rho(P)(X) = \alpha X$ para todo $X \in V$ si y sólo si $P = \beta I$, con $\beta^2 = \alpha$.

Para probarlo pongamos que $P = (a_{ij})$ y apliquemos la relación

$$\rho(P)(X) = \alpha X$$

a la matriz X que tiene todas sus coordenadas nulas salvo $a = 1$. Al igualar los coeficientes resulta:

$$a_{11}a_{32} = a_{12}a_{31}, \quad a_{11}a_{42} = a_{12}a_{41}, \quad a_{21}a_{32} = a_{22}a_{31},$$

$$a_{21}a_{42} = a_{22}a_{41}, \quad a_{31}a_{42} = a_{32}a_{41}, \quad a_{11}a_{22} - a_{12}a_{21} = \alpha.$$

Si fuera $a_{41} \neq 0$, podríamos llamar $\lambda = a_{42}/a_{41}$ y tendríamos que

$$a_{12} = \lambda a_{11}, \quad a_{22} = \lambda a_{21}, \quad a_{32} = \lambda a_{31}, \quad a_{42} = \lambda a_{41},$$

con lo que P tendría dos columnas linealmente dependientes y no sería regular. Por lo tanto, tiene que ser $a_{41} = 0$, e igualmente $a_{42} = a_{31} = a_{32} = 0$.

Teniendo esto en cuenta, consideramos ahora la matriz X que tiene sus componentes nulas salvo $d = 1$ y ahora obtenemos las relaciones

$$a_{22}a_{33} = \alpha \neq 0, \quad a_{12}a_{33} = 0, \quad a_{22}a_{43} = 0, \quad a_{13}a_{22} - a_{12}a_{23} = 0,$$

de donde concluimos que $a_{12} = a_{43} = a_{13} = 0$, y además la relación del caso anterior $a_{11}a_{22} - a_{12}a_{21} = \alpha$ se reduce ahora a $a_{11}a_{22} = \alpha$.

Ahora consideramos la matriz X con componentes nulas salvo $f = 1$, y obtenemos

$$a_{33}a_{44} = \alpha \neq 0, \quad a_{14}a_{33} = 0, \quad a_{23}a_{44} = 0, \quad a_{23}a_{34} - a_{24}a_{33} = 0,$$

de donde $a_{14} = a_{23} = a_{24} = 0$.

Razonando igualmente con las tres matrices restantes de la base canónica de V concluimos que P es una matriz diagonal, así como que

$$a_{11}a_{22} = a_{22}a_{33} = a_{33}a_{44} = a_{11}a_{44} = a_{11}a_{33} = a_{22}a_{33} = \alpha \neq 0,$$

de donde se sigue que $a_{11} = a_{22} = a_{33} = a_{44} = \beta$, con $\beta^2 = \alpha$.

En particular, tomando $\alpha = 1$ concluimos que el núcleo de ρ está formado por las matrices $\pm I$.

Observemos ahora que

$$Q(P^tXP)^2 = |P^tXP| = |P|^2|X| = |P|^2Q(X)^2,$$

luego $Q(P^tXP) = \pm|P|Q(X)$, pero el signo correcto es el positivo, pues esta relación puede verse como una igualdad de polinomios en 42 indeterminadas, que en particular se cumplirá si hacemos $P = I$, en cuyo caso se reduce a $Q(X) = \pm Q(X)$, lo que muestra que el signo correcto es el positivo.

Tenemos, pues, que $Q(\rho(P)(X)) = |P|Q(X)$, luego $\rho(P) \in \mathrm{O}(V)$ si y sólo si $P \in \mathrm{LE}(6, q)$. Por lo tanto, ρ se restringe a un homomorfismo

$$\rho : \mathrm{LE}(4, q) \longrightarrow \mathrm{O}^+(6, q).$$

Más aún, puesto que $\mathrm{LE}(4, q) = \mathrm{LE}(4, q)'$ (teorema 7.16), tenemos en realidad un homomorfismo

$$\rho : \mathrm{LE}(4, q) \longrightarrow \Omega^+(6, q).$$

Hemos visto que $-1 \in \Omega^+(6, q)$ si y sólo si -1 es un cuadrado en C, en cuyo caso hemos probado que $\rho^{-1}[\{\pm 1\}]$ está formado por las matrices αI, con $\alpha^2 = \pm 1$ o, equivalentemente, $\alpha^4 = 1$. En caso contrario, tenemos igualmente que $\rho^{-1}[\{1\}]$ está formado por las matrices αI con $\alpha^2 = 1$, que son las mismas que cumplen $\alpha^4 = 1$. En ambos casos se trata de todas las matrices escalares de $\mathrm{LE}(4, q)$, luego tenemos un monomorfismo

$$\bar{\rho} : \mathrm{LEP}(4, q) \longrightarrow \Omega\mathrm{P}^+(6, q).$$

Como ambos grupos tienen el mismo orden, se trata de un isomorfismo.

Supongamos ahora que q es impar y fijemos una matriz $A \in V$ no singular, que determina un punto $\langle A\rangle \in P(V)$. El estabilizador $\Omega\mathrm{P}^+(6, q)_{\langle A\rangle}$ se corresponde con las clases $[P] \in \mathrm{LEP}(4, q)$ que cumplen $PAP^t = A$ o bien (sólo en el caso en que $-1 = \alpha^2$ es un cuadrado en C) $PAP^t = -A$, pero en este segundo caso $[P] = [\alpha P]$ y, cambiando P por αP se cumple que $PAP^t = A$.

Esto significa que $\Omega\mathrm{P}^+(6,q)_{\langle A\rangle}$ es la imagen por ρ del subgrupo de $\mathrm{LE}(4,q)$ formado por las matrices P que cumplen $PAP^t = A$. Ahora bien, la forma bilineal $F : C^4 \times C^4 \longrightarrow C$ dada por

$$F(x,y) = xAy^t$$

es alternada, luego determina en C^4 una estructura de espacio simpléctico cuyo grupo de isometrías $\mathrm{Sp}(4,q)$ está formado precisamente por los automorfismos cuya matriz P en la base canónica cumple la relación $PAP^t = A$. Así pues, ρ se restringe a un epimorfismo

$$\rho : \mathrm{Sp}(4,q) \longrightarrow \Omega\mathrm{P}^+(6,q)_{\langle A\rangle}$$

cuyo núcleo es $\{\pm 1\}$ (el núcleo de ρ está formado por las homotecias lineales de $\mathrm{LE}(4,q)$, luego su restricción a $\mathrm{Sp}(4,q)$ está formado por las homotecias lineales que están en este subgrupo, que son ± 1). Por lo tanto, ρ induce un isomorfismo

$$\bar{\rho} : \mathrm{SpP}(4,q) \longrightarrow \Omega\mathrm{P}^+(6,q)_{\langle A\rangle}.$$

Por otro lado, el estabilizador de A en $\mathrm{O}^+(6,q)$ es también el estabilizador de $\langle A\rangle^\perp$. Además, tenemos un monomorfismo

$$\mathrm{O}(5,q) \longrightarrow \mathrm{O}^+(6,q)_{\langle A\rangle}$$

que a cada $f \in \mathrm{O}(5,q) = \mathrm{O}(\langle A\rangle^\perp)$ le asigna la extensión determinada por $f(A) = A$. Éste se restringe a un monomorfismo

$$\Omega\mathrm{P}(5,q) = \Omega(5,q) \longrightarrow \Omega^+(6,q)_{\langle A\rangle},$$

que sigue siendo un monomorfismo si lo componemos con la proyección natural

$$\Omega\mathrm{P}(5,q) \longrightarrow \Omega\mathrm{P}^+(6,q)_{\langle A\rangle} \cong \mathrm{SpP}(4,q),$$

pues, en el supuesto de que $-1 \in \Omega^+(6,q)$, la extensión de una transformación $f \in \Omega(5,q)$ no es nunca $\rho(f) = -1$. Como ambos grupos tienen el mismo orden, tenemos un isomorfismo $\Omega\mathrm{P}(5,q) \cong \mathrm{SpP}(4,q)$.

Para probar el tercer isomorfismo consideramos el isomorfismo

$$\bar{\rho} : \mathrm{LEP}(4,q^2) \longrightarrow \Omega\mathrm{P}(6,q^2)$$

que hemos construido, de modo que ahora C es el cuerpo de q^2 elementos, y llamamos R al cuerpo de q elementos, fijado por la conjugación $\bar{\alpha} = \alpha^q$. Sabemos (véase la prueba del teorema 8.39) que podemos expresar $C = R(\omega)$, donde $\omega + \bar{\omega} = -1$.

El C-espacio vectorial V puede verse como un R-espacio vectorial de dimensión 12, dentro del cual podemos considerar el subespacio W formado por las matrices

$$X = \begin{pmatrix} 0 & \alpha & \beta & \gamma \\ -\alpha & 0 & \bar{\gamma} & -\bar{\beta} \\ -\beta & -\bar{\gamma} & 0 & \bar{\alpha} \\ -\gamma & \bar{\beta} & -\bar{\alpha} & 0 \end{pmatrix},$$

de modo que $\dim W = 6$.

Más explícitamente, si llamamos

$$M_1(\alpha) = M_1(\alpha, \bar{\alpha}), \quad M_2(\beta) = M_2(\beta, -\bar{\beta}), \quad M_3(\gamma) = M_3(\gamma, \bar{\gamma}),$$

una base de W está formada por las matrices

$$M_1(1), \quad M_1(\omega), \quad M_2(1), \quad M_2(\omega), \quad M_3(1), \quad M_3(\omega).$$

Observemos que estas 6 matrices son linealmente independientes tanto en W como en V, es decir, tanto si consideramos combinaciones lineales con coeficientes en R o en C. La razón es que la matriz de cambio de base respecto de la base canónica de V es

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ \omega & \bar{\omega} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \omega & -\bar{\omega} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & \omega & \bar{\omega} \end{pmatrix},$$

que tiene determinante no nulo. En otras palabras, las combinaciones lineales de estas seis matrices con coeficientes en R generan W, mientras que las combinaciones lineales con coeficientes en C generan V.

La restricción a W de la forma cuadrática Q toma valores en R, pues es

$$Q(X) = \alpha\bar{\alpha} + \beta\bar{\beta} + \gamma\bar{\gamma},$$

y es fácil ver que se trata de una forma cuadrática en W respecto a la cual

$$W = W_1 \perp W_2 \perp W_3,$$

donde $W_i \leq H_i$ está formado por las matrices $M_i(\alpha)$ con $\alpha \in C$, por lo que cada W_i tiene dimensión 2. Es fácil ver que cada W_i es un subespacio de W no degenerado y, más aún, es no singular, pues $Q(M_i(\alpha)) = \alpha\bar{\alpha} \neq 0$ salvo si $\alpha = 0$.

Observemos ahora que $W_1 \perp W_2$ se puede expresar como suma de dos planos hiperbólicos. La alternativa sería que $W_1 \perp W_2 = H_0 \perp W_0$, donde H_0 es un plano hiperbólico y W_0 un plano no singular, pero, por el teorema de Witt, una isometría entre W_2 y W_0 se extendería a una isometría de W en sí mismo, la cual se restringiría a su vez a una isometría entre W_1 y H_0, lo cual es imposible.

Por lo tanto, W es suma de dos planos hiperbólicos y un plano no singular, lo que se traduce en que su índice de Witt es $m = 2$, luego $\mathrm{O}(W) = \mathrm{O}^-(6, q)$.

Por otra parte, consideremos el grupo $\mathrm{LE}(4, q^2)$, que podemos identificar con el grupo de los automorfismos de determinante 1 del espacio $V_0 = C^4$. Consideramos en éste la forma bilineal hermitiana que en la base canónica tiene matriz identidad, es decir, la dada por

$$F(z, w) = z_1\bar{w}_1 + z_2\bar{w}_2 + z_3\bar{w}_3 + z_4\bar{w}_4.$$

Podemos considerar entonces el grupo $\mathrm{UE}(4, q^2) \leq \mathrm{LE}(4, q^2)$. Vamos a probar que si $f \in \mathrm{UE}(4, q^2)$, su imagen $\rho(f) \in \Omega(V)$ cumple que $\rho(f)[W] = W$.

Como las transvecciones unitarias generan $\mathrm{UE}(4,q^2)$ (teorema 9.17), basta probarlo para una de ellas, digamos $T_{z,\eta}$, donde $z \in C^4$ y $\eta \in C$ cumplen

$$z_1\bar{z}_1 + z_2\bar{z}_2 + z_3\bar{z}_3 + z_4\bar{z}_4 = 0, \qquad \bar{\eta} = -\eta.$$

Recordemos que

$$T_{z,\eta}(w) = w + \eta F(w,z)z,$$

y aplicando esto a los vectores de la base canónica obtenemos que la matriz de $T_{z,\eta}$ es

$$T_{z,\eta} = \begin{pmatrix} 1+\eta\bar{z}_1z_1 & \eta\bar{z}_1z_2 & \eta\bar{z}_1z_3 & \eta\bar{z}_1z_4 \\ \eta\bar{z}_2z_1 & 1+\eta\bar{z}_2z_2 & \eta\bar{z}_2z_3 & \eta\bar{z}_2z_4 \\ \eta\bar{z}_3z_1 & \eta\bar{z}_3z_2 & 1+\eta\bar{z}_3z_3 & \eta\bar{z}_3z_4 \\ \eta\bar{z}_4z_1 & \eta\bar{z}_4z_2 & \eta\bar{z}_4z_3 & 1+\eta\bar{z}_4z_4 \end{pmatrix}.$$

Un cálculo rutinario muestra que $\rho(T_{z,\eta})(M_1(\alpha)) = T_{z,\eta}^t M_1(\alpha) T_{z,\eta}$ es

$$\begin{pmatrix} 0 & \alpha z_1\bar{z}_1\eta + \alpha z_2\bar{z}_2\eta + \alpha & \alpha z_3\bar{z}_2\eta - \bar{\alpha}z_1\bar{z}_4\eta & \bar{\alpha}z_1\bar{z}_3\eta + \alpha z_4\bar{z}_2\eta \\ -\alpha z_1\bar{z}_1\eta - \alpha z_2\bar{z}_2\eta - \alpha & 0 & -\alpha\bar{z}_1z_3\eta - \bar{\alpha}\bar{z}_4z_2\eta & \bar{\alpha}\bar{z}_3z_2\eta - \alpha\bar{z}_1z_4\eta \\ -\alpha z_3\bar{z}_2\eta + \bar{\alpha}z_1\bar{z}_4\eta & \alpha\bar{z}_1z_3\eta + \bar{\alpha}\bar{z}_4z_2\eta & 0 & \bar{\alpha}z_3\bar{z}_3\eta + \bar{\alpha}z_4\bar{z}_4\eta + \bar{\alpha} \\ -\bar{\alpha}z_1\bar{z}_3\eta - \alpha z_4\bar{z}_2\eta & -\bar{\alpha}\bar{z}_3z_2\eta + \alpha\bar{z}_1z_4\eta & -\bar{\alpha}z_3\bar{z}_3\eta - \bar{\alpha}z_4\bar{z}_4\eta - \bar{\alpha} & 0 \end{pmatrix}$$

y, teniendo en cuenta las relaciones que cumplen z y η, es claro que

$$\rho(T_{z,\eta})(M_1(\alpha)) \in W.$$

Igualmente se comprueba que $\rho(T_{z,\eta})(M_2(\beta)), \rho(T_{z,\eta})(M_3(\gamma)) \in W$, con lo que $\rho(T_{z,\eta})[W] \leq W$ y, como ambos subespacios tienen dimensión 6, concluimos que $\rho(T_{z,\eta})[W] = W$. A su vez, esto implica que si $f \in \mathrm{UE}(4,q^2)$, entonces $\rho(f)[W] = W$.

Puesto que $\rho(f) \in \mathrm{O}(V)$, es decir, que f conserva la forma cuadrática Q, lo mismo le sucede a la restricción $\rho(f)|_W$, por lo que $\rho(f)|_W \in \mathrm{O}(W)$. Por lo tanto, tenemos un homomorfismo de grupos

$$\mathrm{UE}(4,q^2) \xrightarrow{\rho} \Omega(V) \longrightarrow \mathrm{O}(W).$$

Más precisamente, como $\mathrm{UE}(4,q^2) = \mathrm{UE}(4,q^2)'$ (teorema 9.20), en realidad se trata de un homomorfismo

$$\mathrm{UE}(4,q^2) \longrightarrow \Omega(W).$$

Más aún, se cumple que $\rho(f)|_W = \pm 1$ si y sólo si $\rho(f) = \pm 1$, pues, si $\rho(f)|_W$ y ± 1 coinciden en W, en particular coinciden en una base de V, luego son iguales. Esto se traduce en que el núcleo del homomorfismo

$$\mathrm{UE}(4,q^2) \longrightarrow \Omega\mathrm{P}(W)$$

es la intersección con $\mathrm{UE}(4,q^2)$ del núcleo de $\bar{\rho}$, luego dicho homomorfismo induce un monomorfismo

$$\mathrm{UEP}(4,q^2) \longrightarrow \Omega\mathrm{P}(W) = \Omega\mathrm{P}^-(6,q).$$

Como ambos grupos tienen el mismo orden, se trata de un isomorfismo. ∎

Así pues, los menores órdenes de grupos simples ortogonales "nuevos" son

$$|\Omega\mathrm{P}^+(8,2)| = 174\,182\,400, \qquad |\Omega\mathrm{P}^-(8,2)| = 197\,406\,720,$$

$$|\Omega\mathrm{P}(7,2)| = 4\,585\,351\,680.$$

Un análisis de las fórmulas que hemos encontrado para los órdenes de los grupos simples clásicos finitos muestra que los únicos casos en los que grupos de dos familias tienen el mismo orden los grupos son los casos en los que ya hemos demostrado que los grupos correspondientes son isomorfos salvo en el caso de los grupos A_8 y $\mathrm{LEP}(3,4)$, que tienen ambos orden 20 160 y no son isomorfos, y el caso

$$|\Omega\mathrm{P}(2m+1,q)| = \frac{1}{2}q^{m^2}\prod_{i=1}^{m}(q^{2i}-1) = |\mathrm{SpP}(2m,q)|,$$

para q impar. Sobre este caso hemos probado que

$$\Omega\mathrm{P}(3,q) \cong \mathrm{LEP}(2,q) \cong \mathrm{SpP}(2,q), \qquad \Omega\mathrm{P}(5,q) \cong \mathrm{SpP}(4,q),$$

por lo que resulta natural conjeturar que la igualdad de órdenes anterior es en realidad el reflejo de otro isomorfismo de grupos, pero los dos teoremas siguientes muestran que no es así:

Teorema 9.62 *Si q es impar, $\mathrm{SpP}(2m,q)$ tiene $E[m/2]+1$ clases de conjugación de elementos de orden 2.*

Demostración: Sea V un espacio simpléctico de dimensión $2m$ sobre el cuerpo de q elementos. Si $t \in \mathrm{Sp}(2m,q)$ representa un elemento de orden 2 en $\mathrm{SpP}(2m,q)$, tenemos que $t^2 = 1$ o $t^2 = -1$.

Supongamos en primer lugar que $t^2 = 1$. Entonces todo $v \in V$ cumple

$$v = \frac{1}{2}(v + t(v)) + \frac{1}{2}(v - t(v)),$$

luego $V = V_+ \oplus V_-$, donde $V_\epsilon = \{v \in V \mid t(v) = \epsilon v\}$. Si $u \in V_+$ y $v \in V_-$, entonces

$$F(u,v) = F(t(u),t(v)) = -F(u,v),$$

luego $F(u,v) = 0$. Así pues, $V = V_+ \perp V_-$. Esto implica que V_+ y V_- son no degenerados. En particular son subespacios simplécticos, luego su dimensión es par. Intercambiando t con $-t$ si es preciso (ambos representan la misma clase en $\mathrm{SpP}(2m,q)$), podemos suponer que $2 \le \dim V_- \le m$.

Supongamos ahora que t' es otro elemento de orden 2 en $\mathrm{Sp}(2m,q)$ y sea $V = V'_+ \perp V'_-$ la descomposición correspondiente de V, donde, intercambiando de nuevo si es preciso t' con $-t'$, podemos suponer también que $2 \le \dim V'_- \le m$.

Si $\dim V_- = \dim V'_-$, existe una transformación $g \in \mathrm{Sp}(2m,q)$ tal que $g[V_+] = V'_+$ y $g[V_-] = V'_-$ (basta descomponer los cuatro subespacios en sumas ortogonales de planos hiperbólicos y considerar isometrías entre ellos). Entonces $g^{-1}tg = t'$. Recíprocamente, si t y t' son conjugados, se cumple trivialmente que $\dim V_- = \dim V'_-$.

Descomponiendo V en suma ortogonal de planos hiperbólicos es fácil construir transformaciones t de orden 2 tales que $\dim V_-$ tome cualquier valor par entre 2 y m, luego hay $E[m/2]$ clases de conjugación de elementos de orden 2 en $\mathrm{SpP}(2m,q)$ representados por elementos de orden 2 de $\mathrm{Sp}(2m,q)$.

Supongamos ahora que $t^2=-1$. Si $4 \mid q-1$, entonces el cuerpo de escalares C, entonces existe $\alpha \in C$ tal que $\alpha^2=-1$, lo que nos permite descomponer

$$v = \frac{1}{2}(v-\alpha t(v)) + \frac{1}{2}(v+\alpha t(v)),$$

de modo que $V = V_+ \oplus V_-$, donde

$$V_\epsilon = \{v \in V \mid t(v) = \epsilon\alpha v\}.$$

Ahora, si $v, v' \in V_\epsilon$, tenemos que

$$F(v,v') = F(t(v),t(v')) = F(\epsilon\alpha v, \epsilon\alpha v') = -F(v,v'),$$

luego $F(v,v')=0$, por lo que ahora los V_ϵ son subespacios totalmente isótropos. Es fácil ver que cada uno de ellos no puede tener dimensión mayor que m, pues, razonando como en la prueba del teorema 8.27, a partir de un subespacio totalmente isótropo $\langle u_1,\dots,u_d\rangle$ se puede formar una suma ortogonal de planos hiperbólicos $\langle u_1,v_1\rangle \perp \cdots \perp \langle u_d,v_d\rangle$.

En efecto, tomando $v_1 \in \langle u_2,\dots,u_d\rangle^\perp \setminus \langle u_1,\dots,u_d\rangle$ obtenemos un plano hiperbólico $H_1 = \langle u_1,v_1\rangle$ tal que $\langle u_2,\dots,u_d\rangle \le H_1^\perp$ y razonando inductivamente, $H_1^\perp$ contiene una suma ortogonal de $d-1$ planos hiperbólicos). Por lo tanto, $\dim V_+ = \dim V_- = m$ (para que su suma pueda ser V). Pero en este contexto podemos refinar la construcción. Veamos lo siguiente:

> *Si V es un espacio simpléctico de dimensión $2m$ y $V = V_1 \oplus V_2$, donde V_1 y V_2 son subespacios totalmente isótropos de dimensión m y $V_1 = \langle u_1,\dots,u_m\rangle$, entonces V_2 tiene una base $v_1,\dots,v_m$ tal que $V = \langle u_1,v_1\rangle \perp \cdots \perp \langle u_m,v_m\rangle$ es una suma ortogonal de planos hiperbólicos.*

En efecto, observemos que $V_i^\perp = V_i$. Sea $V_1' = \langle u_2,\dots,u_m\rangle$, de modo que $V_1 = V_1^\perp \le V_1'^\perp$ y este último espacio tiene dimensión $m+1$, por lo que $\dim V_1'^\perp \cap V_2 = 1$. Sea $v_1 \in V_1'^\perp \cap V_2$ no nulo. No puede ser $F(u_1,v_1)=0$, pues entonces $v_1 \in V_1^\perp \cap V_2 = V_1 \cap V_2 = 0$, luego podemos exigir que $F(u_1,v_1)=1$. Sea $H_1 = \langle u_1,v_1\rangle$.

Llamamos $V_2' = \langle u_1\rangle^\perp \cap V_2$, de modo que $\dim V_1' = \dim V_2' = m-1$ y $H_1^\perp = V_1' \oplus V_2'$, donde los dos sumandos son totalmente isótropos, luego podemos aplicar la hipótesis de inducción y obtenemos la conclusión.

Aplicando este resultado a nuestro caso, concluimos que

$$V = \langle u_1,v_1\rangle \perp \cdots \perp \langle u_m,v_m\rangle,$$

donde $V_+ = \langle u_1,\dots,u_m\rangle$, $V_- = \langle v_1,\dots,v_m\rangle$.

Si t' cumple también $t'^2 = -1$ y $V = V'_+ \oplus V'_-$ es la descomposición correspondiente, la transformación $g \in \mathrm{Sp}(V)$ que hace corresponder las bases de planos hiperbólicos cumple $g[V_\epsilon] = V'_\epsilon$, de donde se concluye que $g^{-1}tg = t'$, luego las transformaciones que cumplen $t^2 = -1$ forman una única clase de conjugación, y en total hay $E[m/2] + 1$ clases.

Supongamos ahora que $4 \nmid q-1$. Si existiera $u \in V$ no nulo tal que $t(u) = \lambda u$, aplicando de nuevo t resultaría que $-u = \lambda^2 u$, luego $\lambda^2 = -1$, pero esto es imposible en el caso que estamos considerando, luego, para todo vector no nulo u, se cumple que $\langle u, t(u)\rangle$ tiene dimensión 2. Si es totalmente isótropo, según hemos visto podemos formar dos planos hiperbólicos $\langle u, v\rangle \perp \langle t(u), v'\rangle$. En particular $F(u, v) = 1$, $F(t(u), v) = 0$. Sea $w = u + t(v)$ y observemos que

$$F(w, t(w)) = F(u+t(v), t(u)-v) = F(u, t(u))-F(u, v)+F(t(v), t(u))-F(t(v), v)$$
$$= -F(u, v) + F(v, u) = -2 \neq 0.$$

Por lo tanto, siempre existe un $w \in V$ tal que $H_1 = \langle w, t(w)\rangle$ es un plano hiperbólico con la propiedad de que $t[H_1] = H_1$. Más precisamente, llamando $d = F(w, t(w))$ y $u_1 = aw + bt(w)$, tenemos que

$$F(u_1, t(u_1)) = F(aw + bt(w), at(w) - bw) = a^2 d + b^2 d.$$

Por el teorema 8.37 podemos elegir a y b de modo que $F(u_1, t(u_1)) = 1$. Razonando por inducción obtenemos que $V = H_1 \perp \cdots \perp H_m$, donde cada plano hiperbólico es de la forma $H_i = \langle u_i, t(u_i)\rangle$.

Nuevamente, si t' es otra transformación que cumple $t'^2 = -1$ y $u'_1, \ldots, u'_m$ determinan la base de V correspondiente, podemos construir $g \in \mathrm{Sp}(V)$ tal que $g[H_i] = H'_i$ y así llegamos igualmente a que $g^{-1}tg = t'$, con lo que hay una única clase de conjugación de transformaciones de este tipo y el número total es, como en el caso anterior, $E[m/2] + 1$. ∎

Teorema 9.63 *Si q es impar, $\Omega\mathrm{P}(2m + 1, q)$ tiene al menos m clases de conjugación de elementos de orden 2.*

Demostración: En vista del isomorfismo $\Omega\mathrm{P}(3, q) \cong \mathrm{SpP}(2, q)$ y del teorema anterior, podemos suponer que $m \geq 2$. Sea V un espacio ortogonal de dimensión $2m+1$ sobre el cuerpo C de q elementos. Notemos que, como $2m+1$ es impar, en realidad tenemos que $\Omega\mathrm{P}(2m+1, q) = \Omega(2m+1, q)$. Consideremos una transformación ortogonal $t \in \Omega(2m + 1, q)$ tal que $t^2 = 1$.

Como en el teorema anterior podemos descomponer $V = V_+ \perp V_-$, donde $V_\epsilon = \{v \in V \mid t(v) = \epsilon v\}$ son dos subespacios no degenerados. Observemos que $V_+ = \mathrm{N}(1 - t)$, luego, teniendo en cuenta el teorema 9.26,

$$V_t = \mathrm{Im}(1 - t) = \mathrm{N}(1 - t)^\perp = V_+^\perp = V_-.$$

Como $t \in \Omega(2m + 1, q) \leq \mathrm{OE}(2m + 1, q)$, según la definición 9.38, tenemos que $\dim V_- = 2k$ es par. Observemos que $V_+ = \mathrm{N}(1 - t)$, luego, teniendo en cuenta el teorema 9.26,

$$V_t = \mathrm{Im}(1 - t) = \mathrm{N}(1 - t)^\perp = V_+^\perp = V_-.$$

Como $t \in \Omega(2m+1,q) \leq \mathrm{OE}(2m+1,q)$, según la definición 9.38, tenemos que $\dim V_- = 2k$ es par. La restricción de t a V_- es -1, luego $-1 \in \Omega^\epsilon(2k,q)$, donde, según hemos visto al calcular los órdenes de los grupos ortogonales, esto sucede si y sólo si $q^k \equiv \epsilon$ (mód 4).

Es claro que si dos transformaciones son conjugadas, las dimensiones de los espacios V_- correspondientes deben coincidir, luego basta probar que existen transformaciones $t \in \Omega(2m+1,q)$ de orden 2 para las que $\dim V_- = 2k$ para todos los valores posibles $1 \leq k \leq m$.

En efecto, fijado k, tomamos el signo $\epsilon = \pm 1$ que cumple $q^k \equiv \epsilon$ (mód 4) y consideramos cualquier espacio cuadrático V_1 de dimensión $2k$ y signo ϵ y cualquier espacio cuadrático V_2 de dimensión $2m+1-2k$. A partir de ellos podemos construir un espacio ortogonal $V' = V_1 \perp V_2$ de dimensión $2m+1$ que no es necesariamente isométrico a V, pero que, si no lo es, pasa a serlo sin más que sustituir su forma cuadrática por un múltiplo adecuado (véase la discusión previa a la definición 8.44), y esto no cambia el signo de V_1 (pues el índice de Witt no cambia). Por lo tanto, podemos descomponer $V = V_1 \perp V_2$, donde V_1 y V_2 son subespacios no degenerados con $\dim V_1 = 2k$ y $\Omega(V_1) = \Omega^\epsilon(2k,q)$. (Hemos encontrado un espacio isométrico a V que admite esta descomposición, luego V también la admite.)

Tenemos entonces que $-1 \in \Omega(V_1)$, lo que nos permite definir $t \in \Omega(V)$ dada por $t|_{V_1} = -1$, $t|_{V_2} = 1$, y así tenemos una transformación de orden 2 para la que $\dim V_- = 2k$. ∎

9.3 Los grupos simples finitos clásicos

Resumimos en esta sección los resultados que hemos obtenido en este capítulo y los anteriores, para dar una visión de conjunto. Los llamados grupos simples (finitos) clásicos son los siguientes:

		Orden	Excepciones
Lineales	$\mathrm{LEP}(n,q)$	$\dfrac{q^{n(n-1)/2}}{(n,q-1)}\prod_{i=1}^{n-1}(q^{i+1}-1)$	$(2,2),(2,3)$
Simplécticos	$\mathrm{SpP}(2m,q)$	$\dfrac{q^{m^2}}{(2,q-1)}\prod_{i=1}^{m}(q^{2i}-1)$	$(2,2),(2,3),(4,2)$
Unitarios	$\mathrm{UEP}(n,q^2)$	$\dfrac{q^{n(n-1)/2}}{(n,q+1)}\prod_{i=1}^{n-1}(q^{i+1}-(-1)^{i+1})$	$(2,4),(2,9),(3,4)$
Ortogonales	$\Omega\mathrm{P}(2m+1,q)$	$(1/2)q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$	$(3,3)$
	$\Omega\mathrm{P}^\epsilon(2m,q)$	$\dfrac{q^{m(m-1)}(q^m-\epsilon)}{(2,q+1)}\prod_{i=1}^{m-1}(q^{2i}-1)$	$m=2,\epsilon=1$

En todos los casos de la tabla anterior $q > 1$ es una potencia de primo, $n \geq 2$, $m \geq 1$. En el caso de los grupos $\Omega(2m+1,q)$ hay que exigir que q sea impar y en los grupos $\Omega^\epsilon(2m,q)$ que $m \geq 2$.

Isomorfismos Entre estas familias de grupos y la familia de los grupos alternados se dan los isomorfismos siguientes (el correspondiente a $\Omega(3,q)$ requiere que q sea impar):

$$\begin{aligned}
&\Omega(3,q) \cong \mathrm{LEP}(2,q) \cong \mathrm{SpP}(2,q) \cong \mathrm{UEP}(2,q^2)\\
&\Omega\mathrm{P}^-(4,q) \cong \mathrm{LEP}(2,q^2)\\
&\Omega\mathrm{P}(5,q) \cong \mathrm{SpP}(4,q)\\
&\Omega\mathrm{P}^+(6,q) \cong \mathrm{LEP}(4,q)\\
&\Omega\mathrm{P}^-(6,q) \cong \mathrm{UEP}(4,q^2)
\end{aligned}$$

	orden
$\mathrm{LEP}(2,4) \cong \mathrm{LEP}(2,5) \cong A_5$	60
$\mathrm{LEP}(2,7) \cong \mathrm{LEP}(3,2)$	168
$\mathrm{LEP}(2,9) \cong A_6$	360
$\mathrm{LEP}(4,2) \cong A_8$	20 160
$\mathrm{UEP}(4,4) \cong \mathrm{SpP}(4,3)$	25 920

Coincidencias de orden Los grupos

$$\mathrm{LEP}(4,2) \cong A_8, \qquad \text{y} \qquad \mathrm{LEP}(3,4)$$

tienen ambos orden 20 160, pero no son isomorfos, e igualmente

$$|\Omega\mathrm{P}(2m+1,q)| = \frac{1}{2}q^{m^2}\prod_{i=1}^{m}(q^{2i}-1) = |\mathrm{SpP}(2m,q)|$$

sin que los grupos correspondientes sean isomorfos para $m \geq 3$. La menor pareja es

$$|\Omega\mathrm{P}(7,2)| = |\mathrm{SpP}(6,2)| = 1\,451\,520.$$

El teorema de clasificación de los grupos simples finitos muestra que éstos son los únicos casos de grupos simples no isomorfos del mismo orden.

La tabla de la página siguiente recoge los 31 subgrupos simples no abelianos de orden menor que 100 000. Entre ellos hay únicamente dos grupos esporádicos (los grupos de Mathieu M_{11} y M_{12}) y un único grupo que no hemos estudiado: el grupo de Suzuki Suz(8), de orden 29 120.

Notación como grupos de tipo de Lie El teorema de clasificación de los grupos simples finitos establece que, aparte de los grupos alternados y los 26 esporádicos, hay 16 familias de grupos simples finitos de tipo de Lie, pero en estos términos los grupos clásicos constituyen 6 de dichas familias. La correspondencia es la siguiente:

$$\begin{aligned}
A_n(q) &= \mathrm{LEP}(n+1,q) & B_n(q) &= \Omega\mathrm{P}(2n+1,q)\\
C_n(q) &= \mathrm{SpP}(2n,q) & D_n(q) &= \Omega\mathrm{P}^+(2n,q)\\
{}^2A_n(q^2) &= \mathrm{UEP}(n+1,q^2) & {}^2D_n(q) &= \Omega\mathrm{P}^-(2n,q).
\end{aligned}$$

Las cuatro primeras familias forman parte de las nueve familias de grupos de Chevalley, mientras que las dos últimas forman parte de las cuatro familias de grupos de Steinberg.

Grupos simples de orden menor que 100 000

60	$2^2 \cdot 3 \cdot 5$	$A_5 = \mathrm{LEP}(2, 2^2) = \mathrm{LEP}(2, 5) = \mathrm{SpP}(2, 2^2)$ $= \mathrm{SpP}(2, 5) = \mathrm{UEP}(2, 2^4) = \mathrm{UEP}(2, 5^2)$ $= \Omega\mathrm{P}(3, 5) = \Omega\mathrm{P}^-(4, 2)$
168	$2^3 \cdot 3 \cdot 7$	$\mathrm{LEP}(2, 7) = \mathrm{LEP}(3, 2) = \mathrm{SpP}(2, 7)$ $= \mathrm{UEP}(2, 7^2) = \Omega\mathrm{P}(3, 7)$
360	$2^3 \cdot 3^2 \cdot 5$	$A_6 = \mathrm{LEP}(2, 3^2) = \mathrm{SpP}(2, 3^2) = \mathrm{UEP}(2, 3^4)$ $= \Omega\mathrm{P}(3, 3^2) = \Omega\mathrm{P}^-(4, 3)$
504	$2^3 \cdot 3^2 \cdot 7$	$\mathrm{LEP}(2, 2^3) = \mathrm{SpP}(2, 2^3) = \mathrm{UEP}(2, 2^6)$
660	$2^2 \cdot 3 \cdot 5 \cdot 11$	$\mathrm{LEP}(2, 11) = \mathrm{SpP}(2, 11) = \mathrm{UEP}(2, 11^2) = \Omega\mathrm{P}(3, 11)$
1 092	$2^2 \cdot 3 \cdot 7 \cdot 13$	$\mathrm{LEP}(2, 13) = \mathrm{SpP}(2, 13) = \mathrm{UEP}(2, 13^2) = \Omega\mathrm{P}(3, 13)$
2 448	$2^4 \cdot 3^2 \cdot 17$	$\mathrm{LEP}(2, 17) = \mathrm{SpP}(2, 17) = \mathrm{UEP}(2, 17^2) = \Omega\mathrm{P}(3, 17)$
2 520	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	A_7
3 420	$2^2 \cdot 3^2 \cdot 5 \cdot 19$	$\mathrm{LEP}(2, 19) = \mathrm{SpP}(2, 19) = \mathrm{UEP}(2, 19^2) = \Omega\mathrm{P}(3, 19)$
4 080	$2^4 \cdot 3 \cdot 5 \cdot 17$	$\mathrm{LEP}(2, 2^4) = \mathrm{SpP}(2, 2^4) = \mathrm{UEP}(2, 2^8) = \Omega\mathrm{P}^-(4, 2^2)$
5 616	$2^4 \cdot 3^3 \cdot 13$	$\mathrm{LEP}(3, 3)$
6 048	$2^5 \cdot 3^3 \cdot 7$	$\mathrm{UEP}(3, 3^2)$
6 072	$2^3 \cdot 3 \cdot 11 \cdot 23$	$\mathrm{LEP}(2, 23) = \mathrm{SpP}(2, 23) = \mathrm{UEP}(2, 23^2) = \Omega\mathrm{P}(3, 23)$
7 800	$2^3 \cdot 3 \cdot 5^2 \cdot 13$	$\mathrm{LEP}(2, 5^2) = \mathrm{SpP}(2, 5^2) = \mathrm{UEP}(2, 5^4)$ $= \Omega\mathrm{P}(3, 5^2) = \Omega\mathrm{P}^-(4, 5)$
7 920	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	M_{11}
9 828	$2^2 \cdot 3^3 \cdot 7 \cdot 13$	$\mathrm{LEP}(2, 3^3) = \mathrm{SpP}(2, 3^3) = \mathrm{UEP}(2, 3^6) = \Omega\mathrm{P}(3, 3^3)$
12 180	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	$\mathrm{LEP}(2, 29) = \mathrm{SpP}(2, 29) = \mathrm{UEP}(2, 29^2) = \Omega\mathrm{P}(3, 29)$
14 880	$2^5 \cdot 3 \cdot 5 \cdot 31$	$\mathrm{LEP}(2, 31) = \mathrm{SpP}(2, 31) = \mathrm{UEP}(2, 31^2) = \Omega\mathrm{P}(3, 31)$
20 160	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	$A_8 = \mathrm{LEP}(4, 2) = \Omega\mathrm{P}^+(6, 2)$
20 160	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	$\mathrm{LEP}(3, 2^2)$
25 308	$2^2 \cdot 3^2 \cdot 19 \cdot 37$	$\mathrm{LEP}(2, 37) = \mathrm{SpP}(2, 37) = \mathrm{UEP}(2, 37^2) = \Omega\mathrm{P}(3, 37)$
25 920	$2^6 \cdot 3^4 \cdot 5$	$\mathrm{SpP}(4, 3) = \mathrm{UEP}(4, 2^2) = \Omega\mathrm{P}(5, 3) = \Omega\mathrm{P}^-(6, 2)$
29 120	$2^6 \cdot 5 \cdot 7 \cdot 13$	$\mathrm{Suz}(8)$
32 736	$2^5 \cdot 3 \cdot 11 \cdot 31$	$\mathrm{LEP}(2, 2^5) = \mathrm{SpP}(2, 2^5) = \mathrm{UEP}(2, 2^{10})$
34 440	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$	$\mathrm{LEP}(2, 41) = \mathrm{SpP}(2, 41) = \mathrm{UEP}(2, 41^2) = \Omega\mathrm{P}(3, 41)$
39 732	$2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$	$\mathrm{LEP}(2, 43) = \mathrm{SpP}(2, 43) = \mathrm{UEP}(2, 43^2) = \Omega\mathrm{P}(3, 43)$
51 888	$2^4 \cdot 3 \cdot 23 \cdot 47$	$\mathrm{LEP}(2, 47) = \mathrm{SpP}(2, 47) = \mathrm{UEP}(2, 47^2) = \Omega\mathrm{P}(3, 47)$
58 800	$2^4 \cdot 3 \cdot 5 \cdot 7^2$	$\mathrm{LEP}(2, 7^2) = \mathrm{SpP}(2, 7^2) = \mathrm{UEP}(2, 7^4)$ $= \Omega\mathrm{P}(3, 7^2) = \Omega\mathrm{P}^-(4, 7)$
62 400	$2^6 \cdot 3 \cdot 5^2 \cdot 13$	$\mathrm{UEP}(3, 2^4)$
74 412	$2^2 \cdot 3^3 \cdot 13 \cdot 53$	$\mathrm{LEP}(2, 53) = \mathrm{SpP}(2, 53) = \mathrm{UEP}(2, 53^2) = \Omega\mathrm{P}(3, 53)$
95 040	$2^6 \cdot 3 \cdot 5 \cdot 11$	M_{12}

Apéndice A

Congruencia a trozos en el espacio euclídeo

En este apéndice demostraremos la paradoja de Banach-Tarski descrita en la introducción, y veremos que es esencialmente una consecuencia del hecho de que el grupo de los giros respecto de un eje que pasa por un punto fijo contiene un subgrupo libre de rango 2.

A.1 La paradoja de Banach-Tarski

Sea G el grupo de los giros en el espacio tridimensional respecto de ejes que pasan por un punto O. Si tomamos O como origen de coordenadas, de acuerdo con la clasificación de las isometrías vista en la sección [G 5.5], los elementos de G se corresponden con las matrices ortogonales de determinante 1, y al final de la sección 3.2 hemos visto que los giros

$$\sigma = \frac{1}{7}\begin{pmatrix} 6 & 2 & -3 \\ 2 & 3 & 6 \\ 3 & -6 & 2 \end{pmatrix}, \qquad \tau = \frac{1}{7}\begin{pmatrix} 2 & 6 & -3 \\ -6 & 3 & 2 \\ 3 & 2 & 6 \end{pmatrix}.$$

generan un subgrupo libre $L = \langle \sigma, \tau \rangle \leq G$ de rango 2. Cada elemento de L distinto del neutro se expresa de forma única como composición de un número finito de giros $\sigma, \sigma^{-1}, \tau, \tau^{-1}$, de modo que un giro nunca aparece seguido de su inverso. Esto nos permite descomponer a L como unión disjunta

$$L = \{1\} \cup L_\sigma \cup L_{\sigma^{-1}} \cup L_\tau \cup L_{\tau^{-1}},$$

donde L_x es el conjunto de los giros de L que terminan en x. Es claro entonces que

$$L = L_\sigma \cup L_{\sigma^{-1}}\sigma = L\tau \cup L_{\tau^{-1}}\tau,$$

pues si $f \in L \setminus L_\sigma$, entonces $f\sigma^{-1} \in L_{\sigma^{-1}}$, luego $f \in L_{\sigma^{-1}}\sigma$, e igualmente con τ. Además ambas uniones son disjuntas.

Esto es una forma abstracta de la paradoja de Banach-Tarski: podemos descomponer L como dos uniones disjuntas de modo que si aplicamos σ^{-1} (resp. τ^{-1}) al segundo conjunto de cada descomposición obtenemos cuatro subconjuntos de L disjuntos dos a dos.

Para convertir estas descomposiciones de L en descomposiciones de esferas consideramos una esfera S (en el sentido de una superficie esférica, sin el interior) de centro O, de modo que cada giro de L distinto de la identidad fija exactamente a dos puntos antípodas de S. Como L es numerable, el conjunto $\tilde{F}$ formado por todos los puntos de S fijados por algún elemento de L es numerable. Llamemos $S_0 = S \setminus \tilde{F}$.

Observemos que si $f \in L$, entonces $f[S_0] = S_0$, pues si $P \in S_0$ y $f(P)$ fuera fijado por un giro $g \in L$, tendríamos que $g(f(P)) = f(P)$, con lo que $(fgf^{-1})(P) = P$, luego $P \in \tilde{F}$, y tenemos una contradicción.

Esto significa que L actúa sobre S_0, luego lo divide en una familia de órbitas disjuntas dos a dos. Llamemos[1] $M \subset S_0$ a un conjunto formado por un punto de cada una de ellas. Así

$$\{f[M] \mid f \in L\}$$

es una partición de S_0, pues si $P \in g_1[M] \cap g_2[M]$, con $g_1, g_2 \in L$, entonces $P = g_1[P_1] = g_2[P_2]$, con $P_1, P_2 \in M$, luego $g_2(g_1(P_1)) = P_2$, y esto significa que P_1 y P_2 están en la misma órbita respecto de la acción de L, luego tiene que ser $P_1 = P_2$, y entonces $g_2(g_1(P_1)) = P_1$, lo que significa que $P_1 \in \tilde{F}$, y esto es una contradicción. (Hemos tenido que eliminar $\tilde{F}$ precisamente para obtener una partición.)

Si $X \subset L$, llamemos $X^* = \bigcup_{g \in X} g[M]$, de modo que

$$(X \cup Y)^* = X^* \cup Y^*, \qquad (X \cap Y)^* = X^* \cap Y^*, \qquad L^* = S_0, \qquad \varnothing^* = \varnothing,$$

por lo que si llamamos $A = L_\sigma^*$, $B = L_{\sigma^{-1}}^*$, $C = L_\tau^*$, $D = L_{\tau^{-1}}^*$, tenemos que

$$\sigma[B] = \bigcup_{g \in L_{\sigma^{-1}}} \sigma[g[M]] = \bigcup_{g \in L_{\sigma^{-1}}\sigma} g[M] = (L_{\sigma^{-1}}\sigma)^*,$$

e igualmente $\tau[D] = (L_{\tau^{-1}}\tau)^*$, luego los conjuntos A^*, B^*, C^*, D^* son subconjuntos de S_0 disjuntos dos a dos pero aplicando giros nos bastan dos de ellos para cubrir S_0:

$$S_0 = A^* \cup \sigma[B^*] = C^* \cup \tau[D^*].$$

Esto es una versión un poco más "concreta" de la paradoja de Banach-Tarski: ahora tenemos cuatro subconjuntos disjuntos de S_0 tales que si giramos dos de ellos obtenemos dos particiones de S_0 (moviendo cuatro trozos de esfera podemos formar dos esferas casi completas). Para eliminar el "casi" (es decir, el conjunto $\tilde{F}$ de puntos fijos), observamos que existe un giro $r \in G$ tal que los conjuntos

$$\tilde{F}, \quad r[\tilde{F}], \quad r^2[\tilde{F}], \quad r^3[\tilde{F}], \quad \dots$$

son disjuntos dos a dos.

[1] La existencia de M está garantizada por el axioma de elección, sin el cual no es posible probar la paradoja de Banach-Tarski, y éste es el único punto de la prueba que lo requiere.

En efecto, fijamos un eje que pase por el centro O de la esfera S y por dos puntos antípodas de S_0, y sea G_0 el subgrupo formado por las rotaciones alrededor de dicho eje. Observemos que a lo sumo hay una rotación en G_0 que transforma un punto de S en otro. Como $\tilde{F}$ es numerable, dado $P \in \tilde{F}$, el conjunto $X_{P,n} = \{r \in G_0 \mid r^n(P) \in \tilde{F}\}$ es numerable, luego también lo es la unión X de todos los conjuntos $X_{P,n}$, mientras que G_0 no es numerable (porque hay una cantidad no numerable de ángulos de giro), luego podemos tomar $r \in G_0 \setminus X$, que tiene la propiedad de que $\tilde{F} \cap r^n[\tilde{F}] = \varnothing$ para todo $n \geq 0$, y esto a su vez implica la propiedad requerida, pues si existiera $P \in r^m[\tilde{F}] \cap r^n[\tilde{F}]$, con $m < n$, entonces $r^{-m}(P) \in \tilde{F} \cap r^{n-m}[\tilde{F}] = \varnothing$.

Sea $\tilde{U} = \bigcup_n r^n[\tilde{F}]$, de modo que $r[\tilde{U}] = \tilde{U} \setminus \tilde{F}$ y $\tilde{V} = S \setminus \tilde{U}$. Así:

$$S = \tilde{U} \cup \tilde{V}, \qquad S \setminus \tilde{F} = r[\tilde{U}] \cup \tilde{V}.$$

Así pues: podemos dividir la esfera S en dos partes disjuntas de modo que, girando una de ellas, obtenemos una descomposición de S_0 en dos partes disjuntas.

Sea ahora X_1 la esfera sólida, es decir, la bola cerrada, con el mismo centro O y el mismo radio que S. Para cada subconjunto $E \subset S$, llamaremos $\bar{E} \subset B$ a la unión de todos los segmentos con un extremo en O (no incluido) y el otro en E (incluido). Llamaremos A, B, C, D, F, U, V a los subconjuntos de X_1 obtenidos de este modo a partir de $A^*, B^*, C^*, D^*, \tilde{F}, \tilde{U}, \tilde{V}$. Tenemos las particiones

$$X_1 = \{O\} \cup U \cup V, \qquad X_1 \setminus F = \{O\} \cup r[U] \cup V,$$
$$X_1 \setminus F = \{O\} \cup A \cup \sigma[B] = \{O\} \cup C \cup \tau[D],$$

así como que $A, B, C, D, F \subset X_1$ son disjuntos dos a dos. Sea T una traslación tal que $X_2 = T[X_1]$ sea una bola de centro $O' = T[O]$ disjunta de X_1, y sea $X = X_1 \cup X_2$.

Combinando las dos particiones

$$X_1 \setminus F = \{O\} \cup r[U] \cup V = \{O\} \cup A \cup \sigma[B]$$

se forma una partición en $\{O\}$ más otros cuatro subconjuntos que, a su vez, podemos trasladar a X_1 mediante r, lo que nos da los cuatro conjuntos

$$A_1 = r^{-1}[r[U] \cap A], \quad A_2 = V \cap A, \quad A_3 = r^{-1}[r[U] \cap \sigma[B]], \quad A_4 = V \cap \sigma[B].$$

Así $r[A_1] \cup r[A_3] = r[U] \cap (A \cup \sigma[B]) = r[U]$, $A_2 \cup A_4 = V$, luego tenemos una partición

$$X_1 = \{O\} \cup A_1 \cup A_2 \cup A_3 \cup A_4$$

tal que si aplicamos r a los conjuntos de índice impar queda

$$X_1 \setminus F = r[A_1] \cup A_2 \cup r[A_3] \cup A_4,$$

donde $r[A_1] \cup A_2 = A$, $r[A_3] \cup A_4 = \sigma[B]$, por lo que si aplicamos σ^{-1} a $r[A_3]$ y a A_4 obtenemos los conjuntos

$$B_1 = r[A_1], \quad B_2 = A_2, \quad B_3 = \sigma^{-1}[r[A_3]], \quad B_4 = \sigma^{-1}[A_4],$$

de modo que $B_1 \cup B_2 \cup B_3 \cup B_4 = A \cup B$.

Llamamos $U' = T[U]$, $V' = T[V]$, $C' = T[C]$, $D' = T[D]$, $F' = T[F]$ y $r' = r^T$ a la rotación de X_2 que resulta de trasladar r mediante T. Definimos

$$A_5 = r'^{-1}[r'[U']\cap C], \quad A_6 = V'\cap C, \quad A_7 = r'^{-1}[r'[U]\cap\tau[D']], \quad A_8 = V'\cap\tau[D'].$$

Como antes, la partición

$$X_2 = \{O'\} \cup A_5 \cup A_6 \cup A_7 \cup A_8,$$

de modo que al aplicar r' a los conjuntos de índice impar queda

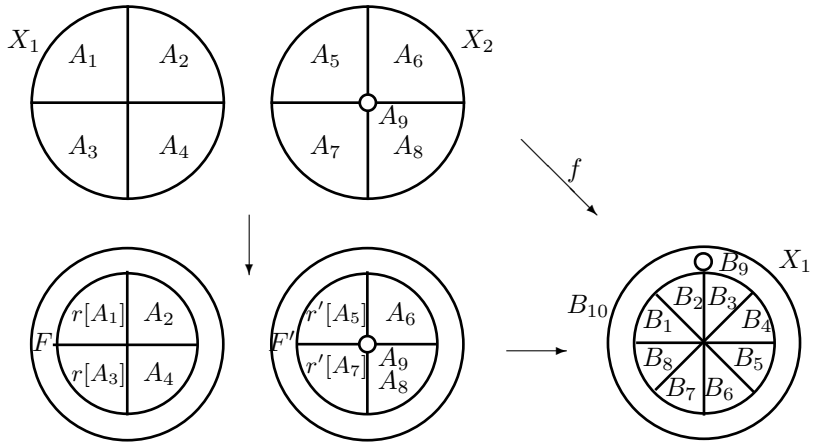
$$X_2 \setminus F' = r'[A_5] \cup A_6 \cup r'[A_7] \cup A_8,$$

con $r'[A_5] \cup A_6 = C'$, $r'[A_7] \cup A_8 = \tau[D']$, por lo que, si definimos

$$B_5 = T^{-1}[r[A_5]], \quad B_6 = T^{-1}[A_6],$$

$$B_7 = T^{-1}[\tau^{-1}[r'[A_7]]], \quad B_8 = T^{-1}[\tau^{-1}[A_8]],$$

se cumple que $B_5 \cup B_6 \cup B_7 \cup B_8 = C \cup D$. La figura siguiente resume la situación junto con una pequeña variante:



En X_1 modificamos la definición de cualquiera de los conjuntos, por ejemplo A_1, para que incluya el punto O. Así sigue siendo cierto que al aplicar r obtenemos una partición de $X_1 \setminus F$ con O incluido en $r[A_1]$. En cambio en X_2 consideramos un conjunto $A_9 = \{O'\}$, que dejamos invariante al aplicar r', pero luego, para que O' y O no tengan la misma imagen, enviamos O' a un punto cualquiera $O'' \in F$, de modo que $B_9 = \{O''\}$ y B_{10} es el complementario de la unión de todos los B_i, para $i = 1, \ldots 9$.

En resumen, hemos definido una aplicación $f : X \longrightarrow X_1$ de modo que

$$X = A_1 \cup \cdots \cup A_9$$

y cada restricción $f|_{A_i} : A_i \longrightarrow B_i$ es un movimiento (una composición de giros y traslaciones). Esto ya es casi la paradoja de Banach-Tarski, salvo por el hecho de que la imagen de los nueve trozos en que hemos partido las dos esferas no cubre toda la esfera, sino que queda un trozo B_{10} sin cubrir.

Para arreglar esto consideramos la inclusión $g : X_1 \longrightarrow X$. En [Al B.10] probamos el teorema de Cantor-Bernstein, que a partir de dos aplicaciones inyectivas $f : X \longrightarrow X_1$, $g : X_1 \longrightarrow X$ nos construye una biyección $h : X \longrightarrow X_1$. Esta biyección se obtiene construyendo primero un conjunto $z \subset X$ tal que $X \setminus z = g[X_1 \setminus f[z]]$. En particular

$$X \setminus z \subset g[X_1] = A_1 \cup A_2 \cup A_3 \cup A_4,$$

luego

$$A_5 \cup A_6 \cup A_7 \cup A_8 \cup A_9 \subset z,$$

luego, aplicando f,

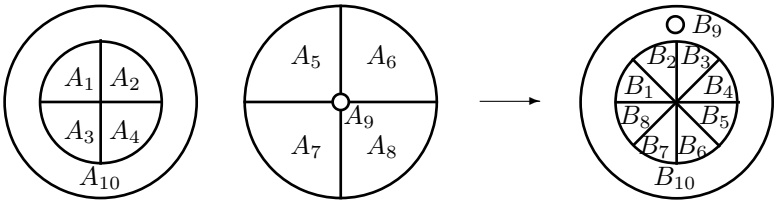
$$B_5 \cup B_6 \cup B_7 \cup B_8 \cup B_9 \subset f[z],$$

luego

$$X_1 \setminus f[z] \subset B_1 \cup B_2 \cup B_3 \cup B_4 \cup B_{10}.$$

Más aún, $B_{10} \subset X_1 \setminus f[z]$, pues B_{10} no corta a la imagen de f.

Vamos a llamar $A_{10} = X \setminus z$ y, para cada $i = 1, \ldots, 4$, redefinimos A_i como $A_i \setminus A_{10}$, de modo que seguimos teniendo una partición $X = A_1 \cup \cdots \cup A_{10}$. Igualmente, redefinimos $B_{10} = X_1 \setminus f[z]$ y, para $i = 1, 2, 3, 4$, redefinimos cada B_i como $B_i \setminus B_{10}$, de modo que seguimos teniendo una partición $X_1 = B_1 \cup \cdots \cup B_{10}$.



Así $A_{10} = g[B_{10}]$ (lo que significa simplemente que $A_{10} = B_{10}$, pues g es la inclusión) y, por otra parte, con las nuevas definiciones, $f[X \setminus A_{10}] = X_1 \setminus B_{10}$, luego, para $i = 1, 2, 3, 4$, si f transformaba el antiguo A_i en el antiguo B_i ahora transforma $A_i \setminus A_{10}$ (el nuevo A_i) en $B_i \setminus B_{10}$ (el nuevo B_i), luego con las nuevas definiciones sigue siendo cierto que $f[A_i] = B_i$, para $i = 1, \ldots, 4$, luego de hecho para $i = 1, \ldots, 9$ y, redefiniendo $f|_{A_{10}}$ como g^{-1} (es decir, como la identidad), tenemos una biyección $f : X \longrightarrow X_1$ con la propiedad de que

$$X = A_1 \cup \cdots \cup A_{10}, \qquad X_1 = B_1 \cup \cdots \cup B_{10}, \qquad f[A_i] = B_i$$

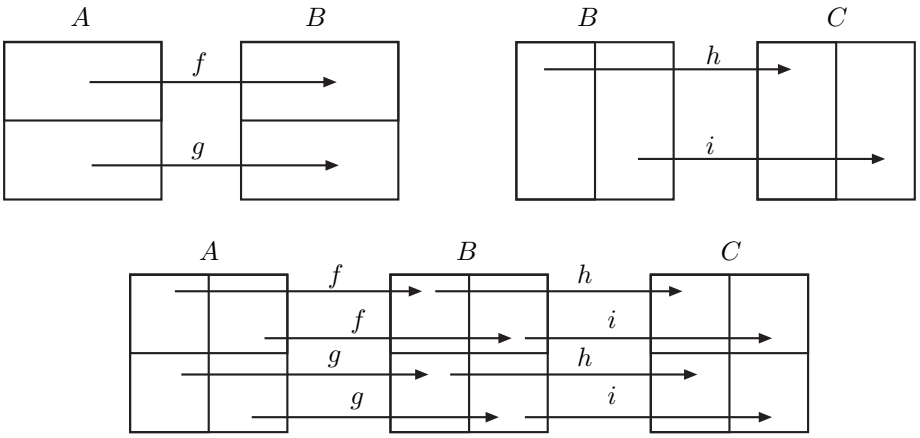
y las restricciones $f|_{A_i} : A_i \longrightarrow B_i$ son movimientos. Considerando f^{-1} y renumerando los conjuntos, hemos probado:

Teorema A.1 (Paradoja de Banach-Tarski) *Es posible dividir una esfera (sólida) B en 10 subconjuntos disjuntos dos a dos, $B = B_1 \cup \cdots \cup B_{10}$, de modo que, aplicando movimientos a los conjuntos B_i, obtenemos otros conjuntos A_i, también disjuntos dos a dos, tales que $A_1 \cup \cdots \cup A_5$ y $A_6 \cup \cdots \cup A_{10}$ son dos esferas del mismo radio que la esfera inicial.*

Es posible probar que bastan cinco piezas, es decir, que una esfera puede partirse en cinco piezas de modo que, reordenando dos de ellas se obtiene una esfera igual a la inicial y, reordenando las otras tres, también, pero con cuatro piezas no es posible.

Más en general, se dice que dos subconjuntos A y B de $\mathbb{R}^3$ son *congruentes* si existe un movimiento que transforma uno en otro y son *congruentes a trozos* si pueden dividirse en un número finito de partes congruentes entre sí. Lo representaremos por $A \sim B$. Hemos probado que una bola cerrada es congruente a trozos con dos bolas disjuntas del mismo radio.

No es difícil probar que la congruencia a trozos es una relación de equivalencia. Lo único que no es inmediato es la transitividad. La figura siguiente esboza la demostración:



Es claro que si $A \sim B$, $A' \sim B'$ y $A \cap A' = B \cap B' = \varnothing$, entonces $A \cup A' \sim B \cup B'$.

Escribiremos $A \preceq B$ para indicar que el conjunto A es congruente a trozos con un subconjunto de B. Es fácil ver que si $A \preceq B \preceq C$, entonces $A \preceq C$. Vamos a probar que si $A \preceq B$ y $B \preceq A$, entonces $A \sim B$.

Tenemos aplicaciones inyectivas $f : A \longrightarrow B$ y $g : B \longrightarrow A$ que son movimientos a trozos, es decir, A está dividido en un número finito de partes y la restricción de f a cada una de ellas es un movimiento. Igualmente con g. Según hemos visto, existe un subconjunto Z de A tal que $g[B \setminus f[Z]] = A \setminus Z$. Claramente, tenemos que $Z \sim f[Z]$ y $B \setminus f[Z] \sim g[B \setminus f[Z]] = A \setminus Z$, luego

$$A = Z \cup (A \setminus Z) \sim f[Z] \cup (B \setminus f[Z]) = B.$$

Teorema A.2 *Una bola cerrada es congruente a trozos con cualquier unión finita de bolas del mismo radio, no necesariamente disjuntas.*

Demostración: Si vale para n bolas, sea B una bola, sea C una unión de n bolas y D otra bola, todas del mismo radio. Tomemos aparte dos bolas

disjuntas B_1 y B_2. Entonces, por hipótesis de inducción, $C \sim B_1$ y $C \setminus D \preceq B_2$. Como son disjuntos,

$$C \cup D \preceq B_1 \cup B_2 \sim B \sim D \preceq C \cup D.$$

Consecuentemente $B \sim C \cup D$, que es una unión de $n+1$ bolas. ∎

De aquí deducimos un resultado general sobre congruencia a trozos:

Teorema A.3 *Si A y A' son subconjuntos de $\mathbb{R}^3$ acotados y de interior no vacío, entonces son congruentes a trozos.*

DEMOSTRACIÓN: A y A' contienen sendas bolas cerradas del mismo radio r, digamos B y B'. Por compacidad, A puede ser cubierto por un número finito de bolas del mismo radio. Sea C dicha unión finita. Sabemos que $B \preceq A \preceq C \sim B$, luego $A \sim B$, y análogamente $A' \sim B' \sim B \sim A$. ∎

Así pues, es posible dividir en un número finito de trozos una bola del tamaño de la Tierra, reordenar los trozos y obtener una bola del tamaño del Sol.

A.2 Medidas finitamente aditivas

Recordemos [An 4.5] que si X es un conjunto, un *anillo* de subconjuntos de X es una familia $\mathcal{A} \subset \mathcal{P}X$ que cumpla las propiedades siguientes:

1. $\varnothing \in \mathcal{A}$.
2. Si $A, B \in \mathcal{A}$, entonces $A \cup B, A \cap B, A \setminus B \in \mathcal{A}$.

Si además cumple $X \in \mathcal{A}$, entonces es un *álgebra* de subconjuntos de X. (Es fácil ver que esta definición equivale a la dada en [An 4.21].)

Es inmediato que si $Y \subset \mathcal{P}X$, la intersección de todas las álgebras de subconjuntos de X que contienen a Y es un álgebra de subconjuntos de X, que recibe el nombre de *álgebra generada* por Y, y se representa por $\langle Y \rangle$.

Teorema A.4 *Si $Y \subset \mathcal{P}X$, el álgebra $\langle Y \rangle$ está formada por los elementos de la forma:*

$$\bigcup_{i=1}^{n} \bigcap_{j=1}^{k_i} A_{ij}, \quad \textit{con} \qquad A_{ij} \in Y \quad \textit{o bien} \quad X \setminus A_{ij} \in Y.$$

DEMOSTRACIÓN: Sea $\mathcal{B}$ la familia de los subconjuntos de X de la forma indicada. Es claro que $\mathcal{B} \subset \langle Y \rangle$, luego basta probar que $\mathcal{B}$ es un álgebra de subconjuntos de X, y así tendremos la inclusión opuesta. Lo probamos en varios pasos. El primero es inmediato:

1. *Si $B \in \mathcal{B}$ y $A \in Y$ o $X \setminus A \in Y$, entonces $A \cap B \in \mathcal{B}$.*

2. *Si A, $B \in \mathcal{B}$, entonces $A \cap B \in \mathcal{B}$.*

   En efecto, si $B = \bigcup_{i=1}^{n} \bigcap_{j=1}^{k_i} A_{ij}$, la propiedad anterior nos da $A \cap A_{i1} \in \mathcal{B}$, de donde a su vez $A \cap A_{i1} \cap A_{i2} \in \mathcal{B}$ y, en definitiva, $A \cap \bigcap_{j=1}^{k_i} x_{ij} \in \mathcal{B}$. Pero es inmediato que la unión de un número finito de elementos de $\mathcal{B}$ está en $\mathcal{B}$, luego de aquí concluimos que $A \cap B \in \mathcal{B}$.

3. *Si $A \in \mathcal{B}$, entonces $X \setminus A \in \mathcal{B}$.*

   En efecto, si $A = \bigcup_{i=1}^{n} \bigcap_{j=1}^{k_i} A_{ij}$, entonces $X \setminus A = \bigcap_{i=1}^{n} \bigcup_{j=1}^{k_i} (X \setminus A_{ij})$ que es una intersección de elementos de $\mathcal{B}$, luego está en $\mathcal{B}$ por la propiedad anterior.

∎

Como consecuencia:

Teorema A.5 *Si un álgebra de subconjuntos de X admite un generador finito, entonces es finita.*

Si $\mathcal{A}$ es un anillo de subconjuntos de X, un *átomo* en $\mathcal{A}$ es un conjunto $A \in \mathcal{A}$ no vacío tal que ningún subconjunto propio no vacío de A está en $\mathcal{A}$. Si $\mathcal{A} \neq \{\varnothing\}$ es finito, es inmediato que todo elemento de $\mathcal{A}$ no vacío contiene un átomo. Más aún, cada $A \in \mathcal{A}$ es la unión de los átomos que contiene, pues si llamamos A_0 a dicha unión, se cumple que $A_0 \subset A$, y si la inclusión fuera estricta $A \setminus A_0$ contendría un átomo, y tenemos una contradicción.

Notemos además que los átomos son disjuntos dos a dos, pues si A, B son átomos y $A \cap B \neq \varnothing$, necesariamente $A = A \cap B = B$.

Teorema A.6 (AE) *Si $\mathcal{A}$ es un anillo de subconjuntos de X, toda medida finitamente aditiva en $\mathcal{A}$ se extiende a una medida finitamente aditiva en $\mathcal{P}X$.*

Demostración: Probemos en primer lugar que si $\mathcal{A} \subset \mathcal{B}$ y $\mathcal{B}$ es un álgebra finita de subconjuntos de X, toda medida[2] finitamente aditiva $\mu : \mathcal{A} \longrightarrow [0, +\infty]$ se extiende a $\mathcal{B}$.

Sea $\mathrm{At}(\mathcal{A})$ el conjunto de todos los átomos de $\mathcal{A}$, de modo que todo elemento no vacío de $\mathcal{A}$ se expresa de forma única como unión de átomos (la unión de los átomos que contiene, que son disjuntos dos a dos, luego no podemos eliminar ninguno). Sea $\mathrm{At}(\mathcal{B})$ el conjunto de los átomos de $\mathcal{B}$, de modo que cada átomo $A \in \mathrm{At}(\mathcal{A})$ se expresa en forma única como unión de átomos de $\mathrm{At}(\mathcal{B})$. Como los átomos de $\mathcal{A}$ son disjuntos dos a dos, un mismo átomo de $\mathcal{B}$ no está contenido en dos átomos de $\mathcal{A}$.

Para cada $A \in \mathrm{At}(\mathcal{A})$ elegimos un átomo $A_0 \in \mathrm{At}(\mathcal{B})$ tal que $A_0 \subset A$ y definimos $\bar{\mu}(A_0) = \mu(A)$, y $\bar{\mu}(A') = 0$, para todo $A' \in \mathrm{At}(\mathcal{B})$ que no sea de la forma A_0, para cierto $A \in \mathrm{At}(\mathcal{A})$.

[2]Notemos que en [An 4.7] considerábamos medida finitamente aditivas $\mu : \mathcal{A} \longrightarrow [0, +\infty[$, mientras que aquí estamos admitiendo que las medidas tomen el valor ∞, lo cual requiere los mismos convenios que en [An 4.19] sobre sumas con sumandos infinitos.

Es claro entonces que si, para cada $B \in \mathcal{B}$, definimos $\bar{\mu}(B)$ como la suma de las medidas de los átomos que contiene, tenemos una medida finitamente aditiva en $\mathcal{B}$ que extiende a μ.

Consideremos ahora un anillo arbitrario $\mathcal{A}$ de subconjuntos de X con una medida finitamente aditiva $\mu : \mathcal{A} \longrightarrow [0, +\infty]$, y sea $P = [0, +\infty]^{\mathcal{P}X}$ considerado como espacio topológico con la topología producto, que es un espacio compacto por el teorema de Tychonoff [An 3.8].

Para cada álgebra finita $\mathcal{B}$ de subconjuntos de X consideramos el conjunto

$$C(\mathcal{B}) = \{\nu \in P \mid \nu|_{\mathcal{B}} \text{ es una medida f.a. que extiende a } \mu|_{\mathcal{A}\cap\mathcal{B}}\}.$$

Observemos que es cerrado, pues si $\nu \in X \setminus C(\mathcal{B})$, o bien $\nu|_{\mathcal{B}}$ no es una medida finitamente aditiva, o bien no extiende a $\mu|_{\mathcal{A}\cap\mathcal{B}}$. En el segundo caso, esto significa que existe un $A \in \mathcal{A}\cap\mathcal{B}$ tal que $\nu(A) \neq \mu(A)$. Entonces el conjunto

$$U = \{\nu \in P \mid \nu(A) \in [0, +\infty] \setminus \{\mu(A)\}\}$$

es abierto en P y $\nu \in U \subset P \setminus C(\mathcal{B})$, pues toda medida $\nu' \in U$ cumple que $\nu'(A) \neq \mu(A)$.

Si el problema es que $\nu|_{\mathcal{B}}$ no es una medida finitamente aditiva, esto puede deberse a que $\nu(\varnothing) \neq 0$ (en cuyo caso no extiende a $\mu|_{\mathcal{A}\cap\mathcal{B}}$, luego ya hemos tratado esta posibilidad) o bien existen A, $B \in \mathcal{B}$ tales que $A \cap B = \varnothing$ pero $\nu(A \cup B) \neq \nu(A) + \nu(B)$.

Por la propiedad de Hausdorff existen abiertos disjuntos V_1, V_2 en $[0, +\infty]$ tales que $\nu(A \cup B) \in V_1$, $\nu(A) + \nu(B) \in V_2$. La suma

$$f : [0, +\infty] \times [0, +\infty] \longrightarrow [0, +\infty]$$

es una aplicación continua, luego existe un entorno de $(\nu(A), \nu(B))$, que podemos tomar de la forma $U_1 \times U_2$, tal que $(\nu(A), \nu(B)) \in U_1 \times U_2 \subset f^{-1}[V_2]$. El conjunto

$$W = \{\nu \in P \mid \nu(A) \in U_1,\ \nu(B) \in U_2,\ \nu(A \cup B) \in V_1\}$$

es un abierto básico en el producto X y se cumple que $\nu \in W \subset P \setminus C(\mathcal{B})$, pues cualquier $\nu' \in W$ cumple que $\nu'(A \cup B) \neq \nu'(A) + \nu'(B)$.

En ambos casos hemos llegado a que $X \setminus C(\mathcal{B})$ es entorno de ν, luego es abierto y $C(\mathcal{B})$ es cerrado. Además es no vacío, pues hemos probado que $\mu|_{\mathcal{A}\cap\mathcal{B}}$ admite una extensión a $\mathcal{B}$, que a su vez puede extenderse a $C(\mathcal{B})$ sin más que darle el valor 0 fuera de $\mathcal{B}$.

La familia de cerrados $C(\mathcal{B})$, cuando $\mathcal{B}$ recorre las álgebras finitas de subconjuntos de X, tiene la propiedad de la intersección finita, pues si $\mathcal{B}_1, \ldots, \mathcal{B}_n$ son álgebras finitas de subconjuntos de X, el álgebra $\mathcal{B}$ generada por ellas es finita, por el teorema A.5, y claramente $C(\mathcal{B}) \subset C(\mathcal{B}_1) \cap \cdots \cap C(\mathcal{B}_n)$. Por la compacidad de X concluimos que existe $\bar{\mu} \in \bigcap_{\mathcal{B}} C(\mathcal{B})$, donde $\mathcal{B}$ recorre las álgebras finitas de subconjuntos de X, y dicha $\bar{\mu}$ es la extensión buscada.

Por ejemplo, para probar que es una medida finitamente aditiva tomamos A, $B \in \mathcal{P}X$ tales que $A \cap B = \varnothing$ y consideramos el álgebra $\mathcal{B}$ generada por A y B, que es finita. Como $\bar{\mu} \in C(\mathcal{B})$, resulta que $\bar{\mu}|_{\mathcal{B}}$ es una medida finitamente aditiva, luego $\bar{\mu}(A \cup B) = \bar{\mu}(A) + \bar{\mu}(B)$. Igualmente se comprueba que $\bar{\mu}(\varnothing) = 0$. ∎

Así pues, la medida de Lebesgue en $\mathbb{R}^n$ se extiende a una medida finitamente aditiva en $\mathcal{P}\mathbb{R}^n$. Pero vamos a demostrar más todavía, y es que la extensión puede tomarse invariante por traslaciones. Para ello necesitamos definir la integral asociada a una medida finitamente aditiva.

Definición A.7 Sea X un conjunto y sea $B(X)$ el conjunto de todas las funciones $f : X \longrightarrow \mathbb{R}$ acotadas, es decir, tales que existe un $M > 0$ de modo que $f[X] \subset [-M, M]$. Podemos considerar a $B(X)$ como anillo con la suma dada por $(f + g)(x) = f(x) + g(x)$ y el producto dado por $(fg)(x) = f(x)g(x)$. A su vez, $\mathbb{R}$ se identifica con un subcuerpo de $B(X)$ sin más que identificar cada número real α con la función que toma constantemente el valor α.

Consideramos en $B(X)$ la relación de orden parcial dada por $f \leq g$ si para todo $x \in X$ se cumple que $f(x) \leq g(x)$.

Una *función simple* es una función $f \in B(X)$ que toma un número finito de valores.

Si llamamos $\alpha_1, \ldots, \alpha_n$ a los valores no nulos que toma f y $X_i = f^{-1}[\alpha_i]$, entonces $f = \sum_{i=1}^{n} \alpha_i \operatorname{car} X_i$, donde $\operatorname{car} X_i$ a la función característica de X_i, es decir, la función dada por

$$\operatorname{car} X_i(x) = \begin{cases} 1 & \text{si } x \in X_i, \\ 0 & \text{si } x \notin X_i. \end{cases}$$

y la expresión es única si exigimos que los conjuntos X_i sean disjuntos y los α_i distintos dos a dos. Recíprocamente, toda función de esta forma es simple.

Definición A.8 Sea X un conjunto y μ una medida unitaria y finitamente aditiva en $\mathcal{P}X$. Para cada función simple $s = \sum_{i=1}^{n} \alpha_i \operatorname{car} X_i$, definimos su *integral* respecto de μ como

$$\int s \, d\mu = \sum_{i=1}^{n} \alpha_i \mu(X_i).$$

Teorema A.9 *Sea X un conjunto, μ una medida unitaria y finitamente aditiva en $\mathcal{P}X$, sean s, t funciones simples y α, $\beta \in \mathbb{R}$. Entonces*

$$\int (\alpha f + \beta g) \, d\mu = \alpha \int f \, d\mu + \beta \int g \, d\mu.$$

Demostración: Sean $s = \sum_{i=1}^{n} \alpha_i \operatorname{car} X_i$, $t = \sum_{j=1}^{m} \beta_j \operatorname{car} Y_j$. Llamamos $X_{ij} = X_i \cap Y_j$ y completamos estos conjuntos con

$$X_{i0} = X_i \setminus \bigcup_{j=1}^{m} Y_j, \qquad X_{0j} = Y_j \setminus \bigcup_{i=1}^{n} X_i, \qquad X_{00} = \varnothing.$$

Así, conviniendo además en que $\alpha_0 = \beta_0 = 0$:

$$\alpha s + \beta t = \sum_{i=0}^{n}\sum_{j=0}^{m} \alpha\alpha_i \operatorname{car} X_{ij} + \sum_{j=0}^{m}\sum_{i=0}^{n} \beta\beta_j \operatorname{car} X_{ij} = \sum_{ij}(\alpha\alpha_i + \beta\beta_j)\operatorname{car} X_{ij},$$

luego

$$\int (\alpha s + \beta t)\, d\mu = \sum_{i,j}(\alpha\alpha_i + \beta\beta_j)\,\mu(X_{ij}) = \alpha\sum_{i,j}\alpha_i\mu(X_{ij}) + \beta\sum_{i,j}\beta_j\mu(X_{ij})$$

$$= \alpha\sum_{i=1}^{n}\alpha_i\sum_{j=0}^{m}\mu(X_{ij}) + \beta\sum_{j=1}^{m}\beta_j\sum_{i=0}^{n}\mu(X_{ij}) = \alpha\sum_{i=1}^{n}\alpha_i\mu(X_i) + \beta\sum_{j=1}^{m}\beta_j\mu(Y_j)$$

$$= \alpha\int s\, d\mu + \beta\int t\, d\mu. \qquad \blacksquare$$

Observemos que si una función simple cumple $s \geq 0$, entonces, por la propia definición de integral tenemos que $\int s\, d\mu \geq 0$, luego si $s \leq t$, se cumple que $t - s \geq 0$ (y es una función simple, porque toma un número finito de valores), luego $\int t\, d\mu - \int s\, d\mu \geq 0$, luego $\int s\, d\mu \leq \int t\, d\mu$.

Definición A.10 Sea X un conjunto y μ una medida unitaria y finitamente aditiva en $\mathcal{P}X$. Si $f \in B(X)$, definimos

$$\int f\, d\mu = \sup\{\int s\, d\mu \mid s \in B(X),\ s \text{ es una función simple y } s \leq f\}.$$

Notemos que, como f está acotada, digamos $-M \leq f \leq M$, siempre existe una función simple $M \operatorname{car} X \leq f$.

La observación previa a la definición implica que si f es simple esta integral coincide con la que ya teníamos definida.

Teorema A.11 *Si $f \in B(X)$ y $\epsilon > 0$, existe una función simple $s \leq f$ tal que $f - s \leq \epsilon$.*

Demostración: Pongamos que $f[X] \subset [a, b[$ y consideremos un número natural N tal que $(b-a)/N < \epsilon$. Entonces los conjuntos

$$Y_n = \left[a + \frac{n(b-a)}{N}, a + \frac{(n+1)(b-a)}{N}\right[,$$

para $n < N$ forman una partición de $[a, b[$, luego los conjuntos $X_n = f^{-1}[Y_n]$ forman una partición de X y la función

$$s = \sum_{n<N}\left(a + \frac{n(b-a)}{N}\right)\operatorname{car} X_n$$

cumple lo pedido. $\blacksquare$

Observemos que, en las condiciones del teorema y de la definición anterior,

$$\int f\,d\mu - \int s\,d\mu \le \epsilon.$$

En efecto, si $u \le f$ es una función simple, entonces $u - s \le f - s \le \epsilon$, luego

$$\int u\,d\mu - \int s\,d\mu \le \int u - s\,d\mu \le \int \epsilon\,d\mu = \epsilon,$$

luego $\int u\,d\mu \le \int s\,d\mu + \epsilon$ y, tomando supremos $\int f\,d\mu \le \int s\,d\mu + \epsilon$.

Teorema A.12 *En las condiciones de la definición* A.10, *si* f, $g \in B(X)$, *entonces*

$$\int (f+g)\,d\mu = \int f\,d\mu + \int g\,d\mu.$$

Demostración: Dado $\epsilon > 0$, sean $s \le f$, $t \le g$ funciones simples tales que $f - s \le \epsilon/4$, $f - g \le \epsilon/4$, de donde a su vez $(f+g) - (s+t) \le \epsilon/2$. Por la observación precedente al teorema

$$\left|\int f+g\,d\mu - \int f\,d\mu - \int g\,d\mu\right| \le \left|\int f+g\,d\mu - \int s+t\,d\mu\right|$$

$$+\left|\int f\,d\mu - \int s\,d\mu\right| + \left|\int g\,d\mu - \int t\,d\mu\right| \le \frac{\epsilon}{2} + \frac{\epsilon}{4} + \frac{\epsilon}{4} = \epsilon.$$

Como esto vale para todo $\epsilon > 0$, tiene que darse la igualdad del enunciado. ∎

Éstas son las únicas propiedades que vamos a necesitar de la integral que hemos construido:

Teorema A.13 *Sea* X *un conjunto,* μ *una medida unitaria finitamente aditiva en* $\mathcal{P}X$, f, $g \in B(X)$ *y* α, $\beta \in \mathbb{R}$. *Entonces*

1. $\displaystyle\int (\alpha f + \beta g)\,d\mu = \alpha \int f\,d\mu + \beta \int g\,d\mu.$
2. *Si* $f \ge 0$ *entonces* $\displaystyle\int f\,d\mu \ge 0.$
3. $\displaystyle\int \operatorname{car} X\,d\mu = 1.$

Demostración: Observemos en primer lugar que si $f \le g$, entonces toda $s \le f$ simple cumple $s \le g$, luego $\int s\,d\mu \le \int g\,d\mu$, luego $\int f\,d\mu \le \int g\,d\mu$.

a) Por el teorema anterior, basta probar que

$$\int \alpha f\,d\mu = \alpha \int f\,d\mu.$$

Vamos a suponer que $\alpha < 0$, pues el caso $\alpha > 0$ es más sencillo. Si $s \leq f$ es una función simple, entonces $\alpha s \geq \alpha f$, luego, por la monotonía que hemos probado al principio de la prueba $\alpha \int s\,d\mu = \int \alpha s\,d\mu \geq \int \alpha f\,d\mu$, luego

$$\int s\,d\mu \leq \frac{1}{\alpha}\int \alpha f\,d\mu,$$

y esto vale para toda $s \leq f$ simple, luego

$$\int f\,d\mu \leq \frac{1}{\alpha}\int \alpha f\,d\mu,$$

luego $\alpha \int f\,d\mu \geq \int \alpha f\,d\mu$. Ahora, si $s \leq \alpha f$ es una función simple, entonces $(1/\alpha)s \geq f$, luego

$$\frac{1}{\alpha}\int s\,d\mu \geq \int f\,d\mu, \quad \text{luego} \quad \int s\,d\mu \leq \alpha \int f\,d\mu,$$

y esto para todo $s \leq \alpha f$ simple, luego $\int \alpha f\,d\mu \leq \alpha \int f\,d\mu$.

b) Como $0 = \operatorname{car} \varnothing$ es una función simple, si $f \geq 0$, por la propia definición de integral $0 = \int \operatorname{car} \varnothing\,d\mu \leq \int f\,d\mu$.

c) Por definición de integral de una función simple $\int \operatorname{car} X\,d\mu = \mu(X) = 1$. ∎

La medida de Lebesgue en $\mathbb{R}^n$ es invariante por isometrías. Ahora vamos a estudiar si las extensiones proporcionadas por el teorema A.6 pueden tomarse invariantes por traslaciones, o por isometrías en general. Para ello introducimos un concepto general de invarianza de medidas:

Definición A.14 Si $\mathcal{A}$ es un anillo de subconjuntos de X y G es un grupo que actúa sobre X, diremos que $\mathcal{A}$ es *G-invariante* si para todo $A \in \mathcal{A}$ y todo $g \in G$ se cumple que $g[A] \in \mathcal{A}$. Si $\mu : \mathcal{A} \longrightarrow [0, +\infty]$ es una medida finitamente aditiva, diremos que es *G-invariante* si para todo $A \in \mathcal{A}$ y todo $g \in G$ se cumple que $\mu(g[A]) = \mu(A)$.

Por ejemplo, si $\mathcal{A}$ es el álgebra de los subconjuntos medibles Lebesgue de $\mathbb{R}^n$ y G es el grupo de las isometrías de R^n, entonces G actúa sobre $\mathbb{R}^n$ y la medida de Lebesgue es G-invariante.

Si la medida dada en el teorema A.6 es G invariante para cierto grupo G, vamos a probar que una condición suficiente para que admita una extensión G-invariante es que la propia álgebra $\mathcal{P}G$ admita una medida G-invariante respecto de la acción de G en $\mathcal{P}G$ dada por $A \mapsto Ag$. Específicamente:

Definición A.15 Un grupo G es *medible* si existe una medida unitaria finitamente aditiva $\mu : \mathcal{P}G \longrightarrow [0, 1]$ que sea *G-invariante por la derecha,* es decir, tal que para todo $A \in \mathcal{P}G$ se cumpla $\mu(Ag) = \mu(A)$.

El teorema siguiente prueba que la invarianza de una medida se traduce a una propiedad de invarianza de la integral definida a partir de ella, y será la última propiedad de las integrales que tenemos que demostrar recurriendo a la definición:

Teorema A.16 *Si G es un grupo y μ es una medida unitaria finitamente aditiva en $\mathcal{P}G$ que es G-invariante por la derecha, entonces, para toda $f \in B(G)$ y todo $g \in G$ se cumple que*

$$\int f_g \, d\mu = \int f \, d\mu,$$

donde $f_g(h) = f(hg^{-1})$.

DEMOSTRACIÓN: Veámoslo primero para funciones de la forma $\operatorname{car} A$, con $A \in \mathcal{P}G$. Se comprueba inmediatamente que $(\operatorname{car} A)_g = \operatorname{car} Ag$, luego

$$\int (\operatorname{car} A)_g \, d\mu = \mu(Ag) = \mu(A) = \int \operatorname{car} A \, d\mu.$$

Si $s = \sum_{i=1}^{n} \alpha_i \operatorname{car} A_i$ es una función simple, entonces $s_g = \sum_{i=1}^{n} \alpha_i (\operatorname{car} A_i)_g$ y el caso probado para funciones características implica inmediatamente el caso para funciones simples.

Por último, si $s \le f$, entonces $s_g \le f_g$, luego $\int s \, d\mu = \int s_g \, d\mu \le \int f_g \, d\mu$, luego

$$\int f \, d\mu \le \int f_g \, d\mu.$$

Recíprocamente, si $s \le f_g$, es claro que $s_{g^{-1}} \le (f_g)_{g^{-1}} = f$, luego

$$\int s \, d\mu = \int s_{g^{-1}} \, d\mu \le \int f \, d\mu,$$

luego $\int f_g \, d\mu \le \int f \, d\mu$ y tenemos la igualdad. ∎

Una medida G-invariante por la derecha no tiene por qué serlo por la izquierda, es decir, no tiene por qué cumplir que $\mu(gA) = \mu(A)$, pero a partir de ella podemos obtener otra que sí que lo sea:

Teorema A.17 *Todo grupo medible admite una medida unitaria finitamente aditiva invariante por la izquierda y por la derecha.*

DEMOSTRACIÓN: Sea μ una medida invariante por la derecha. Para cada $A \in \mathcal{P}G$, definimos $f_A \in B(G)$ mediante $f_A(g) = \mu(gA^{-1})$ y $\nu(A) = \int f_A \, d\mu$.

Vamos a probar que ν es una medida invariante por la izquierda y por la derecha. Observemos que $f_\varnothing = 0$ y que $f_G(g) = \mu(gG^{-1}) = \mu(G) = 1$, pues $gG^{-1} = G$, luego $\nu(\varnothing) = 0$ y $\nu(G) = 1$.

Además, si $A \cap B = \varnothing$, tenemos que

$$f_{A\cup B}(g) = \mu(gA^{-1} \cup gB^{-1}) = \mu(gA^{-1}) + \mu(gB^{-1}) = f_A(g) + f_B(g),$$

luego al integrar queda que $\nu(A \cup B) = \nu(A) + \nu(B)$.

Finalmente, $f_{gA}(h) = \mu(hA^{-1}g^{-1}) = \mu(hA^{-1}) = f_A(h)$, luego $f_{gA} = f_A$, mientras que $f_{Ag}(h) = \mu(hg^{-1}A^{-1}) = f_A(hg^{-1}) = (f_A)_g(h)$, luego $f_{Ag} = (f_A)_g$, de donde al integrar queda $\nu(gA) = \nu(A)$ y $\nu(Ag) = \nu(A)$. ∎

Ahora podemos refinar el teorema A.6:

Teorema A.18 (AE) *Si G es un grupo medible que actúa sobre un conjunto X y $\mathcal{A}$ es un anillo G-invariante de subconjuntos de X, entonces toda medida finitamente aditiva y G-invariante en $\mathcal{A}$ se extiende a una medida finitamente aditiva G-invariante en $\mathcal{P}X$.*

Demostración: Sea ν una medida unitaria G-invariante en $\mathcal{P}G$ y sea μ una medida G-invariante en $\mathcal{A}$. Por el teorema A.6 sabemos que μ se extiende a una medida $\bar{\mu}$ en $\mathcal{P}X$.

Para cada $B \in \mathcal{P}X$, sea $f_B : G \longrightarrow [0, +\infty]$ la función dada por $f_B(g) = \bar{\mu}(g^{-1}[B])$. Definimos $\mu^* : \mathcal{P}X \longrightarrow [0, +\infty]$ mediante

$$\mu^*(B) = \begin{cases} \displaystyle\int f_B \, d\nu & \text{si } f_B \in B(G), \\ +\infty & \text{si } f_B \notin B(G). \end{cases}$$

Vamos a probar que se trata de una medida finitamente aditiva G-invariante que extiende a μ.

En primer lugar, $f_\varnothing(g) = \bar{\mu}(g^{-1}[\varnothing]) = \bar{\mu}(\varnothing) = 0$, luego $\mu^*(\varnothing) = 0$. Si $B \cap C = \varnothing$, entonces

$$f_{B\cup C}(g) = \bar{\mu}(g^{-1}[B] \cup g^{-1}[C]) = \bar{\mu}(g^{-1}[B]) + \bar{\mu}(g^{-1}[C]) = f_B(g) + f_C(g),$$

luego $f_{B\cup C} = f_B + f_C$. Si f_B, $f_C \in B(G)$, entonces $f_{B\cup C} \in B(G)$, e integrando obtenemos que $\mu^*(B \cup C) = \mu^*(B) + \mu^*(C)$. En caso contrario $f_{B\cup C} \notin B(G)$ y se cumple la misma igualdad con ambos miembros infinitos. Esto prueba que μ^* es una medida finitamente aditiva.

Si $B \in \mathcal{A}$, entonces $f_B(g) = \mu(g^{-1}[B]) = \mu(B)$, luego

$$\mu^*(B) = \int \mu(B) \, d\nu = \mu(B).$$

Falta probar que μ^* es G-invariante. En efecto:

$$f_{h[B]}(g) = \bar{\mu}(g^{-1}[h[B]]) = f_B(gh^{-1}) = (f_B)_h(g),$$

luego $f_{h[B]} = (f_B)_h$. Si $f_B \in B(G)$, también $f_{h[B]} \in B(G)$ y entonces

$$\mu^*(h[B]) = \int f_{h[B]} \, d\nu = \int (f_B)_h \, d\nu = \int f_B \, d\nu = \mu^*(B).$$

Si $f_B \notin B(G)$ lo mismo vale para $f_{h[B]}$, luego $\mu^*(h[B]) = +\infty = \mu^*(B)$. ∎

Así pues, una condición suficiente para que exista una extensión de la medida de Lebesgue en $\mathbb{R}^n$ a una medida finitamente aditiva en $\mathcal{P}\mathbb{R}^n$ que sea invariante por el grupo de las isometrías de $\mathbb{R}^n$ (o por uno de sus subgrupos G, por ejemplo, el de las traslaciones) es que dicho grupo G sea medible, ya que la medida de Lebesgue es G-invariante. Veamos, pues, algunos resultados que nos permitan estudiar la medibilidad de un grupo dado.

Teorema A.19 (AE) *Sea G un grupo y $\mathcal{F}$ una familia de subgrupos tal que $G = \bigcup \mathcal{F}$ y, para cada H_1, $H_2 \in \mathcal{F}$, existe un $H \in \mathcal{F}$ tal que $H_1 \cup H_2 \subset H$. Si todos los grupos de $\mathcal{F}$ son medibles, entonces G también lo es.*

Demostración: Sea $P = [0,1]^{\mathcal{P}G}$, que es un espacio topológico compacto. Para cada $H \in \mathcal{F}$, sea

$$C(H) = \{\mu \in P \mid \mu \text{ es una medida unitaria finitamente aditiva y si}$$

$$A \in \mathcal{P}G,\ h \in H \text{ entonces } \mu(h[A]) = \mu(A)\}.$$

Se cumple que $C(H) \neq \varnothing$, pues si $\nu : \mathcal{P}H \longrightarrow [0,1]$ es una medida unitaria finitamente aditiva y G-invariante por la derecha, entonces $\mu : \mathcal{P}G \longrightarrow [0,1]$ dada por $\mu(A) = \nu(A \cap H)$ cumple que $\mu \in C(H)$.

La familia de conjuntos $C(H)$ tiene la propiedad de la intersección finita, pues si $H_1, \ldots, H_n \in \mathcal{F}$, existe un $H \in \mathcal{F}$ tal que $H_1 \cup \cdots \cup H_n \subset H$ y

$$\varnothing \neq C(H) \subset C(H_1) \cap \cdots \cap C(H_n).$$

Un argumento similar al empleado en la prueba de A.6 nos da que los conjuntos $C(H)$ son cerrados, luego por compacidad existe $\mu \in \bigcap_{H \in \mathcal{F}} C(H)$.

Es obvio que μ es una medida unitaria finitamente aditiva en G que prueba que G es medible. ∎

Ahora ya podemos demostrar:

Teorema A.20 (AE) *Todo grupo abeliano es medible.*

Demostración: El teorema anterior reduce el problema al caso de grupos abelianos finitamente generados.[3] Sea, pues, $G = \langle X \rangle$ un grupo abeliano con un generador finito $X = \{g_1, \ldots, g_n\}$. Esto significa que

$$G = \{g_1^{k_1} \cdots g_n^{k_n} \mid k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Basta probar que, para cada $\epsilon > 0$, existe una medida unitaria finitamente aditiva $\mu_\epsilon : \mathcal{P}G \longrightarrow [0,1]$ que es casi invariante, en el sentido de que, para todo $A \in \mathcal{P}G$ y cada $i \in \{1, \ldots, n\}$, se cumple que $|\mu_\epsilon(A) - \mu_\epsilon(Ag_i)| < \epsilon$.

En efecto, si existen tales medidas, llamamos $C_\epsilon \subset [0,1]^{\mathcal{P}G}$ al conjunto de todas las medidas μ_ϵ que cumplen las condiciones indicadas. Se comprueba

[3]Los subgrupos de G de la forma $\langle X \rangle$ con X finito cumplen las condiciones de A.19, pues $\langle X \rangle \cup \langle Y \rangle \subset \langle X \cup Y \rangle$.

fácilmente que es cerrado y la familia de todos los conjuntos C_ϵ tiene la propiedad de la intersección finita, pues $\epsilon < \epsilon' \to C_\epsilon \subset C_{\epsilon'}$. Por compacidad podemos tomar $\mu \in \bigcap_{\epsilon>0} C_\epsilon$, que es una medida unitaria G-invariante en $\mathcal{P}G$.

Para construir una medida μ_ϵ tomamos un natural N tal que $2/N < \epsilon$ y, para cada $A \in \mathcal{P}G$, definimos

$$\mu_\epsilon(A) = \frac{|\{(k_1,\dots,k_n) \in \{1,\dots,N\}^n \mid g_1^{k_1}\cdots g_n^{k_n} \in A\}|}{N^n}.$$

Es inmediato que μ_ϵ es una medida unitaria finitamente aditiva y

$$g_1^{k_1}\cdots g_n^{k_n} \in Ag_i \leftrightarrow g_1^{k_1}\cdots g_i^{k_i-1}\cdots g_n^{k_n} \in A,$$

luego $\mu_\epsilon(Ag_i)$ y $\mu_\epsilon(A)$ se diferencian a lo sumo en

$$\frac{|\{(k_1,\dots,k_n) \in \{1,\dots,N\}^n \mid k_i = 1 \text{ o } k_i = N\}|}{N^n} = \frac{2N^{n-1}}{N^n} = \frac{2}{N} < \epsilon.$$

■

Por ejemplo, como el grupo T de las traslaciones de $\mathbb{R}^n$ es abeliano (es isomorfo a $\mathbb{R}^n$) el teorema A.18 aplicado al álgebra $\mathcal{A}$ de los conjuntos medibles Lebesgue y a la medida de Lebesgue $\mu : \mathcal{A} \longrightarrow [0,+\infty]$ (que es T-invariante) nos da que existe una medida finitamente aditiva $m : \mathcal{P}\mathbb{R}^n \longrightarrow [0,+\infty]$ invariante por traslaciones que extiende a la medida de Lebesgue.

No podemos razonar igualmente con el grupo de las isometrías de $\mathbb{R}^n$ porque no es abeliano, pero la clase de los grupos medibles incluye a todos los grupos resolubles:

Teorema A.21 *Se cumplen las propiedades siguientes:*

1. *Todo grupo finito es medible.*
2. *Todo subgrupo de un grupo medible bien ordenable es medible.*
3. *Todo cociente de un grupo medible es medible.*
4. *Si G es un grupo y N es un subgrupo normal tal que tanto N como G/N son medibles, entonces G es medible.*
5. (AE) *Todo grupo resoluble es medible.*

Demostración: a) Si $|G| = n$ basta definir $\mu(A) = |A|/n$ para tener una medida unitaria finitamente aditiva y G-invariante en $\mathcal{P}G$.

b) Sea H un subgrupo de un grupo medible G. Entonces $\{gH \mid g \in G\}$ es una descomposición de G en conjuntos disjuntos dos a dos y podemos tomar un conjunto E que contenga un elemento de cada conjunto gH.

Si $\mu : \mathcal{P}G \longrightarrow [0,1]$ es una medida unitaria finitamente aditiva y G-invariante por la derecha, definimos $\nu : \mathcal{P}H \longrightarrow [0,1]$ mediante $\nu(A) = \mu(\bigcup\{gA \mid g \in E\})$.

Así es claro que ν es una medida finitamente aditiva, unitaria, pues se cumple que $\nu(H) = \mu(G) = 1$, y es H-invariante pues

$$\nu(Ah) = \mu(\{gA \mid g \in G\}h) = \mu(\{gA \mid g \in G\}) = \nu(A).$$

c) Si N es un subgrupo normal en G y μ es como antes, definimos la medida finitamente aditiva $\nu : \mathcal{P}(G/N) \longrightarrow [0,1]$ mediante $\nu(A) = \mu(\bigcup A)$. Es inmediato que cumple lo requerido.

d) Suponemos que tenemos medidas $\mu_s : \mathcal{P}N \longrightarrow [0,1]$, $\mu_c : \mathcal{P}G/N \longrightarrow [0,1]$ para un subgrupo normal y su grupo cociente.

Para cada $A \in \mathcal{P}G$ definimos $f_A : G \longrightarrow \mathbb{R}$ mediante $f_A(g) = \mu_s(N \cap Ag^{-1})$. Así, si $Ng_1 = Ng_2$ entonces $f_A(g_1) = f_A(g_2)$, pues si $g_1g_2^{-1} = n \in N$, entonces

$$\mu_s(N \cap Ag_2^{-1}) = \mu_s(N \cap Ag_1^{-1}n) = \mu_s((N \cap Ag_1^{-1})n) = \mu_s(N \cap Ag_1^{-1}).$$

Por consiguiente, f_A induce una aplicación $f_A : G/N \longrightarrow \mathbb{R}$. Definimos $\mu(A) = \int f_A \, d\mu_c$. Veamos que se trata de una medida finitamente aditiva en $\mathcal{P}G$. Como f_G vale siempre 1, vemos que $\mu(G) = 1$. Si $A, B \in \mathcal{P}G$ son disjuntos, para todo $g \in G$ se cumple que $Ag^{-1} \cap Bg^{-1} = \varnothing$, luego $f_{A\cup B}(g) = f_A(g) + f_B(g)$, de donde se sigue a su vez que $\mu(A \cup B) = \mu(A) + \mu(B)$.

Por último, $f_{Ag}(h) = \mu_s(N \cap Agh^{-1}) = f_A(hg^{-1}) = (f_A)_g(h)$, luego

$$\mu(Ag) = \int (f_A)_g \, d\mu_c = \int f_A \, d\mu_c = \mu(A).$$

Esto prueba que G es medible.

e) Si G es resoluble existe una sucesión

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

tal que todos los cocientes G_i/G_{i-1} son abelianos. El apartado d) y el teorema anterior permiten probar inductivamente que todos los G_i son medibles. ∎

Al final de la sección 4.1 hemos visto que el grupo de las isometrías del plano euclídeo es resoluble, luego es medible por el teorema anterior, y así el teorema A.18 aplicado a la medida de Lebesgue, definida sobre la σ-álgebra $\mathcal{A}$ de los conjuntos medibles Lebesgue en el plano e invariante por isometrías, se extiende a una medida finitamente aditiva $\mu : \mathcal{P}\mathbb{R}^2 \longrightarrow [0, +\infty]$ invariante por isometrías. Esto implica que no existe un análogo en el plano de la paradoja de Banach-Tarski.

Índice de Materias