

Leandro Vendramin

Teoría de grupos

– Primer cuatrimestre de 2021 –

26 de junio de 2021

Prefacio

Estas notas corresponden a un curso dictado el primer cuatrimestre de 2021 en el Departamento de Matemática de la FCEN, Universidad de Buenos Aires.

Quiero agradecer a todas las personas que leyeron las notas y me enviaron correcciones y comentarios. Agradecimientos especialmente van para Carlos Miguel Soto, Martín Mereb, Santiago Varela .

Índice general

Parte I Álgebras semisimples

1. El teorema de Wedderburn	3
2. El radical de Jacobson	13
3. El teorema de Kolchin	17

Parte II Representaciones de grupos

4. El teorema de Maschke	25
5. Representaciones de grupos	31
6. Teoría de caracteres	39
7. El grado de un caracter	47
8. Ejemplos de tablas de caracteres	55
9. Conmutadores	65
10. El teorema de Cauchy-Frobenius-Burnside	71
11. El teorema de Brauer-Fowler	79
12. Inducción y restricción	85
13. El teorema de Frobenius	97
14. Algunos teoremas de Burnside	103
15. Grupos resolubles y teorema de Burnside	107

16. Un teorema de Hurwitz	111
Parte III Teoría de grupos	
17. El teorema de Itô	119
18. El teorema del matrimonio de Hall	121
19. Los teoremas de Hall y Wielandt	125
20. Nilpotencia	131
21. La cantidad de grupos finitos	145
22. El subgrupo de Frattini	151
23. El subgrupo de Fitting	157
24. Super resolubilidad	161
25. Derivaciones	169
26. El teorema de Schur–Zassenhaus	173
27. Extensiones y cohomología	179
28. Teoría de Hall para grupos resolubles	187
29. Sistemas de Sylow	189
30. Subnormalidad	193
31. El teorema de la cremallera	197
32. El subgrupo de Chermak–Delgado	205
33. El morfismo de transferencia	211
34. Un teorema de Schur	215
35. El teorema del complemento normal	219
Referencias	227
Índice alfabético	229

Parte I
Álgebras semisimples

Capítulo 1

El teorema de Wedderburn

Un espacio vectorial A sobre un cuerpo K es un **álgebra** sobre K (o una K -álgebra) si posee una multiplicación asociativa $A \times A \rightarrow A$, $(a, b) \mapsto ab$, tal que $(\lambda a + \mu b)c = \lambda(ac) + \mu(bc)$ y $a(\lambda b + \mu c) = \lambda(ab) + \mu(ac)$ para todo $a, b, c \in A$ y $\lambda, \mu \in K$. Existe además un elemento $1_A \in A$ tal que $1_A a = a 1_A = a$ para todo $a \in A$.

Un álgebra A se dirá **conmutativa** si $ab = ba$ para todo $a, b \in A$.

La **dimensión** de un álgebra A es la dimensión de A como K -espacio vectorial. Justamente esta es quizá una de las claves de la definición, un álgebra es en particular un espacio vectorial y cuando sea necesario podremos utilizar argumentos que involucren el concepto de dimensión.

Ejemplo 1.1. Todo cuerpo K es una K -álgebra.

Ejemplo 1.2. Si K es un cuerpo, $K[X]$ es una K -álgebra.

Similarmente, el anillo de polinomios $K[X, Y]$ y el anillo $K[[X]]$ de series de potencias son ejemplos de álgebras sobre el cuerpo K .

Ejemplo 1.3. Si A es un álgebra, entonces $M_n(A)$ es un álgebra.

Ejemplo 1.4. El conjunto de funciones continuas $[0, 1] \rightarrow \mathbb{R}$ es un álgebra sobre \mathbb{R} con las operaciones usuales, $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$.

Un **morfismo de álgebras** es un morfismo de anillos $f: A \rightarrow B$ que es además una transformación lineal. Observemos que es necesario pedir que un morfismo de álgebras sea una transformación lineal, por ejemplo, la conjugación $\mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto \bar{z}$, es un morfismo de anillos que no es un morfismo de álgebras sobre \mathbb{C} .

Definición 1.5. Un **ideal** de un álgebra es un ideal del anillo que además es un subespacio.

Análogamente se definen ideales a izquierda y a derecha de un álgebra.

Si A es un álgebra, entonces todo ideal a izquierda del anillo A es un ideal a izquierda del álgebra A . Si L es un ideal de A y $\lambda \in K$ y $x \in L$, entonces

$$\lambda x = \lambda(1_A x) = (\lambda 1_A)x$$

y luego, como $\lambda 1_A \in A$, se concluye que $\lambda L = (\lambda 1_A)L \subseteq L$. Análogamente se demuestra que todo ideal a derecha del anillo unitario A es también un ideal de A como álgebra.

Ejercicio 1.6. Demuestre que si A es un álgebra, entonces todo ideal a derecha del anillo A es un ideal a derecha del álgebra A .

Puede demostrarse que si A es un álgebra e I es un ideal de A , entonces el anillo cociente A/I tiene una única estructura de álgebra que hace que el morfismo canónico $A \rightarrow A/I$, $a \mapsto a + I$, sea un morfismo de álgebras.

Ejemplo 1.7. Si $n \in \mathbb{N}$, entonces $K[X]/(X^n)$ es un álgebra de dimensión finita, se conoce como el **álgebra de polinomios truncados**.

Sea A un álgebra. Un elemento $a \in A$ se dice **algebraico** sobre K si existe un polinomio no nulo $f \in K[X]$ tal que $f(a) = 0$. Si todo elemento de A es algebraico, A se dice **algebraica**. Por ejemplo, sabemos que en la \mathbb{Q} -álgebra $A = \mathbb{R}$ el elemento $\sqrt{2}$ es algebraico, pues $\sqrt{2}$ es raíz del polinomio $X^2 - 2 \in \mathbb{Q}[X]$, y que π no lo es. Todo elemento de \mathbb{R} como \mathbb{R} -álgebra es algebraico.

lem:algebraica

Proposición 1.8. Toda álgebra de dimensión finita es algebraica.

Demostración. Sea A un álgebra de dimensión finita n y sea $a \in A$. Como el conjunto $\{1, a, a^2, \dots, a^n\}$ es linealmente dependiente, existe un polinomio no nulo $f \in k[X]$ tal que $f(a) = 0$. \square

Sea A un álgebra de dimensión finita. Observemos que si M es un A -módulo, entonces M es un espacio vectorial con

$$\lambda m = (\lambda 1_A) \cdot m$$

para $\lambda \in K$ y $m \in M$. Además M es finitamente generado si y sólo si M tiene dimensión finita.

Trabajemos con A -módulos finitamente generados.

Observemos que A es un A -módulo con la multiplicación a izquierda, es decir $a \cdot b = ab$, $a, b \in A$. Este módulo se conoce como la **representación regular** de A .

Definición 1.9. Diremos que un A -módulo M es **simple** si $M \neq \{0\}$ y los únicos submódulos de M son $\{0\}$ y M .

Definición 1.10. Diremos que M es **semisimple** si $M \neq \{0\}$ y además M es suma directa de finitos submódulos simples.

La suma directa de módulos semisimples es semisimple.

Lema 1.11 (Schur). Si S y T son A -módulos simples y $f: S \rightarrow T$ es un morfismo no nulo, entonces f es un isomorfismo.

Demostración. Como $f \neq 0$, $\ker f$ es un submódulo propio de S . Como S es simple, entonces $\ker f = \{0\}$. Similarmente $f(S)$ es un submódulo no nulo de T y luego $f(S) = T$ por la simplicidad de T . \square

Proposición 1.12. *Si A es un álgebra de dimensión finita y S es un módulo simple entonces S es de dimensión finita.*

Demostración. Sea $s \in S \setminus \{0\}$. Como S es simple, $\varphi: A \rightarrow S, a \mapsto a \cdot s$, es un epimorfismo. En particular, $A/\ker \varphi \simeq S$ y luego $\dim S = \dim(A/\ker \varphi) \leq \dim A$. \square

Veamos una caracterización de la semisimplicidad.

pro:semisimple

Proposición 1.13. *Sea M un A -módulo de dimensión finita. Las siguientes afirmaciones son equivalentes:*

- 1) M es semisimple.
- 2) $M = \sum_{i=1}^k S_i$, donde los S_i son submódulos simples de M .
- 3) Si S es un submódulo de M , existe un submódulo T de M tal que $M = S \oplus T$.

Demostración. Demostremos que (2) \implies (3). Sea $N \neq \{0\}$ un submódulo de M . Como $N \neq \{0\}$ y $\dim M < \infty$, existe un submódulo no nulo T de M de dimensión maximal tal que $N \cap T = \{0\}$. Si $S_i \subseteq N \oplus T$ para todo $i \in \{1, \dots, k\}$, entonces, como M es suma de los S_i , tenemos $M = N \oplus T$. Si, en cambio, existe algún $i \in \{1, \dots, k\}$ tal que $S_i \not\subseteq N \oplus T$, entonces $S_i \cap (N \oplus T) \subseteq S_i$. Como S_i es simple, se tiene que $S_i \cap (N \oplus T) = \{0\}$. Luego $N \cap (S_i \oplus T) = \{0\}$, una contradicción a la maximalidad de T .

La implicación (1) \implies (2) es trivial.

Veamos ahora que (2) \implies (1). Sea J un subconjunto de $\{1, \dots, k\}$ maximal tal que la suma de los S_j con $j \in J$ es directa. Sea $N = \bigoplus_{j \in J} S_j$. Veamos que $M = N$. Para cada $i \in \{1, \dots, k\}$, se tiene que $S_i \cap N = \{0\}$ o bien que $S_i \cap N = S_i$, pues S_i es simple. Si $S_i \cap N = S_i$ para todo $i \in \{1, \dots, k\}$, entonces $S_i \subseteq N$ para todo $i \in \{1, \dots, k\}$. Si, en cambio, existe $i \in \{1, \dots, k\}$ tal que $S_i \cap N = \{0\}$, entonces N y S_i estarán en suma directa, una contradicción a la maximalidad del conjunto J .

Demostremos por último que (3) \implies (1). Procederemos por inducción en $\dim M$. Si $\dim M = 1$ el resultado es trivial. Si $\dim M \geq 1$, sea S un submódulo no nulo de M de dimensión minimal. En particular, S es simple. Por hipótesis sabemos que existe un submódulo T de M tal que $M = S \oplus T$. Veamos que T verifica la hipótesis. Si X es un submódulo de T , entonces, como en particular T es un submódulo de M , existe un submódulo Y de M tal que $M = X \oplus Y$. Luego

$$T = T \cap M = T \cap (X \oplus Y) = X \oplus (T \cap Y),$$

pues $X \subseteq T$. Como $\dim T < \dim M$ y además $T \cap Y$ es un submódulo de T , la hipótesis inductiva implica que T es suma directa de módulos simples. Luego M también es suma directa de submódulos simples. \square

Proposición 1.14. *Si M es un A -módulo semisimple y N es un submódulo, entonces N y M/N son semisimples.*

Demostración. Supongamos que $M = S_1 + \cdots + S_k$, donde los S_i son submódulos simples. Si $\pi: M \rightarrow M/N$ es el morfismo canónico, el lema de Schur nos dice que cada restricción $\pi|_{S_i}$ es cero o un isomorfismo. Luego

$$M/N = \pi(M) = \sum_{i=1}^k (\pi|_{S_i})(S_i)$$

es también una suma finita de módulos simples. Como además existe un submódulo T tal que $M = N \oplus T$, se tiene que $N \simeq M/T$ es también semisimple. \square

Definición 1.15. Un álgebra A se dirá **semisimple** si todo A -módulo finitamente generado es semisimple.

Proposición 1.16. Sea A un álgebra de dimensión finita. Entonces A es semisimple si y sólo si la representación regular de A es semisimple.

Demostración. Demostremos la implicación no trivial. Sea M un A -módulo finitamente generado, digamos $M = (m_1, \dots, m_k)$. La función

$$\bigoplus_{i=1}^k A \rightarrow M, \quad (a_1, \dots, a_k) \mapsto \sum_{i=1}^k a_i \cdot m_i,$$

es un epimorfismo de A -módulos. Como A es semisimple, $\bigoplus_{i=1}^k A$ es semisimple. Luego M es semisimple por ser isomorfo al cociente de un semisimple. \square

Teorema 1.17. Sea A un álgebra semisimple de dimensión finita. Si ${}_A A = \bigoplus_{i=1}^k S_i$, donde los S_i son submódulos simples y S es un A -módulo simple, entonces $S \simeq S_i$ para algún $i \in \{1, \dots, k\}$.

Demostración. Sea $s \in S \setminus \{0\}$. La función $\varphi: A \rightarrow S, a \mapsto a \cdot s$, es un morfismo de A -módulos sobreyectivo. Como $\varphi \neq 0$, existe $i \in \{1, \dots, k\}$ tal que alguna restricción $\varphi|_{S_i}: S_i \rightarrow S$ es no nula. Por el lema de Schur, $\varphi|_{S_i}$ es un isomorfismo. \square

Como aplicación inmediata tenemos que un álgebra semisimple A de dimensión finita admite, salvo isomorfismo, únicamente finitos módulos simples. Cuando digamos que S_1, \dots, S_k son los simples de A estaremos refiriéndonos a que los S_i son representantes de las clases de isomorfismo de todos los A -módulos simples, es decir que todo simple es isomorfo a alguno de los S_i y además $S_i \not\simeq S_j$ si $i \neq j$.

Si A y B son álgebras, M es un A -módulo y N es un B -módulo, entonces $A \times B$ actúa en $M \oplus N$ por

$$(a, b) \cdot (m, n) = (a \cdot m, b \cdot n).$$

Todo módulo M finitamente generado sobre un anillo de división es libre, es decir posee una base. Tal como pasa en espacios vectoriales, vale además que todo conjunto linealmente independiente de M puede extenderse a una base.

Recordemos que si V es un A -módulo, $\text{End}_A(V)$ se define como el conjunto de morfismos de módulos $V \rightarrow V$. En realidad, $\text{End}_A(V)$ es un álgebra con las operaciones: $(f+g)(v) = f(v) + g(v)$, $(af)(v) = af(v)$ y $(fg)(v) = f(g(v))$ para todo $f, g \in \text{End}_A(V)$, $a \in A$ y $v \in V$.

Lema 1.18. *Sea D un álgebra de división y sea V un D -módulo finitamente generado. Entonces V es un $\text{End}_D(V)$ -módulo simple y además existe $n \in \mathbb{N}$ tal que $\text{End}_D(V) \simeq nV$ es semisimple.*

Demostración. Sea $\{v_1, \dots, v_n\}$ una base de V . La función

$$\text{End}_D(V) \rightarrow \underbrace{V \oplus \dots \oplus V}_{n\text{-veces}}, \quad f \mapsto (f(v_1), \dots, f(v_n)),$$

es un isomorfismo de $\text{End}_D(V)$ -módulos. Luego

$$\text{End}_D(V) \simeq \bigoplus_{i=1}^n V = nV.$$

Falta ver que V es simple. Para eso alcanza con demostrar que $V = (v)$ para todo $v \in V \setminus \{0\}$. Sea $v \in V \setminus \{0\}$. Si $w \in V \setminus \{0\}$, existen w_2, \dots, w_n tal que $\{w, w_2, \dots, w_n\}$ es una base de V . Existe $f \in \text{End}_D(V)$ tal que $f \cdot v = f(v) = w$. En consecuencia, $w \in (v)$ y entonces $V = (v)$. \square

En lenguaje matricial, el lema anterior nos dice que si D es un álgebra de división, entonces D^n es un $M_n(D)$ -módulo simple y que $M_n(D) \simeq nD^n$ como $M_n(D)$ -módulos.

Teorema 1.19. *Sea A un álgebra de dimensión finita y sean S_1, \dots, S_k los representantes de las clases de isomorfismo de los A -módulos simples. Si*

$$M \simeq n_1 S_1 \oplus \dots \oplus n_k S_k,$$

entonces los n_j quedan únivocamente determinados.

Demostración. Como los S_j son módulos simples no isomorfos, el lema de Schur nos dice que si $i \neq j$ entonces $\text{Hom}_A(S_i, S_j) = \{0\}$. Para cada $j \in \{1, \dots, k\}$ tenemos entonces que

$$\text{Hom}_A(M, S_j) \simeq \text{Hom}_A\left(\bigoplus_{i=1}^k n_i S_i, S_j\right) \simeq n_j \text{Hom}_A(S_j, S_j).$$

Como M y los S_j son espacios vectoriales de dimensión finita, $\text{Hom}_A(M, S_j)$ y $\text{Hom}_A(S_j, S_j)$ son también espacios vectoriales de dimensión finita. Además $\dim \text{Hom}_A(S_j, S_j) \geq 1$ pues $\text{id} \in \text{Hom}_A(S_j, S_j)$. Luego los n_j quedan únivocamente determinados, pues

$$n_j = \frac{\dim \text{Hom}_A(M, S_j)}{\dim \text{Hom}_A(S_j, S_j)}.$$

\square

Si A es un álgebra, definimos el **álgebra opuesta** A^{op} como el espacio vectorial A con el producto $(a, b) \mapsto ba = a \cdot_{\text{op}} b$.

lem:A^op

Lema 1.20. Si A es un álgebra, $A^{\text{op}} \simeq \text{End}_A(A)$ como álgebras.

Demostración. Primero observemos que $\text{End}_A(A) = \{\rho_a : a \in A\}$, donde $\rho_a : A \rightarrow A$ está dado por $x \mapsto xa$. En efecto, si $f \in \text{End}_A(A)$ entonces $f(1) = a \in A$. Además $f(b) = f(b1) = bf(1) = ba$ y luego $f = \rho_a$. Tenemos entonces una biyección $\text{End}_A(A) \rightarrow A^{\text{op}}$ que es morfismo de álgebras pues

$$\rho_a \rho_b(x) = \rho_a(\rho_b(x)) = \rho_a(xb) = x(ba) = \rho_{ba}(x). \quad \square$$

lem:Mn_op

Lema 1.21. Si A es un álgebra y $n \in \mathbb{N}$, entonces $M_n(A)^{\text{op}} \simeq M_n(A^{\text{op}})$ como álgebras.

Demostración. Sea $\psi : M_n(A)^{\text{op}} \rightarrow M_n(A^{\text{op}})$ dada por $X \mapsto X^T$, donde X^T es la traspuesta de X . Como ψ es una transformación lineal biyectiva, basta ver que ψ es morfismo. Si $i, j \in \{1, \dots, n\}$, $a = (a_{ij})$ y $b = (b_{ij})$ entonces

$$\begin{aligned} (\psi(a)\psi(b))_{ij} &= \sum_{k=1}^n \psi(a)_{ik} \psi(b)_{kj} = \sum_{k=1}^n a_{ki} \cdot_{\text{op}} b_{jk} \\ &= \sum_{k=1}^n b_{jk} a_{ki} = (ba)_{ji} = ((ba)^T)_{ij} = \psi(a \cdot_{\text{op}} b)_{ij}. \end{aligned} \quad \square$$

lem:simple

Lema 1.22. Si S es un módulo simple y $n \in \mathbb{N}$, entonces

$$\text{End}_A(nS) \simeq M_n(\text{End}_A(S))$$

como álgebras.

Demostración. Sea (φ_{ij}) una matriz con entradas en $\text{End}_A(S)$. Vamos a definir una función $nS \rightarrow nS$ de la siguiente forma:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & \ddots & \vdots \\ \varphi_{n1} & \cdots & \varphi_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \varphi_{11}(x_1) + \cdots + \varphi_{1n}(x_n) \\ \vdots \\ \varphi_{n1}(x_1) + \cdots + \varphi_{nn}(x_n) \end{pmatrix}.$$

Dejamos como ejercicio demostrar que esta aplicación define un morfismo inyectivo de álgebras

$$M_n(\text{End}_A(S)) \rightarrow \text{End}_A(nS).$$

Este morfismo es sobreyectivo pues si $\psi \in \text{End}(nS)$ y para cada $i, j \in \{1, \dots, n\}$ es posible definir a los ψ_{ij} mediante las ecuaciones

$$\psi \begin{pmatrix} x \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \psi_{11}(x) \\ \psi_{21}(x) \\ \vdots \\ \psi_{n1}(x) \end{pmatrix}, \dots, \psi \begin{pmatrix} 0 \\ 0 \\ \vdots \\ x \end{pmatrix} = \begin{pmatrix} \psi_{1n}(x) \\ \psi_{2n}(x) \\ \vdots \\ \psi_{nn}(x) \end{pmatrix}. \quad \square$$

Teorema 1.23 (Artin–Wedderburn). *Sea A un álgebra semisimple y de dimensión finita, digamos con k clases de isomorfismos de A -módulos simples. Entonces*

$$A \simeq M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

para ciertos $n_1, \dots, n_k \in \mathbb{N}$ y ciertas álgebras de división D_1, \dots, D_k .

Demostración. Al agrupar los finitos submódulos simples de la representación regular de A podemos escribir

$$A = \bigoplus_{i=1}^k n_i S_i,$$

donde los S_i son submódulos simples tales que $S_i \not\simeq S_j$ si $i \neq j$. Dejamos como ejercicio verificar que, gracias al lema de Schur, tenemos

$$\text{End}_A(A) \simeq \text{End}_A\left(\bigoplus_{i=1}^k n_i S_i\right) \simeq \prod_{i=1}^k \text{End}_A(n_i S_i) \simeq \prod_{i=1}^k M_{n_i}(\text{End}_A(S_i)),$$

donde cada $D_i = \text{End}_A(S_i)$ es un álgebra de división. Tenemos entonces que

$$\text{End}_A(A) \simeq \prod_{i=1}^k M_{n_i}(D_i).$$

Como $\text{End}_A(A) \simeq A^{\text{op}}$, entonces

$$A = (A^{\text{op}})^{\text{op}} \simeq \prod_{i=1}^k M_{n_i}(D_i)^{\text{op}} \simeq \prod_{i=1}^k M_{n_i}(D_i^{\text{op}}).$$

Como además cada D_i es un álgebra de división, cada D_i^{op} también lo es. □

Utilizaremos el teorema de Wedderburn en el caso de los números complejos.

Corolario 1.24 (Mollien). *Si A es un álgebra compleja de dimensión finita semisimple, entonces*

$$A \simeq \prod_{i=1}^k M_{n_i}(\mathbb{C})$$

para ciertos $n_1, \dots, n_k \in \mathbb{N}$.

Demostración. Vimos en la demostración del teorema de Wedderburn que

$$A \simeq \prod_{i=1}^k M_{n_i}(\text{End}_A(S_i)),$$

donde S_1, \dots, S_k son representantes de las clases de isomorfismos de los A -módulos simples y cada $\text{End}_A(S_i)$ es un álgebra de división. Veamos que

$$\text{End}_A(S_i) = \{\lambda \text{ id} : \lambda \in \mathbb{C}\} \simeq \mathbb{C}$$

para todo $i \in \{1, \dots, k\}$. En efecto, si $f \in \text{End}_A(S_i)$, entonces f tiene un autovalor $\lambda \in \mathbb{C}$. Como entonces $f - \lambda \text{ id}$ no es un isomorfismo, el lema de Schur implica que $f - \lambda \text{ id} = 0$, es decir $f = \lambda \text{ id}$. Luego $\text{End}_A(S_i) \rightarrow \mathbb{C}$, $\varphi \mapsto \lambda$, es un isomorfismo de álgebras. En particular,

$$A \simeq \prod_{i=1}^k M_{n_i}(\mathbb{C}). \quad \square$$

Ejercicio 1.25. Sean A y B álgebras. Demuestre que los ideales de $A \times B$ son de la forma $I \times J$, donde I es un ideal de A y J es un ideal de B .

Definición 1.26. Un álgebra A se dice **simple** si sus únicos ideales son $\{0\}$ y A .

Proposición 1.27. Sea A un álgebra simple de dimensión finita. Entonces existe un ideal a izquierda no nulo I de dimensión minimal. Este ideal es un A -módulo simple y todo A -módulo simple es isomorfo a I .

Demostración. Como A es de dimensión finita y A es un ideal a izquierda de A , existe un ideal a izquierda no nulo I de dimensión minimal. La minimalidad de $\dim I$ implica que I es simple como A -módulo.

Sea M un A -módulo simple. En particular, $M \neq \{0\}$. Como

$$\text{Ann}(M) = \{a \in A : a \cdot M = \{0\}\}$$

es un ideal de A y además $1 \in A \setminus \text{Ann}(M)$, la simplicidad de A implica que $\text{Ann}(M) = \{0\}$ y luego $I \cdot M \neq \{0\}$ (pues $I \cdot m \neq 0$ para todo $m \in M$ implica que $I \subseteq \text{Ann}(M)$ e I es no nulo, una contradicción). Sea $m \in M$ tal que $I \cdot m \neq \{0\}$. La función

$$\varphi: I \rightarrow M, \quad x \mapsto x \cdot m,$$

es un morfismo de módulos. Como $I \cdot m \neq \{0\}$, el morfismo φ es no nulo. Como I y M son A -módulos simples, el lema de Schur implica que φ es un isomorfismo. \square

Si D es un álgebra de división, el álgebra de matrices $M_n(D)$ es un álgebra simple. La proposición anterior nos dice en particular que $M_n(D)$ tiene una única clase de isomorfismos de $M_n(D)$ -módulos simples. Como sabemos, estos módulos son isomorfos a D^n .

Proposición 1.28. Sea A un álgebra de dimensión finita. Si A es simple, entonces A es semisimple.

Demostración. Sea S la suma de los submódulos simples de la representación regular de A . Afirmamos que S es un ideal de A . Sabemos que S es un ideal a izquierda, pues los submódulos de la representación regular de A son exactamente los ideales a izquierda de A . Para ver que $Sa \subseteq S$ para todo $a \in A$, debemos demostrar que $Ta \subseteq S$ para todo submódulo simple T de A . Si $T \subseteq A$ es un submódulo simple y

$a \in A$, sea $f: T \rightarrow Ta$, $t \mapsto ta$. Como f es un morfismo de A -módulos y T es simple, $\ker f = \{0\}$ o bien $\ker f = T$. Si $\ker f = T$, entonces $f(T) = Ta = \{0\} \subseteq S$. Si $\ker f = \{0\}$, entonces $T \simeq f(T) = Ta$ y luego Ta es simple y entonces $Ta \subseteq S$.

Como S es un ideal de A y A es un álgebra simple, entonces $S = \{0\}$ o bien $S = A$. Como $S \neq \{0\}$, pues existe un ideal a izquierda no nulo I de A tal que $I \neq \{0\}$ de dimensión minimal, se concluye que $S = A$, es decir la representación regular de A es semisimple (por ser suma de submódulos simples) y luego el álgebra A es semisimple. \square

Teorema 1.29 (Wedderburn). *Sea A un álgebra de dimensión finita. Si A es simple, entonces $A \simeq M_n(D)$ para algún $n \in \mathbb{N}$ y alguna álgebra de división D .*

Demostración. Como A es simple, entonces A es semisimple. El teorema de Artin–Wedderburn implica que $A \simeq \prod_{i=1}^k M_{n_i}(D_i)$ para ciertos n_1, \dots, n_k y ciertas álgebras de división D_1, \dots, D_k . Además A tiene k clases de isomorfismos de módulos simples. Como A es simple, A tiene solamente una clase de isomorfismos de módulos simples. Luego $k = 1$ y entonces $A \simeq M_n(D)$ para algún $n \in \mathbb{N}$ y alguna álgebra de división D . \square

Capítulo 2

El radical de Jacobson

Definición 2.1. Si A es un álgebra, el **radical de Jacobson** $J(A)$ es la intersección de los ideales a izquierda maximales de A .

Como A es un álgebra unitaria, A contiene al menos un ideal maximal a izquierda, es decir $J(A) \neq A$.

pro:radical

Proposición 2.2. Sea A un álgebra y sea $a \in A$. Las siguientes afirmaciones son equivalentes:

- 1) $a \in J(A)$.
- 2) Para todo $b \in A$, $1 - ab$ tiene inversa a derecha.
- 3) Para todo $b \in A$, $1 - ab$ es inversible.
- 4) a pertenece a la intersección de los ideales a derecha maximales de A .
- 5) Para todo $b \in A$, $1 - ba$ tiene inversa a izquierda.
- 6) Para todo $b \in A$, $1 - ba$ es inversible.

Demostración. Demostremos que (1) \implies (5). Sea $b \in A$ tal que $1 - ba$ no tiene inversa a izquierda. Existe entonces un ideal a izquierda maximal I tal que $1 - ba \in I$. Como por definición $J(A) \subseteq I$, se concluye que $1 \in I$, una contradicción.

Veamos ahora que (5) \implies (6). Si existe $c \in A$ tal que $c(1 - ba) = 1$ entonces

$$c = 1 + cba = 1 - (-cb)a.$$

Como por hipótesis este elemento tiene inversa a izquierda, existe $d \in A$ tal que $1 = dc$. Luego $d = 1 - ba$ es inversible a derecha.

La implicación (6) \implies (5) es trivial.

Veamos que (5) \implies (1). Si $a \notin J(A)$ sea I un ideal a izquierda maximal tal que $a \notin I$. Por maximalidad, $A = I + Aa$. Entonces existen $x \in I$ y $b \in A$ tales que $1 = x + ba$. Luego $x = 1 - ba \in I$ no tiene inversa a izquierda, pues de lo contrario tendríamos $yx = 1 \in I$ para algún $y \in A$.

Análogamente se demuestra que (2) \iff (3) \iff (4).

Para finalizar demostremos que (3) \iff (6). Si $1 - ab$ tiene inversa c entonces, como $(1 - ab)c = 1$,

$$1 = 1 - ba + ba = 1 - ba + b(1 - ab)ca = 1 - ba + bca - babca = (1 - ba)(1 + bca).$$

Similarmemente, si $c(1 - ab) = 1$, entonces $1 = (1 + bca)(1 - ba)$. \square

La proposición anterior implica que $J(A)$ es un ideal a derecha, pues es también la intersección de los ideales a derecha de A maximales. En consecuencia, $J(A)$ es un ideal.

Definición 2.3. Un ideal I de un álgebra se dice **nilpotente** si $I^m = \{0\}$ para algún $m \in \mathbb{N}$, es decir si $x_1 \cdots x_m = 0$ para todo $x_1, \dots, x_m \in I$.

pro:J_propiedades

Proposición 2.4. Si A y B son álgebras, valen las siguientes propiedades:

- 1) $J(A \times B) = J(A) \times J(B)$.
- 2) $J(A/J(A)) = \{0\}$.
- 3) Si I es un ideal nilpotente de A , entonces $I \subseteq J(A)$.

Demostración. Para la primera afirmación:

$$\begin{aligned} (a, b) \in J(A \times B) &\iff (1, 1) - (x, y)(a, b) \text{ es inversible para todo } (x, y) \in A \times B \\ &\iff (1 - xa, 1 - yb) \text{ es inversible para todo } (x, y) \in A \times B \\ &\iff 1 - xa \text{ y } 1 - yb \text{ son inversibles todo } x \in A, y \in B \\ &\iff (a, b) \in J(A) \times J(B). \end{aligned}$$

Demostremos ahora la segunda afirmación. Sea $\pi: A \rightarrow A/J(A)$ es el morfismo canónico. Sea $\pi(a) \in J(A/J(A))$. Si $a \notin J(A)$, entonces existe un ideal a izquierda de A maximal tal que $a \notin I$. Como por el teorema de la correspondencia $\pi(I)$ es un ideal a izquierda maximal de $A/J(A)$, entonces $\pi(a) \in \pi(I)$, lo que implica en particular que existe $y \in I$ tal que $a - y \in J(A) \subseteq I$, una contradicción pues $a \notin I$.

Demostremos la tercera afirmación. Sea I un ideal de A tal que $I^m = \{0\}$. Si $a \in A$ y $x \in I$, entonces $(ax)^m \in I^m = \{0\}$. Entonces $x \in J(A)$ pues $1 - ax$ es inversible, ya que

$$1 = 1 - (ax)^m = (1 + ax + (ax)^2 + \cdots + (ax)^{m-1})(1 - ax) \quad \square.$$

Lema 2.5. Sea A un álgebra de dimensión finita. Existen finitos ideales a izquierda maximales I_1, \dots, I_k tales que $J(A) = I_1 \cap \cdots \cap I_k$.

Demostración. Sea X el conjunto de ideales a izquierda formados por intersecciones finitas de ideales a izquierda maximales de A . Como A tiene ideales maximales a izquierda, X es no vacío. Sea $J = I_1 \cap \cdots \cap I_k$ un elemento de X de dimensión minimal. Veamos que $J = J(A)$. Como $J(A)$ es la intersección de los ideales a izquierda maximales de A , solamente hay que demostrar que $J(A) \supseteq J$. Si existe $a \in J \setminus J(A)$, entonces sea M un ideal a izquierda maximal de A tal que $a \notin M$. Pero $J \cap M$ es un ideal a izquierda de A que es intersección finita de ideales a izquierda maximales y tal que $M \cap J \subsetneq J$, una contradicción a la minimalidad de $\dim J$. \square

Lema 2.6 (Nakayama). Sea A un álgebra y sea M un A -módulo finitamente generado. Si $I \subseteq A$ es un ideal tal que $I \subseteq J(A)$ y $I \cdot M = M$ entonces $M = \{0\}$.

Demostración. Supongamos que $M \neq \{0\}$ y sea $\{m_1, \dots, m_k\}$ un conjunto minimal de generadores del módulo M . Como $m_k \in M = I \cdot M$, existen $a_1, \dots, a_k \in I$ tales que

$$m_k = a_1 \cdot m_1 + \dots + a_k \cdot m_k,$$

es decir: $(1 - a_k) \cdot m_k = a_1 \cdot m_1 + \dots + a_{k-1} \cdot m_{k-1}$. Como $I \subseteq J(A)$, el elemento $1 - a_k$ es inversible. Luego m_k pertenece al submódulo generado por m_1, \dots, m_{k-1} , una contradicción. \square

pro:J_nilpotente

Proposición 2.7. Si A es un álgebra de dimensión finita, entonces el radical $J(A)$ es un ideal nilpotente.

Demostración. Como A tiene dimensión finita, la sucesión de ideales

$$A \supseteq J(A) \supseteq J(A)^2 \supseteq \dots$$

se estabiliza, es decir que existe $m \in \mathbb{N}$ tal que $J(A)^{m+k} = J(A)^m$ para todo $k \in \mathbb{N}$. En particular, $J(A)J(A)^m = J(A)^{m+1} \subseteq J(A)^m$. El lema de Nakayama con $I = J(A)$ y el módulo $M = J(A)^m$, que es finitamente generado, implica que $J(A)^m = \{0\}$. \square

Teorema 2.8. Sea A un álgebra de dimensión finita. Las siguientes afirmaciones son equivalentes.

- 1) A es semisimple.
- 2) $J(A) = \{0\}$.
- 3) A no tiene ideales nilpotentes no nulos.

Demostración. Demostremos que (1) \implies (2). Si A es semisimple, entonces, por el teorema de Wedderburn, $A \simeq M_{n_1}(D_1) \times \dots \times M_{n_k}(D_k)$ para ciertos $n_1, \dots, n_k \in \mathbb{N}$ y ciertas álgebras de división D_1, \dots, D_k . Entonces

$$\begin{aligned} J(A) &\simeq J(M_{n_1}(D_1) \times \dots \times M_{n_k}(D_k)) \\ &\simeq J(M_{n_1}(D_1)) \times \dots \times J(M_{n_k}(D_k)) \simeq \{0\}, \end{aligned}$$

pues cada $M_{n_j}(D_j)$ es un álgebra simple.

Demostremos (2) \implies (1). Supongamos entonces que $J(A) = \{0\}$. Vimos que $J(A) = I_1 \cap \dots \cap I_k$ para finitos ideales a izquierda maximales I_1, \dots, I_k . Como cada A/I_j es un A -módulo simple, entonces $(A/I_1) \oplus \dots \oplus (A/I_1)$ es un A -módulo semisimple. El morfismo de A -módulos

$$A \rightarrow (A/I_1) \oplus \dots \oplus (A/I_1), \quad a \mapsto (a + I_1, \dots, a + I_k),$$

tiene núcleo $I_1 \cap \dots \cap I_k = J(A) = \{0\}$ y luego es inyectivo. En consecuencia, la representación regular de A es un módulo semisimple, por ser isomorfo a un submódulo de un módulo semisimple. Esto implica que el álgebra A es también semisimple.

La equivalencia entre (2) y (3) es ahora fácil pues vimos que $J(A)$ es un ideal nilpotente que contiene a todo ideal nilpotente de A . \square

Capítulo 3

El teorema de Kolchin

Consideraremos ahora álgebras posiblemente sin unidad.

Si A es un álgebra y $a \in A$, diremos que a es **nil** (o nil) si $a^n = 0$ para algún $n \in \mathbb{N}$. Diremos que el álgebra A es **nil** si todo $a \in A$ es nil. Un álgebra nil no puede tener unidad.

Lema 3.1. *Si A es un álgebra, entonces existen un álgebra con unidad B y un ideal I de B tales que $I \simeq A$ y $B/I \simeq K$.*

Demostración. Sea $B = K \times A$ con las operaciones

$$(\lambda, u)(\mu, v) = (\lambda\mu, \lambda v + \mu u + uv)$$

Dejamos como ejercicio verificar B es un álgebra con unidad $(1, 0)$ y que el conjunto $I = \{(0, a) : a \in A\}$ es un ideal de B tal que $I \simeq A$ y además $B/I \simeq K$. \square

Proposición 3.2. *Sea A un álgebra no nula (posiblemente sin unidad). Si A no tiene ideales nilpotentes no nulos, entonces A es un álgebra con unidad.*

Demostración. Consideramos el álgebra con unidad B del lema anterior, es decir que I es un ideal de B tal que $I \simeq A$ y $B/I \simeq K$. Sea J un ideal nilpotente de B . Como $J \cap I \subseteq I$ es un ideal nilpotente de A , entonces $J \cap I = \{0\}$. Por el segundo teorema de isomorfismos,

$$J \simeq J/(J \cap I) \simeq (I + J)/I$$

y luego $(I + J)/I$ es un ideal nilpotente de $B/I \simeq K$. Como K es un cuerpo, K no tiene ideales propios no nulos. Luego $J = \{0\}$ y entonces B no tiene ideales nilpotentes no nulos. En particular, B es semisimple. Por el teorema de Wedderburn, B es producto directo de álgebras de matrices sobre álgebras de división, digamos

$$B \simeq M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k).$$

Como los ideales de $M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ son de la forma $I_1 \times \cdots \times I_k$, donde cada I_j es un ideal de $M_{n_j}(D_j)$ y cada $M_{n_i}(D_i)$ es un álgebra simple, se concluye que

los ideales no nulos de B son álgebras con unidad. Luego A es también un álgebra con unidad, pues $A \simeq I$. \square

Solamente tenemos definido el radical de Jacobson para álgebras con unidad. Para extender la definición a álgebras sin unidad primero observamos que la suma de ideales nilpotentes es un ideal nilpotente:

Lema 3.3. *Sea A un álgebra. Si I y J son ideales nilpotentes, entonces $I + J$ también.*

Demostración. Sean $n, m \in \mathbb{N}$ tales que $I^n = \{0\}$ y $J^m = \{0\}$. Vamos a demostrar que $(I + J)^{n+m} = \{0\}$. Sean $x_1, \dots, x_{n+m} \in I + J$. Sin perder generalidad podemos escribir $x_1 x_2 \cdots x_{n+m}$ como una suma de elementos de la forma $y_1 \cdots y_{n+m}$, donde cada $y_j \in I \cup J$. Sea $k = \#\{i : y_i \in I\}$. Si $k \geq n$ entonces $y_1 \cdots y_{n+m} = 0$ pues $I^n = 0$; en caso contrario, $\#\{j \in y_j \in J\} \geq m$ y luego $y_1 \cdots y_{n+m} = 0$ pues $J^m = 0$. \square

Definimos el **radical de Jacobson** de un álgebra A sin unidad de dimensión finita como el mayor ideal nilpotente de A , es decir

$$J_0(A) = \sum \{I : I \text{ ideal nilpotente de } A\}.$$

Como $\dim A < \infty$, la suma que define al radical $J(A)$ es una suma finita. El lema anterior implica entonces que $J_0(A)$ es un ideal nilpotente y obviamente contiene a cualquier ideal nilpotente de A .

Queda por verificar que esta definición extiende al radical que conocemos para álgebras con unidad:

Proposición 3.4. *Si A es un álgebra con unidad de dimensión finita, entonces $J(A) = J_0(A)$.*

Demostración. Como el radical $J(A)$ es un ideal nilpotente por la proposición 2.7, entonces $J(A) \subseteq J_0(A)$. Recíprocamente, como $J_0(A)$ es un ideal nilpotente, entonces $J_0(A) \subseteq J(A)$ por la proposición 2.4. \square

La proposición anterior nos permite definir el radical de Jacobson de álgebras de dimensión finita posiblemente sin unidad. Como no hay peligro de confusión, el radical de un álgebra A de dimensión finita será denotado por $J(A)$.

Una matriz a se dice nil si $a^n = 0$ para algún $n \in \mathbb{N}$.

Necesitamos un lema:

Lema 3.5. *El espacio vectorial $M_n(\mathbb{C})$ no posee una base formada por matrices nil.*

Demostración. Supongamos que existen matrices nil A_1, \dots, A_{n^2} tales que generan $M_n(\mathbb{C})$. Entonces existen escalares $\lambda_1, \dots, \lambda_{n^2} \in \mathbb{C}$ tales que

$$E_{11} = \lambda_1 A_1 + \cdots + \lambda_{n^2} A_{n^2}.$$

Para cada $i \in \{1, \dots, n^2\}$ sabemos que $\text{traza}(A_i) = 0$ pues A_i es nil. Como estamos en los complejos, A_i es similar a una matriz triangular superior. Pero por otro lado, $\text{traza}(E_{11}) = 1$, una contradicción. \square

lem:base_de_nilpotentes

Necesitaremos el siguiente resultado sobre álgebras:

Teorema 3.6 (Wedderburn). *Sea A un álgebra compleja de dimensión finita generada como espacio vectorial por elementos nil. Entonces A es nil.*

Demostración. Procederemos por inducción en $\dim A$. Si $\dim A = 1$, sea $a \in A$ un elemento nil tal que $\{a\}$ una base de A . Todo elemento de A es de la forma λa y luego es nil. Supongamos entonces que $\dim A > 1$. Como A es de dimensión finita, el radical $J(A)$ es nilpotente, digamos $J(A)^n = \{0\}$.

Si $J(A) = A$, no hay nada para demostrar. (Esto podría pasar, ya que no suponemos que A tiene unidad.)

Si $J(A) \neq \{0\}$, entonces, como $\dim A/J(A) < \dim A$, por hipótesis inductiva, $A/J(A)$ es nil, digamos $(A/J(A))^m = \{0\}$. Sea $\pi: A \rightarrow A/J(A)$ el epimorfismo canónico y sea $N = nm$. Veamos que $A^N = \{0\}$. En efecto, primero observamos que cualquier producto de m elementos de A pertenece a $J(A)$, pues si $a_1, a_2, \dots, a_m \in A$, entonces $a_1 a_2 \cdots a_m \in J(A)$, ya que

$$\pi(a_1 a_2 \cdots a_m) = \pi(a_1) \pi(a_2) \cdots \pi(a_m) = 0$$

pues $(A/J(A))^m = \{0\}$. Sean ahora $a_1, \dots, a_N \in A$. Entonces $a_1 \cdots a_N = 0$ pues $a_1 \cdots a_N$ es un producto de nm factores, y cada producto de n factores de la forma $b_1 \cdots b_m$ es un elemento de $J(A)$.

Si $J(A) = \{0\}$, entonces, en particular A no contiene ideales nilpotentes no nulos. Luego A tiene unidad y en particular A es semisimple. El teorema de Mollien implica entonces que existen enteros positivos n_1, \dots, n_k tales que

$$A \simeq M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C}).$$

Como A posee una base formada por elementos nil, $M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$ también, es decir $M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$ posee una base formada por matrices nil, una contradicción al lema anterior. \square

Sea $V = \mathbb{C}^{n \times 1}$. Una sucesión de subespacios

$$\{0\} = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = V$$

es una **bandera completa** en V . La notación que usaremos es (V_1, \dots, V_n) . Observemos que si (V_1, \dots, V_n) es una bandera completa, entonces $\dim V_i = i$ para todo $i \in \{1, \dots, n\}$.

La **bandera estándar** es la bandera (V_1, \dots, V_n) , donde $V_i = \langle v_1, \dots, v_i \rangle$ es el espacio vectorial complejo generado por los vectores v_1, \dots, v_n de la base estándar de V . Por convención, $V_0 = \{0\}$.

El grupo $\mathbf{GL}_n(\mathbb{C})$ actúa en el conjunto de banderas completas de V por

$$g \cdot (V_1, \dots, V_n) = (T_g(V_1), \dots, T_g(V_n)),$$

donde $T_g: V \rightarrow V, x \mapsto gx$, es una transformación lineal inversible.

La acción de G en el conjunto de banderas completas es transitiva, pues si (W_1, \dots, W_n) es una bandera completa en V , digamos $W_i = \langle w_1, \dots, w_i \rangle$, donde $\{w_1, \dots, w_n\}$ es una base de V , entonces la matriz $g = (w_1 | \dots | w_n)$ cuyas columnas son los w_j es inversible y cumple que $gv_i = w_i$ para todo $i \in \{1, \dots, n\}$. Luego $g \cdot (V_1, \dots, V_n) = (W_1, \dots, W_n)$.

El estabilizador de la bandera estándar (V_1, \dots, V_n) es

$$G_{(V_1, \dots, V_n)} = \{g \in \mathbf{GL}_n(\mathbb{C}) : T_g(V_i) = V_i \text{ para todo } i\},$$

el subgrupo B de matrices $b = (b_{ij})$ con $b_{ij} = 0$ si $i > j$. El subgrupo $B = G_{(V_1, \dots, V_n)}$ se llama **subgrupo de Borel**. Cualquier conjugado de B será denominado también subgrupo de Borel. Sea U el subgrupo de matrices $u \in \mathbf{GL}_n(\mathbb{C})$ tales que

$$u_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i > j, \end{cases}$$

y sea T el subgrupo de $\mathbf{GL}_n(\mathbb{C})$ formado por las matrices diagonales, es decir las $t \in \mathbf{GL}_n(\mathbb{C})$ tales que $t_{ij} = 0$ si $i \neq j$.

Proposición 3.7. $B = U \rtimes T$.

Demostración. Es evidente que $U \cap T = \{I\}$. Veamos que U es normal en B . En efecto, sea

$$f: B \rightarrow T, \quad b \mapsto \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{nn} \end{pmatrix}$$

Como f es un morfismo de grupos, $U = \ker f$ es un subgrupo normal de B . Falta ver que $B \subseteq UT$. Si $b \in B$, entonces $bf(b)^{-1} \in \ker f = U$, es decir $b \in UT$. \square

Una matriz $a \in \mathbf{GL}_n(\mathbb{C})$ se dice **unipotente** si su polinomio característico es de la forma $(X - 1)^n$. Un subgrupo G de $\mathbf{GL}_n(\mathbb{C})$ es un **grupo unipotente** si todo $g \in G$ es unipotente.

Proposición 3.8. Si G es un subgrupo unipotente de $\mathbf{GL}_n(\mathbb{C})$, existe $v \in \mathbb{C}^{n \times 1}$ no nulo tal que $gv = v$ para todo $g \in G$.

Demostración. Sea V el subespacio de $\mathbf{GL}_n(\mathbb{C})$ generado por $\{g - I : g \in G\}$, donde I es la matriz identidad. Si $g \in G$, entonces, por el teorema de Cayley–Hamilton, $(g - I)^n = 0$, pues g es unipotente. Luego todo elemento de V es nil. Si $g, h \in G$, entonces

$$(g - I)(h - I) = (gh - I) - (g - I) - (h - I) \in V,$$

es decir V es cerrado por multiplicación. Como V es entonces un álgebra que está generado como espacio vectorial por elementos nil, V es nil por el teorema de Wedderburn. En particular, existe $m \in \mathbb{N}$ minimal tal que

$$(g_1 - I) \cdots (g_m - I) = 0$$

para todo $g_1, \dots, g_m \in G$. La minimalidad de m implica que existen $h_1, \dots, h_{m-1} \in G$ tales que $(h_1 - I) \cdots (h_{m-1} - I) \neq 0$. En particular, existe $w \in \mathbb{C}^{m \times 1}$ no nulo tal que $v = (h_1 - I) \cdots (h_{m-1} - I)w \neq 0$. Para todo $g \in G$ tenemos entonces que

$$(g - I)v = (g - I)(h_1 - I) \cdots (h_{m-1} - I)w = 0w = 0,$$

es decir $gv = v$. □

Teorema 3.9 (Kolchin). *Todo subgrupo de $\mathbf{GL}_n(\mathbb{C})$ unipotente es conjugado de algún subgrupo de U .*

Demostración. Sea G un subgrupo de $\mathbf{GL}_n(\mathbb{C})$ unipotente. Si $G \subseteq G_{(W_1, \dots, W_n)}$ para alguna bandera completa (W_1, \dots, W_n) de $V = \mathbb{C}^{n \times 1}$, sea $g \in \mathbf{GL}_n(\mathbb{C})$ tal que

$$g \cdot (V_1, \dots, V_n) = (W_1, \dots, W_n),$$

donde (V_1, \dots, V_n) denota la bandera estándar de V . Entonces

$$G \subseteq G_{g \cdot (V_1, \dots, V_n)} = gG_{(V_1, \dots, V_n)}g^{-1} = gBg^{-1}.$$

Como G es unipotente, $G = G \cap (gBg^{-1}) \subseteq gUg^{-1}$.

Veamos que $G \subseteq G_{(W_1, \dots, W_n)}$ para alguna bandera completa (W_1, \dots, W_n) . Procederemos por inducción en $n = \dim V$. El caso $n = 1$ es trivial. Supongamos entonces que el resultado vale para $n - 1$. Por la proposición anterior, existe $v \in V$ no nulo tal que $gv = v$ para todo $g \in G$. Consideramos entonces el espacio vectorial $Q = V / \langle v \rangle$ de dimensión $n - 1$. El grupo G actúa en Q por

$$g(w + \langle v \rangle) = gw + \langle v \rangle$$

pues si $w - w' \in \langle v \rangle$, entonces $w - w' = \lambda v$ para algún $\lambda \in \mathbb{C}$ y luego

$$gw - gw' = g(w - w') = g(\lambda v) = \lambda gv = \lambda v \in \langle v \rangle,$$

es decir $gw + \langle v \rangle = gw' + \langle v \rangle$. La acción induce un morfismo $\rho: G \rightarrow \mathbf{GL}_{n-1}(\mathbb{C})$. Como G es unipotente, $\rho(G)$ es también unipotente. En efecto, sea $g \in G$. Si completamos $\{v\}$ a una base $\{v, w_1, \dots, w_{n-1}\}$ de V , entonces la matriz de g en esa base es una matriz por bloques, digamos

$$\left(\begin{array}{c|c} 1 & * \\ \hline 0 & \rho(g) \end{array} \right),$$

donde el bloque $\rho(g)$ corresponde a la matriz de $\rho(g)$ en la base $\{w_1, \dots, w_{n-1}\}$. Luego $\rho(g)$ es unipotente pues su polinomio característico es de la forma $(X - 1)^m$, un divisor de $(X - 1)^n$.

Por hipótesis inductiva, el subgrupo $\rho(G)$ de $\mathbf{GL}_{n-1}(\mathbb{C})$ estabiliza una bandera completa (Q_1, \dots, Q_{n-1}) , digamos

$$Q_1 = \langle \pi(v_1) \rangle, \quad Q_2 = \langle \pi(v_1), \pi(v_2) \rangle, \quad \dots \quad Q_{n-1} = \langle \pi(v_1), \dots, \pi(v_{n-1}) \rangle.$$

donde $\pi: V \rightarrow Q$ es el morfismo canónico. Sean

$$\begin{aligned} W_0 &= \langle v \rangle, \\ W_1 &= \langle v, v_1 \rangle, \\ W_2 &= \langle v, v_1, v_2 \rangle, \\ &\vdots \\ W_{n-1} &= \langle v, v_1, \dots, v_{n-1} \rangle. \end{aligned}$$

Como (Q_1, \dots, Q_{n-1}) es una bandera completa de Q , $\{\pi(v_j) : 1 \leq j \leq n-1\}$ es un conjunto linealmente independiente. Luego $\{v, v_1, \dots, v_{n-1}\}$ es también linealmente independiente, pues

$$\sum_{i=1}^{n-1} \lambda_i v_i + \lambda v = 0 \implies \sum_{i=1}^{n-1} \lambda_i \pi(v_i) = 0 \implies \lambda_1 = \dots = \lambda_{n-1} = 0 \implies \lambda = 0.$$

En particular, $\dim W_i = i + 1$ para todo $i \in \{0, \dots, n-1\}$.

Para terminar, falta ver que G estabiliza a la bandera completa (W_1, \dots, W_n) , es decir $G \subseteq G_{(W_1, \dots, W_n)}$. Sea $g \in G$. Trivialmente tenemos que $gW_0 \subseteq W_0$ pues $gv = v$. Veamos que $gW_i \subseteq W_i$ para $j \geq 1$. Fijemos j . Sabemos que existen $\lambda_1, \dots, \lambda_j \in \mathbb{C}$ tales que

$$\pi(gv_j) = \sum_{i \leq j} \lambda_i \pi(v_i),$$

pues $\pi(Q_j) \subseteq Q_j$, lo que implica que $gv_j - \sum_{i \leq j} \lambda_i v_i = \lambda v$ para algún $\lambda \in \mathbb{C}$. En particular,

$$gv_j = \sum_{i \leq j} \lambda_i v_i + \lambda v \in \langle v, v_1, \dots, v_j \rangle = W_j. \quad \square$$

Parte II
Representaciones de grupos

Capítulo 4

El teorema de Maschke

Sea K un cuerpo y sea G un grupo finito. El **álgebra de grupo** $K[G]$ es el K -espacio vectorial con base $\{g : g \in G\}$ con la estructura de álgebra dada por el producto

$$\left(\sum_{g \in G} \lambda_g g \right) \left(\sum_{h \in G} \mu_h h \right) = \sum_{g, h \in G} \lambda_g \mu_h (gh).$$

Observemos que el álgebra $K[G]$ es conmutativa si y sólo si G es abeliano. Además $\dim K[G] = |G|$.

Ejemplo 4.1. Sea $G = \{1, g, g^2\}$ el grupo cíclico de orden tres y sea $A = \mathbb{C}[G]$ el álgebra (compleja) del grupo G . Si $\alpha = a_1 1 + a_2 g + a_3 g^2$ y $\beta = b_1 1 + b_2 g + b_3 g^2 \in A$, donde $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{C}$, entonces la suma de A está dada por

$$\alpha + \beta = (a_1 + b_1)1 + (a_2 + b_2)g + (a_3 + b_3)g^2$$

y el producto por

$$\alpha\beta = (a_1 b_1 + a_2 b_3 + a_3 b_2)1 + (a_1 b_2 + a_2 b_1 + a_3 b_3)g + (a_1 b_3 + a_2 b_2 + a_3 b_1)g^2.$$

Si G es un grupo finito no trivial, entonces $K[G]$ posee ideales propios no triviales. Esto es porque el conjunto

$$I(G) = \left\{ \sum_{g \in G} \lambda_g g \in K[G] : \sum_{g \in G} \lambda_g = 0 \right\}$$

es un ideal propio y no nulo de $K[G]$ (pues $\dim I(G) = \dim K[G] - 1$). Este conjunto se conoce como el **ideal de aumentación** de $K[G]$.

Ejercicio 4.2. Sea $G = C_n$ el grupo cíclico de orden n (escrito multiplicativamente). Demuestre que $K[G] \simeq K[X]/(X^n - 1)$.

Proposición 4.3. Si G es un grupo finito no trivial, entonces $K[G]$ tiene divisores de cero.

Demostración. Sea $g \in G \setminus \{1\}$ y sea n el orden de g . Para ver que $K[G]$ tiene divisores de cero alcanza con observar que $(1 - g)(1 + g + \cdots + g^{n-1}) = 0$. \square

Si A es un álgebra, entonces $\mathcal{U}(A)$ es el grupo de unidades del anillo A . La proposición que sigue se conoce como la propiedad universal del álgebra de grupo.

Proposición 4.4. Sean A un álgebra y G un grupo finito. Si $f: G \rightarrow \mathcal{U}(A)$ es un morfismo de grupos, entonces existe un único morfismo $\varphi: K[G] \rightarrow A$ de álgebras tal que la restricción $\varphi|_G$ de φ al grupo G es igual a f , es decir $\varphi|_G = f$.

Demostración. Como G es base de $K[G]$, puede verificarse que el morfismo φ de álgebras queda unívocamente determinado por

$$\varphi\left(\sum_{g \in G} \lambda_g g\right) = \sum_{g \in G} \lambda_g f(g). \quad \square$$

La proposición anterior nos dice que si G es un grupo finito y A es un álgebra, para definir un morfismo de álgebras $K[G] \rightarrow A$ alcanza con tener un morfismo de grupos $G \rightarrow \mathcal{U}(A)$.

Ejercicio 4.5. Sea M un módulo. Si $p: M \rightarrow M$ es un morfismo tal que $p^2 = p$, entonces $M = \ker p \oplus p(M)$.

Recordemos que una **proyección** (o proyector) de un módulo M es un morfismo $p: M \rightarrow M$ tal que $p^2 = p$.

Teorema 4.6 (Maschke). Sea K un cuerpo de característica cero. Sea G un grupo finito y sea M un $K[G]$ -módulo de dimensión finita. Entonces M es semisimple.

Demostración. Alcanza con demostrar que todo submódulo S de M se complementa. Como, en particular, S es un subespacio de M , existe un subespacio T_0 de M tal que $M = S \oplus T_0$ (como espacios vectoriales). Vamos a usar el espacio vectorial T_0 para construir un submódulo T de M que complementa a S . Como $M = S \oplus T_0$, cada $m \in M$ puede escribirse unívocamente como $m = s + t_0$ para ciertos $s \in S$ y $t_0 \in T_0$. Podemos definir entonces la transformación lineal

$$p_0: M \rightarrow S, \quad p_0(m) = s,$$

donde $m = s + t_0$ con $s \in S$ y $t_0 \in T_0$. Observemos que si $s \in S$, entonces $p_0(s) = s$. En particular, $p_0^2 = p_0$ pues $p_0(m) \in S$.

El problema es que p_0 no es, en general, un morfismo de $K[G]$ -módulos. Promediamos sobre el grupo G para conseguir un morfismo de grupos: Sea

$$p: M \rightarrow S, \quad p(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot p_0(g \cdot m).$$

Primero demostramos que p es un morfismo de $K[G]$ -módulos. Alcanza con ver que $p(g \cdot m) = g \cdot p(m)$ para todo $g \in G$ y $m \in M$. En efecto,

$$p(g \cdot m) = \frac{1}{|G|} \sum_{h \in G} h^{-1} \cdot p_0(h \cdot (g \cdot m)) = \frac{1}{|G|} \sum_{h \in G} (gh^{-1}) \cdot p_0(h \cdot m) = g \cdot p(m).$$

Veamos ahora que $p(M) = S$. La inclusión \subseteq es trivial, pues S es un submódulo de M y además $p_0(M) \subseteq S$. Recíprocamente, si $s \in S$, entonces $g \cdot s \in S$, pues S es un submódulo. Luego $s = g^{-1} \cdot (g \cdot s) = g^{-1} \cdot p_0(g \cdot s)$ y en consecuencia

$$s = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot (g \cdot s) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot (p_0(g \cdot s)) = p(s).$$

Como $p(m) \in S$ para todo $m \in M$, entonces $p^2(m) = p(m)$, es decir que p es un proyectador en S . Luego S se complementa en M , es decir $M = S \oplus \ker(p)$. \square

Podemos utilizar este resultado sobre el cuerpo de los números racionales, reales o complejos. Sin embargo, la descomposición de un módulo sobre el álgebra de grupo dependerá fuertemente del cuerpo sobre el que se trabaje.

Ejemplo 4.7. Sea $G = \langle g \rangle$ el grupo cíclico de orden cuatro y sea $\rho_g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Sea $M = \mathbb{C}^{2 \times 1}$ con la estructura de $\mathbb{C}[G]$ -módulo dada por

$$g \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} -v \\ u \end{pmatrix},$$

es decir, si $a, b, c, d \in \mathbb{C}$, entonces

$$(a1 + bg + cg^2 + dg^3) \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} (a-d)u + (c-b)v \\ (1-b)u + (a-d)v \end{pmatrix}.$$

Sabemos por el teorema de Maschke que M es semisimple. Veamos cómo descomponer el módulo M como suma directa de simples. Como $\dim M = 2$, tendremos que M es suma directa de dos submódulos de dimensión uno. Observemos que si S es un submódulo tal que $\{0\} \subsetneq S \subsetneq M$, entonces $\dim S = 1$. Además

$$S = \left\{ \lambda \begin{pmatrix} u_0 \\ v_0 \end{pmatrix} : \lambda \in \mathbb{C} \right\} \text{ es un submódulo de } M \iff \begin{pmatrix} u_0 \\ v_0 \end{pmatrix} \text{ es autovector de } \rho_g.$$

Como la matriz ρ_g tiene polinomio característico $X^2 + 1$, se sigue que $\begin{pmatrix} i \\ 1 \end{pmatrix}$ es autovector de ρ_g de autovalor $-i$ y que $\begin{pmatrix} -i \\ 1 \end{pmatrix}$ es autovector de autovalor i . Luego M se descompone en suma directa de simples como

$$M = \mathbb{C} \begin{pmatrix} i \\ 1 \end{pmatrix} \oplus \mathbb{C} \begin{pmatrix} -i \\ 1 \end{pmatrix}$$

Observar que en ejemplo anterior pudimos descomponer a la matriz ρ_g gracias a la existencia de autovectores, algo que no pasaría si consideramos módulos sobre el álgebra de grupo real.

Ejemplo 4.8. Sea $G = \langle g \rangle$ el grupo cíclico de orden cuatro y sea $\rho_g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Sea $M = \mathbb{R}^{2 \times 1}$ con la estructura de $\mathbb{R}[G]$ -módulo dada por

$$g \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} -v \\ u \end{pmatrix}.$$

Tal como hicimos en el ejemplo anterior, como $\dim M = 2$, si S es un submódulo de M tal que $\{0\} \subsetneq S \subsetneq M$, entonces $\dim S = 1$. Pero como ρ_g no tiene autovectores reales, M no tendrá submódulos de dimensión uno. En consecuencia, M es simple como $\mathbb{R}[G]$ -módulo.

Es posible dar una versión multiplicativa del teorema de Maschke.

Un grupo G **actúa por automorfismos** en A si existe un morfismo de grupos $G \rightarrow \text{Aut}(A)$, es decir que se tiene una acción de G en A tal que $g \cdot 1_A = 1_A$ y $g \cdot (ab) = (g \cdot a)(g \cdot b)$ para todo $g \in G$ y $a, b \in A$.

Teorema 4.9. Sea K un grupo finito de orden m que actúa por automorfismos en $V = U \times W$, donde W es un subgrupo de V y U es un subgrupo de V abeliano y K -invariante. Si la función $u \mapsto u^m$ es biyectiva en U , entonces existe un subgrupo normal K -invariante N de V tal que $V = U \times N$.

Demostración. Sea $\theta: U \times W \rightarrow U$, $(u, w) \mapsto u$. Entonces θ es un morfismo de grupos tal que $\theta(u) = u$ para todo $u \in U$. Como U es K -invariante, entonces

$$k^{-1} \cdot \theta(k \cdot v) \in U$$

para todo $k \in K$ y $v \in V$. Como además K es finito y U es abeliano, queda bien definida la función

$$\varphi: V \rightarrow U, \quad v \mapsto \prod_{k \in K} k^{-1} \cdot \theta(k \cdot v).$$

Veamos que φ es un morfismo de grupos. Si $x, y \in V$, entonces

$$\begin{aligned} \varphi(xy) &= \prod_{k \in K} k^{-1} \cdot \theta(k \cdot (xy)) \\ &= \prod_{k \in K} k^{-1} \cdot (\theta(k \cdot x) \theta(k \cdot y)) \\ &= \prod_{k \in K} k^{-1} \cdot \theta(k \cdot x) \prod_{k \in K} k^{-1} \cdot \theta(k \cdot y) = \varphi(x) \varphi(y), \end{aligned}$$

pues U es abeliano y K actúa por automorfismos en V .

Vamos a demostrar ahora que $N = \ker \varphi$ es K -invariante. Alcanza con ver que $\varphi(l \cdot x) = l \cdot \varphi(x)$ para todo $l \in K$ y $x \in V$. Si $l \in K$ y $x \in V$, entonces

$$l^{-1} \cdot \varphi(l \cdot x) = l^{-1} \cdot \left(\prod_{k \in K} k^{-1} \cdot \theta(k \cdot (l \cdot x)) \right) = \prod_{k \in K} (kl)^{-1} \cdot \theta((kl) \cdot x) = \varphi(x),$$

pues kl recorre todos los elementos de K si k recorre todos los elementos de K . Se concluye entonces que $\ker \varphi$ es K -invariante.

Nos falta demostrar que V es el producto directo de U y N . Por hipótesis, U es normal en V . Veamos primero que $U \cap N = \{1\}$. Si $u \in U$, entonces $k \cdot u \in U$ para todo $k \in K$, lo que implica que $k^{-1} \cdot \theta(k \cdot u) = k^{-1} \cdot (k \cdot u) = u$. Luego $\varphi(u) = u^m$. Como por hipótesis esta función es biyectiva, se concluye que

$$U \cap N = U \cap \ker \varphi = \{1\}.$$

Veamos ahora que $V \subseteq UN$, ya que la otra inclusión es trivial. Como $N = \ker \varphi$, entonces

$$\varphi(V) \subseteq U = \varphi(U) = \varphi(U)\varphi(N) = \varphi(UN)$$

y luego $V \subseteq (UN)N = UN$. Luego V es el producto directo de U y N , pues N es normal en V . \square

Corolario 4.10. *Sean p un primo, K un grupo finito de orden coprimo con p y V un p -grupo elemental abeliano. Si K actúa por automorfismos en V y U es un subgrupo K -invariante de V , existe un subgrupo K -invariante N de V tal que $V = U \times N$.*

Demostración. Sea $m = |K|$. Como m y $|U|$ son coprimos, la función $u \mapsto u^m$ es biyectiva en U . Como V es un espacio vectorial sobre el cuerpo \mathbb{Z}/p , tenemos que $V = U \times W$ para algún subgrupo W de V . El corolario se obtiene entonces al aplicar el teorema anterior. \square

Supongamos que G es un grupo finito. Sabemos por el teorema de Maschke que $\mathbb{C}[G]$ es un álgebra semisimple. Por el teorema de Mollien, existe $r \in \mathbb{N}$ y existen $n_1, \dots, n_r \in \mathbb{N}$ tales que

$$\mathbb{C}[G] \simeq \prod_{i=1}^r M_{n_i}(\mathbb{C}),$$

donde r es la cantidad de módulos simples de $\mathbb{C}[G]$. Además

$$|G| = \dim \mathbb{C}[G] = \sum_{i=1}^r n_i^2.$$

Dado que \mathbb{C} es un $\mathbb{C}[G]$ -módulo de dimensión uno, es simple. Sin perder generalidad podemos suponer entonces que $n_1 = 1$.

Teorema 4.11. *Un grupo finito tiene tantas clases de isomorfismo de simples como clases de conjugación.*

Demostración. Sea G un grupo finito. Como $\mathbb{C}[G] \simeq \prod_{i=1}^r M_{n_i}(\mathbb{C})$ por el teorema de Wedderburn, entonces

$$Z(\mathbb{C}[G]) \simeq \prod_{i=1}^r Z(M_{n_i}(\mathbb{C})) \simeq \mathbb{C}^r.$$

En particular, $\dim Z(\mathbb{C}[G]) = r$. Por otro lado, si $\alpha = \sum_{g \in G} \lambda_g g \in Z(\mathbb{C}[G])$, entonces $h^{-1} \alpha h = \alpha$ para todo $h \in G$. Esto implica que

$$\sum_{g \in G} \lambda_{hgh^{-1}} g = \sum_{g \in G} \lambda_g h^{-1} g h = \sum_{g \in G} \lambda_g g.$$

Luego $\lambda_g = \lambda_{hgh^{-1}}$ para todo $g, h \in G$. Una base para $Z(\mathbb{C}[G])$ está dada entonces por los elementos de la forma

$$\sum_{g \in K} g,$$

donde K es una clase de conjugación de G . Luego $\dim Z(\mathbb{C}[G])$ es igual a la cantidad de clases de conjugación de G . \square

Ejemplo 4.12. Como el grupo C_4 cíclico de orden cuatro es abeliano, se tiene que $\mathbb{C}[C_4] \simeq \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$ como álgebras.

Ejemplo 4.13. Vimos en el ejemplo 5.18 que S_3 tiene una representación irreducible de grado dos. Como $6 = 1 + n_2^2 + \cdots + n_k^2$, se concluye que $k = 3$ y $n_2 = 1$. Alternativamente podríamos haber obtenido $k = 3$ al observar que S_3 tiene tres clases de conjugación, de donde se sigue inmediatamente que $n_1 = n_2 = 1$ y $n_3 = 2$. En conclusión,

$$\mathbb{C}[S_3] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$$

como álgebras.

Capítulo 5

Representaciones de grupos

Salvo que se mencione lo contrario, trabajaremos sobre el cuerpo \mathbb{C} de los números complejos.

Definición 5.1. Si G es un grupo y V es un espacio vectorial, un morfismo de grupos $\rho: G \rightarrow \mathbf{GL}(V)$, $g \mapsto \rho_g$, es una **representación** de G . La dimensión de V es el **grado** de la representación, es decir $\deg \rho = \dim V$.

Si el espacio vectorial V tiene dimensión finita n , al fijar una base para V podemos considerar $\rho: G \rightarrow \mathbf{GL}(V) \simeq \mathbf{GL}_n(\mathbb{C})$. Consideraremos solamente representaciones de grado finita de grupo finitos.

Ejemplo 5.2. Como $\mathbb{S}_3 = \langle (12), (123) \rangle$, la función $\rho: \mathbb{S}_3 \rightarrow \mathbf{GL}_3(\mathbb{C})$,

$$(12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

es una representación de \mathbb{S}_3 .

Ejemplo 5.3. Sea $G = \langle g \rangle$ cíclico de orden seis. La función $\rho: G \rightarrow \mathbf{GL}_2(\mathbb{C})$,

$$g \mapsto \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

es una representación del grupo G cíclico de orden seis.

Ejemplo 5.4. Sea $G = \langle g \rangle$ cíclico de orden cuatro. La función $\rho: G \rightarrow \mathbf{GL}_2(\mathbb{C})$,

$$g \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

es una representación del grupo G cíclico de orden cuatro.

Ejemplo 5.5. Sea $G = \langle a, b : a^2 = b^3 = (ab)^3 = 1 \rangle$. La asignación

$$a \mapsto \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

define una representación $G \rightarrow \mathbf{GL}_3(\mathbb{C})$.

Ejemplo 5.6. Sea G un grupo finito que actúa en un conjunto finito X . Sea $V = \mathbb{C}X$ el espacio vectorial con base $\{x : x \in X\}$. Entonces

$$\rho : G \rightarrow \mathbf{GL}(V), \quad \rho_g \left(\sum_{x \in X} \lambda_x x \right) = \sum_{x \in X} \lambda_x \rho_g(x) = \sum_{x \in X} \lambda_{g^{-1} \cdot x} x$$

es una representación de grado $|X|$.

Ejemplo 5.7. El signo $\text{sign} : \mathbb{S}_n \rightarrow \mathbf{GL}_1(\mathbb{C}) = \mathbb{C}^\times$ es una representación de \mathbb{S}_n .

Una representación $\rho : G \rightarrow \mathbf{GL}(V)$ se dice **fiel** si ρ es inyectivo.

Ejemplo 5.8. Sea $Q_8 = \langle i, j, k : i^2 = j^2 = k^2, i^4 = 1, ij = k \rangle$. Entonces

$$\rho : Q_8 \rightarrow \mathbf{GL}_2(\mathbb{C}), \quad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$

es una representación fiel.

Observemos que existe una correspondencia biyectiva

$$\{\text{representaciones de } G\} \leftrightarrow \{\mathbb{C}[G]\text{-módulos}\}.$$

Además representaciones de grado finito se corresponderán con $\mathbb{C}[G]$ -módulos de dimensión finita. Si $\rho : G \rightarrow \mathbf{GL}(V)$ es una representación, entonces V es un $\mathbb{C}[G]$ -módulo con

$$\left(\sum_{g \in G} \lambda_g g \right) \cdot v = \sum_{g \in G} \lambda_g \rho(g)(v).$$

Recíprocamente, si V es un $\mathbb{C}[G]$ -módulo, entonces $\rho : G \rightarrow \mathbf{GL}(V)$, $\rho(g)(v) = g \cdot v$, es una representación de G en V . Puede verificarse que estas construcciones son una la inversa de la otra.

Proposición 5.9. Sean G un grupo finito, $g \in G$ y $\rho : G \rightarrow \mathbf{GL}(V)$ una representación. Entonces ρ_g es diagonalizable.

Demostración. Como G es finito, existe $n \in \mathbb{N}$ tal que $g^n = 1$. Luego ρ_g es raíz del polinomio $X^n - 1$. Como este polinomio tiene todas sus raíces distintas y se factoriza linealmente en $\mathbb{C}[X]$, también tiene estas propiedades el polinomio minimal de ρ_g . Luego ρ_g es diagonalizable. \square

Definición 5.10. Sea G un grupo y sean $\phi: G \rightarrow \mathbf{GL}(V)$ y $\psi: G \rightarrow \mathbf{GL}(W)$ representaciones. Se dice que ϕ y ψ son **equivalentes** si existe un isomorfismo $T: V \rightarrow W$ tal que

$$\psi_g \circ T = T \circ \phi_g$$

para todo $g \in G$. Notación: $\phi \simeq \psi$.

Observemos que $\phi \simeq \psi$ si y sólo si V y W son isomorfos como $\mathbb{C}[G]$ -módulos.

Ejemplo 5.11. La representación

$$\phi: \mathbb{Z}/n \rightarrow \mathbf{GL}_2(\mathbb{C}), \quad \phi(m) = \begin{pmatrix} \cos(2\pi m/n) & -\sin(2\pi m/n) \\ \sin(2\pi m/n) & \cos(2\pi m/n) \end{pmatrix},$$

es equivalente a la representación

$$\psi: \mathbb{Z}/n \rightarrow \mathbf{GL}_2(\mathbb{C}), \quad \psi(m) = \begin{pmatrix} e^{2\pi i m/n} & 0 \\ 0 & e^{-2\pi i m/n} \end{pmatrix}.$$

La equivalencia se realiza con la matriz $T = \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}$. En efecto, $\phi_m \circ T = T \circ \psi_m$ para todo m .

Traducimos ahora la noción de submódulo al lenguaje de la teoría de representaciones. Utilizaremos ambos lenguajes tanto como nos resulte conveniente.

Definición 5.12. Sea $\phi: G \rightarrow \mathbf{GL}(V)$ una representación. Un subespacio $W \subseteq V$ se dice **G -invariante** si $\phi_g(W) \subseteq W$ para todo $g \in G$. Si W es un subespacio G -invariante, entonces la restricción $\rho|_W$ de ϕ a W es una representación, que se llama **subrepresentación** de ϕ .

Si $\rho: G \rightarrow \mathbf{GL}(V)$ es una representación y W es un subespacio de V , entonces W es subespacio G -invariante de V si y sólo si W es un $\mathbb{C}[G]$ -submódulo de V .

Definición 5.13. Una representación $\phi: G \rightarrow \mathbf{GL}(V)$ no nula se dice **irreducible** si los $\{0\}$ y V son los únicos subespacios G -invariantes de V .

Claramente una representación $\rho: G \rightarrow \mathbf{GL}(V)$ es irreducible si y sólo si V es simple como $\mathbb{C}[G]$ -módulo.

Ejemplo 5.14. Toda representación de grado uno es irreducible.

En el siguiente ejemplo trabajaremos sobre los números reales.

Ejemplo 5.15. Sea $G = \langle g \rangle$ cíclico de orden tres y sea

$$\rho: G \rightarrow \mathbf{GL}_3(\mathbb{R}), \quad g \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

es decir que g actúa en \mathbb{R}^3 por multiplicación de matrices,

$$g \cdot (x, y, z) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

El conjunto

$$N = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0\}$$

es un subespacio G -invariante de \mathbb{R}^3 .

Veamos que N es irreducible. Si N contiene un subespacio no nulo G -invariante S , sea $(x_0, y_0, z_0) \in S \setminus \{(0, 0, 0)\}$. Como S es G -invariante,

$$\begin{pmatrix} y_0 \\ z_0 \\ x_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \in S.$$

Afirmamos que $\{(x_0, y_0, z_0), (y_0, z_0, x_0)\}$ es un conjunto linealmente independiente. Si existe $\lambda \in \mathbb{R}$ tal que $\lambda(x_0, y_0, z_0) = (y_0, z_0, x_0)$, entonces $x_0 = \lambda^3 x_0$. Como $x_0 = 0$ implica que $y_0 = z_0 = 0$, entonces $\lambda = 1$. En particular, $x_0 = y_0 = z_0$, una contradicción, pues $x_0 + y_0 + z_0 = 0$. Luego $\dim S = 2$ y entonces $S = N$.

Ejercicio 5.16. ¿Qué pasa en el ejemplo anterior sobre los números complejos?

pro:deg2

Proposición 5.17. Sea $\phi: G \rightarrow \mathbf{GL}(V)$, $g \mapsto \phi_g$, una representación de grado dos. Entonces ϕ es irreducible si y sólo si no existe autovector común para todos los ϕ_g .

Demostración. Supongamos que ϕ no es irreducible. Existe entonces $W \subseteq V$ subespacio propio no nulo G -invariante, $\dim W = 1$. Sea $w \in W \setminus \{0\}$. Para cada $g \in G$, $\phi_g(w) \in W$ y entonces $\phi_g(w) = \lambda w$ para algún λ . Luego w es un autovector común para todos los ϕ_g . Recíprocamente, si ϕ admite un autovector en común $v \in V$, entonces el subespacio generado por v es G -invariante. \square

exa:S3deg2

Ejemplo 5.18. Sabemos que \mathbb{S}_3 está generado por (12) y (23). La asignación

$$(12) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (23) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$$

define una representación ϕ de \mathbb{S}_3 . La proposición 5.17 nos dice que esta representación es irreducible pues las matrices $\phi_{(12)}$ y $\phi_{(23)}$ no tienen autovectores en común.

Definición 5.19. Una representación $\rho: G \rightarrow \mathbf{GL}(V)$ se dice **completamente reducible** si V puede descomponerse como $V = V_1 \oplus \cdots \oplus V_n$, donde cada V_i es un subespacio G -invariantes y cada restricción $\rho|_{V_i}$ es irreducible.

Es claro que una representación $\rho: G \rightarrow \mathbf{GL}(V)$ es completamente reducible si y sólo si V es semisimple como $\mathbb{C}[G]$ -módulo.

proposition:Lin(G)

Proposición 5.20. Sea G un grupo finito. Las representaciones de grado uno están en biyección con las representaciones de grado uno del grupo $G/[G, G]$.

Demostración. Sea $\pi: G \rightarrow G/[G, G]$ el morfismo canónico. Si $\rho: G/[G, G] \rightarrow \mathbb{C}^\times$ es una representación, $\rho \circ \pi: G \rightarrow \mathbb{C}^\times$ también es una representación.

Veamos que toda representación de G de grado uno se obtiene de esta forma. Sea $\phi: G \rightarrow \mathbb{C}^\times$ una representación de grado uno. Como $G/\ker \phi \simeq \phi(G)$ es abeliano, $[G, G] \subseteq \ker \phi$. Sea $\rho: G/[G, G] \rightarrow \mathbb{C}^\times$, $x[G, G] \mapsto \phi(x)$. La función ρ está bien definida pues si $x[G, G] = y[G, G]$ entonces $xy^{-1} \in [G, G]$ y luego

$$\rho(x[G, G]) = \phi(x) = \phi(y) = \rho(y[G, G]).$$

Además ρ es morfismo pues

$$\rho(x[G, G]y[G, G]) = \rho(xy[G, G]) = \phi(xy) = \phi(x)\phi(y) = \rho(x[G, G])\rho(y[G, G]).$$

Por construcción, $\rho \circ \pi = \phi$. □

xca:n+3mgeq4k

Ejercicio 5.21. Si G es un grupo finito de orden n con k clases de conjugación y $m = (G : [G, G])$, entonces $n + 3m \geq 4k$.

Ejemplo 5.22. El grupo cíclico $G = \langle g \rangle$ de orden dos tiene dos representaciones de grado uno. En efecto, si $\rho: G \rightarrow \mathbb{C}^\times$ es una representación de grado uno, entonces, como $g^2 = 1$, se tiene que $\rho_g \in \{-1, 1\}$.

Ejemplo 5.23. Como $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$ y $(\mathbb{S}_n : \mathbb{A}_n) = 2$, el grupo simétrico \mathbb{S}_n tiene dos representaciones lineales. Una de esas representaciones está dada por el morfismo trivial y la otra por el signo.

Veamos algunos ejemplos generales de representaciones:

Ejemplo 5.24. El morfismo trivial $\rho: G \rightarrow \mathbf{GL}_1(\mathbb{C}) = \mathbb{C}^\times$, $g \mapsto 1$, es una representación, es la **representación trivial** de G . En el lenguaje de módulos, \mathbb{C} es trivial como $\mathbb{C}[G]$ -módulo con la acción

$$g \cdot \lambda = \lambda$$

para $g \in G$ y $\lambda \in \mathbb{C}$.

Ejemplo 5.25. Sean $\rho: G \rightarrow \mathbf{GL}(V)$ y $\psi: G \rightarrow \mathbf{GL}(W)$ dos representaciones. Entonces $\rho \oplus \psi: G \rightarrow \mathbf{GL}(V \oplus W)$, $g \mapsto (\rho_g, \psi_g)$, es una representación, es la **suma directa** de las representaciones y corresponde al $\mathbb{C}[G]$ -módulo $V \oplus W$ dado por

$$g \cdot (v, w) = (g \cdot v, g \cdot w)$$

para $g \in G$, $v \in V$ y $w \in W$.

Para los ejemplos que siguen necesitamos productos tensoriales.

El **producto tensorial** de los K -espacios vectoriales U y V es el espacio vectorial cociente $K[U \times V]/T$, donde $K[U \times V]$ es el espacio vectorial sobre K con base $\{(u, v) : u \in U, v \in V\}$ y T es el subespacio generado por los elementos de la forma

$$(\lambda u + \mu u', v) - \lambda(u, v) - \mu(u', v), \quad (u, \lambda v + \mu v') - \lambda(u, v) - \mu(u, v')$$

para $\lambda, \mu \in K$, $u, u' \in U$ y $v, v' \in V$.

El producto tensorial de U y V será denotado por $U \otimes_K V$ o por $U \otimes V$ si la referencia al cuerpo K puede omitirse. Dados $u \in U$ y $v \in V$ escribiremos $u \otimes v$ para denotar a la coclase $(u, v) + T$.

Teorema 5.26. *Sean U y V espacios vectoriales. Existe entonces una función bilineal $U \times V \rightarrow U \otimes V$, $(u, v) \mapsto u \otimes v$, tal que todo elemento de $U \otimes V$ es una suma finita de la forma*

$$\sum_{i=1}^N u_i \otimes v_i$$

para $u_1, \dots, u_N \in U$ y $v_1, \dots, v_N \in V$. Más aún, dado un espacio vectorial W y una función bilineal $\beta: U \times V \rightarrow W$, existe una función lineal $\bar{\beta}: U \otimes V \rightarrow W$ tal que $\bar{\beta}(u \otimes v) = \beta(u, v)$ para todo $u \in U$ y $v \in V$.

Demostración. Por la definición del producto tensorial, la función

$$U \times V \rightarrow U \otimes V, \quad (u, v) \mapsto u \otimes v,$$

es bilineal. También de la definición se deduce inmediatamente que todo elemento de $U \otimes V$ es una combinación lineal finita de elementos de la forma $u \otimes v$, donde $u \in U$ y $v \in V$. Como $\lambda(u \otimes v) = (\lambda u) \otimes v$ para todo $\lambda \in K$, la primera afirmación queda demostrada.

Como $U \times V$ es base de $K[U \times V]$, existe una transformación lineal

$$\gamma: K[U \times V] \rightarrow W, \quad \gamma(u, v) = \beta(u, v).$$

Como β es bilineal por hipótesis, $T \subseteq \ker \gamma$. Existe entonces una transformación lineal $\bar{\beta}: U \otimes V \rightarrow W$ tal que

$$\begin{array}{ccc} K[U \times V] & \xrightarrow{\quad} & W \\ \downarrow & \nearrow & \\ U \otimes V & & \end{array}$$

conmuta. En particular, $\bar{\beta}(u \otimes v) = \beta(u, v)$. □

xca:tensorial_unicidad

Ejercicio 5.27. Demuestre que las propiedades mencionadas en el teorema anterior caracterizan el producto tensorial salvo isomorfismo.

Veamos algunas propiedades del producto tensorial de espacios vectoriales.

Lema 5.28. *Sean $\varphi: U \rightarrow U'$ y $\psi: V \rightarrow V'$ transformaciones lineales. Existe entonces una única transformación lineal $\varphi \otimes \psi: U \otimes V \rightarrow U' \otimes V'$ tal que*

$$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v)$$

para todo $u \in U$ y $v \in V$.

Demostración. Como la función $U \times V \rightarrow U \otimes V$, $(u, v) \mapsto \varphi(u) \otimes \psi(v)$, es bilineal, existe una transformación lineal $U \otimes V \rightarrow U \otimes V$, $u \otimes v \mapsto \varphi(u) \otimes \psi(v)$. Luego la función

$$\sum u_i \otimes v_i \mapsto \sum \varphi(u_i) \otimes \psi(v_i)$$

está bien definida. \square

Ejercicio 5.29. Demuestre las siguientes afirmaciones:

- 1) $(\varphi \otimes \psi)(\varphi' \otimes \psi') = (\varphi\varphi') \otimes (\psi\psi')$.
- 2) Si φ y ψ son isomorfismos, entonces $\varphi \otimes \psi$ es un isomorfismo.
- 3) $(\lambda\varphi + \lambda'\varphi') \otimes \psi = \lambda\varphi \otimes \psi + \lambda'\varphi' \otimes \psi$.
- 4) $\varphi \otimes (\lambda\psi + \lambda'\psi') = \lambda\varphi \otimes \psi + \lambda'\varphi \otimes \psi'$.
- 5) Si $U \simeq U'$ y $V \simeq V'$, entonces $U \otimes V \simeq U' \otimes V'$.

Lema 5.30. Si U y V son espacios vectoriales, entonces $U \otimes V \simeq V \otimes U$.

Demostración. Como la función $U \times V \rightarrow V \otimes U$, $(u, v) \mapsto v \otimes u$, existe una transformación lineal $U \otimes V \rightarrow V \otimes U$, $u \otimes v \mapsto v \otimes u$. Similarmente se demuestra que existe una transformación lineal $V \otimes U \rightarrow U \otimes V$, $v \otimes u \mapsto u \otimes v$. Luego $U \otimes V \simeq V \otimes U$. \square

xca:UxVxW

Ejercicio 5.31. Demuestre que $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$.

xca:UxK

Ejercicio 5.32. Demuestre que $U \otimes K \simeq U \simeq K \otimes U$.

lem:U_LI

Lema 5.33. Sea $\{u_1, \dots, u_n\} \subseteq U$ un conjunto linealmente independiente y sean $v_1, \dots, v_n \in V$ tales que $\sum_{i=1}^n u_i \otimes v_i = 0$. Entonces $v_i = 0$ para todo $i \in \{1, \dots, n\}$.

Demostración. Sea U_1 el espacio vectorial con base $\{u_1, \dots, u_n\}$. Para $i \in \{1, \dots, n\}$ sea $f_i: U_1 \rightarrow K$, $f_i(u_j) = \delta_{ij}$. Como la función $U_1 \times V \rightarrow V$, $(u, v) \mapsto f_i(u)v$, es bilineal, existe una función $\alpha_i: U_1 \otimes V \rightarrow V$ lineal tal que $\alpha_i(u \otimes v) = f_i(u)v$. Luego

$$v_i = \sum_{j=1}^n \alpha_i(u_j \otimes v_j) = \alpha_i\left(\sum_{j=1}^n u_j \otimes v_j\right) = 0. \quad \square$$

xca:uxv=0

Ejercicio 5.34. Demuestre que si $u \otimes v = 0$ y $v \neq 0$, entonces $u = 0$.

Teorema 5.35. Si $\{u_i: i \in I\}$ es una base de U y $\{v_j: j \in J\}$ es una base de V , entonces $\{u_i \otimes v_j: i \in I, j \in J\}$ es una base de $U \otimes V$.

Demostración. Los $u_i \otimes v_j$ forman un conjunto de generadores pues si $u = \sum_i \lambda_i u_i$ y $v = \sum_j \mu_j v_j$, entonces $u \otimes v = \sum_{i,j} \lambda_i \mu_j u_i \otimes v_j$. Veamos ahora que los $u_i \otimes v_j$ son linealmente independientes. Para eso, queremos ver que cualquier subconjunto finito de los $u_i \otimes v_j$ es linealmente independiente. Si $\sum_k \sum_l \lambda_{kl} u_{i_k} \otimes v_{j_l} = 0$, entonces $0 = \sum_k u_{i_k} \otimes (\sum_l \lambda_{kl} v_{j_l})$ y luego, como los u_{i_k} son linealmente independientes, el lema 5.33 implica que $\sum_l \lambda_{kl} v_{j_l} = 0$. Luego $\lambda_{kl} = 0$ para todo k, l pues los v_{j_l} son linealmente independientes. \square

El teorema anterior implica inmediatamente que si U y V son espacios vectoriales de dimensión finita entonces

$$\dim(U \otimes V) = (\dim U)(\dim V).$$

Corolario 5.36. Si $\{u_i : i \in I\}$ es base de U , entonces todo elemento de $U \otimes V$ se escribe unívocamente como una suma finita $\sum_i u_i \otimes v_i$.

Demostración. Sabemos que todo elemento de $U \otimes V$ es una suma finita $\sum_i x_i \otimes y_i$, donde $x_i \in U$ y $y_i \in V$. Si escribimos $x_i = \sum_j \lambda_{ij} u_j$, entonces

$$\sum_i x_i \otimes y_i = \sum_i \left(\sum_j \lambda_{ij} u_j \right) \otimes y_i = \sum_j u_j \otimes \left(\sum_i \lambda_{ij} y_i \right).$$

Dejamos la unicidad como ejercicio. □

Ahora sí, el ejemplo que estábamos esperando.

Ejercicio 5.37. Sea G un grupo finito. Demuestre que si V y W son $\mathbb{C}[G]$ -módulos, el producto tensorial $V \otimes W$ es un $\mathbb{C}[G]$ -módulo con

$$g \cdot (v \otimes w) = g \cdot v \otimes g \cdot w$$

para $g \in G$, $v \in V$ y $w \in W$.

Otro ejemplo importante:

Proposición 5.38. Sea G un grupo finito. Si V y W son $\mathbb{C}[G]$ -módulos, entonces $\text{Hom}_{\mathbb{C}}(V, W)$ es un $\mathbb{C}[G]$ -módulo con

$$(gf)(v) = gf(g^{-1}v),$$

donde $g \in G$, $f \in \text{Hom}_{\mathbb{C}}(V, W)$ y $v \in V$.

Demostración. Calculamos

$$\begin{aligned} ((gh)f)(u) &= (gh)f((gh)^{-1}u) \\ &= g(h(f(h^{-1}(gu)))) = h((hf)(gu)) = (g(hf))(u). \end{aligned} \quad \square$$

La proposición anterior nos dice, en particular, que el dual $V^* = \text{Hom}_{\mathbb{C}}(V, \mathbb{C})$ es un $\mathbb{C}[G]$ -módulo con $(gf)(v) = f(g^{-1}v)$.

Ejercicio 5.39. Sea G un grupo finito. Si V y W son $\mathbb{C}[G]$ -módulos de dimensión finita, entonces $V^* \otimes W \simeq \text{Hom}_{\mathbb{C}}(V, W)$ como $\mathbb{C}[G]$ -módulos.

Capítulo 6

Teoría de caracteres

Definición 6.1. Sea $\phi: G \rightarrow \mathbf{GL}(V)$ una representación. El **carácter** de ϕ es la función $\chi_\phi: G \rightarrow \mathbb{C}$, $\chi_\phi(g) = \text{traza}(\phi_g)$. Si ϕ es irreducible, χ_ϕ se dice un **carácter irreducible**. El **grado** de χ_ϕ es el número $\deg \chi_\phi = \deg \phi = \chi_\phi(1) = \dim V$.

pro:chi(1)

Proposición 6.2. Sea ϕ una representación con carácter χ y sea $g \in G$. Valen las siguientes afirmaciones:

- 1) $\chi(1) = \deg \phi$.
- 2) $\chi(g) = \chi(hgh^{-1})$ para todo $h \in G$.
- 3) $\chi(g)$ es suma de $\chi(1)$ raíces $|g|$ -ésimas de la unidad.
- 4) $\chi(g^{-1}) = \overline{\chi(g)}$.
- 5) $|\chi(g)| \leq \chi(1)$.

Demostración. La primera propiedad es evidente pues $\phi_1 = \text{id}$. La segunda:

$$\chi(hgh^{-1}) = \text{traza} \phi_{hgh^{-1}} = \text{traza}(\phi_h \phi_g \phi_h^{-1}) = \text{traza} \phi_g = \chi(g),$$

pues $\text{traza}(AB) = \text{traza}(BA)$ para todo A, B . La tercera es fácil pues la traza de ϕ_g es la suma de los autovalores de ϕ_g , que son raíces del polinomio $X^{|g|} - 1$. Para demostrar la cuarta afirmación supongamos que $\chi(g) = \lambda_1 + \dots + \lambda_k$, donde los λ_j son raíces de la unidad. Entonces

$$\overline{\chi(g)} = \sum_{j=1}^k \overline{\lambda_j} = \sum_{j=1}^k \lambda_j^{-1} = \text{traza} \phi_g^{-1} = \text{traza}(\phi_{g^{-1}}) = \chi(g^{-1}).$$

La última afirmación es evidente pues $\chi(g)$ es suma de raíces de la unidad. □

Si χ y ψ son caracteres de G , en particular son funciones $G \rightarrow \mathbb{C}$ y podemos entonces definir suma, producto y producto por escalares como

$$(\chi + \psi)(g) = \chi(g) + \psi(g), \quad (\chi\psi)(g) = \chi(g)\psi(g), \quad (\lambda\chi)(g) = \lambda\chi(g)$$

para $\lambda \in \mathbb{C}$. Sin embargo, estas funciones no necesariamente dan caracteres.

Teorema 6.3. *Sea G un grupo finito. Los caracteres irreducibles de G son linealmente independientes.*

Demostración. Sean S_1, \dots, S_k las clases de isomorfismos de los $\mathbb{C}[G]$ -módulos simples y sea $f: \mathbb{C}[G] \rightarrow M_{n_1}(\mathbb{C}) \times \dots \times M_{n_k}(\mathbb{C})$ el isomorfismo del teorema de Wedderburn. Para cada j tenemos $n_j = \dim S_j$, pues $M_{n_j}(\mathbb{C}) \simeq S_j \oplus \dots \oplus S_j$ (n_j -veces). Para cada $j \in \{1, \dots, k\}$ sea $e_j = f^{-1}(I_j) \in \mathbb{C}[G]$, donde I_j la matriz identidad de $M_{n_j}(\mathbb{C})$. Supongamos que $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. Si $\alpha = \sum_{g \in G} \lambda_g g \in \mathbb{C}[G]$, para cada $i \in \{1, \dots, k\}$ definimos $\chi_i(\alpha) = \sum_{g \in G} \lambda_g \chi_i(g)$. Vamos a demostrar que

$$\chi_i(e_j) = \begin{cases} \dim S_i & \text{si } i = j, \\ 0 & \text{en otro caso,} \end{cases}$$

para todo $i, j \in \{1, \dots, k\}$. Cada $\chi_j(g)$ es la traza de la restricción de la acción de g al simple S_j . En particular, como $e_i e_j = 0$ si $i \neq j$, tenemos $\chi_i(e_j) = 0$ si $i \neq j$. Como además e_j actúa por la identidad en S_j , tenemos $\chi_j(e_j) = \text{traza}(I_j) = \dim S_j$.

Sean $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ tales que $\sum_{i=1}^k \lambda_i \chi_i = 0$. Al evaluar esta expresión en cada e_j vemos que $\lambda_j = 0$ para todo j . \square

Proposición 6.4. *Si U y V son $\mathbb{C}[G]$ -módulos, entonces $\chi_{U \oplus V} = \chi_U + \chi_V$.*

Demostración. Sea $\{u_1, \dots, u_r\}$ una base de U y sea $\{v_1, \dots, v_s\}$ una base de V . Entonces $\{u_1, \dots, u_r, v_1, \dots, v_s\}$ es una base de $U \oplus V$. Sea $\rho: G \rightarrow \mathbf{GL}(U \otimes V)$ la representación que corresponde al módulo $U \oplus V$. Si $g \in G$, en esta base

$$\rho_g = \begin{pmatrix} \rho_g|_U & * \\ 0 & \rho_g|_V \end{pmatrix}.$$

Luego $\chi_{U \oplus V}(g) = \text{traza}(\rho_g) = \text{traza} \rho_g|_U + \text{traza} \rho_g|_V = \chi_U(g) + \chi_V(g)$. \square

Teorema 6.5. *Sea G un grupo finito. Si S_1, \dots, S_k son los representantes de las clases de isomorfismos de los $\mathbb{C}[G]$ -módulos simples y $V = a_1 S_1 \oplus \dots \oplus a_k S_k$, entonces*

$$\chi_V = a_1 \chi_1 + \dots + a_k \chi_k.$$

En particular, si U y V son $\mathbb{C}[G]$ -módulos, entonces $U \simeq V$ si y sólo si $\chi_U = \chi_V$.

Demostración. La primera afirmación se obtiene de la proposición anterior.

Supongamos que $U \simeq V$, es decir que existe un isomorfismo $f: U \rightarrow V$ de $\mathbb{C}[G]$ -módulos. Si $\rho: G \rightarrow \mathbf{GL}(U)$ es la representación que corresponde al módulo U y $\psi: G \rightarrow \mathbf{GL}(V)$ es la que corresponde al módulo V , entonces que f sea morfismo de módulos puede escribirse como $f \circ \rho_g \circ f^{-1} = \psi_g$. Luego

$$\chi_V(g) = \text{traza} \psi_g = \text{traza}(f \circ \rho_g \circ f^{-1}) = \text{traza} \rho_g = \chi_U(g).$$

Supongamos ahora que $\chi_U = \chi_V$. Como $\mathbb{C}[G]$ es semisimple, podemos escribir $U \simeq \bigoplus_{i=1}^k a_i S_i$ y también $V \simeq \bigoplus_{i=1}^k b_i S_i$ para ciertos $a_1, \dots, a_k, b_1, \dots, b_k \geq 0$. Como

$0 = \chi_U - \chi_V = \sum_{i=1}^k (a_i - b_i) \chi_i$ y además los χ_i son linealmente independientes, se concluye que $a_i = b_i$ para todo $i \in \{1, \dots, k\}$, es decir $U \simeq V$. \square

Proposición 6.6. Si G es un grupo finito y V y W son $\mathbb{C}[G]$ -módulos, entonces

- 1) $\chi_{V \otimes W} = \chi_V \chi_W$,
- 2) $\chi_{V^*} = \overline{\chi_V}$.

Demostración. Demostremos la primera afirmación. Sea $\phi: G \rightarrow \mathbf{GL}(V)$ la representación que corresponde a U y sea $\psi: G \rightarrow \mathbf{GL}(W)$ la representación que corresponde a W . Sabemos que ϕ y ψ son diagonalizables. Sea $g \in G$ y sea $\{v_1, \dots, v_n\}$ una base de autovectores de ϕ_g con autovalores $\lambda_1, \dots, \lambda_n$ y sea $\{w_1, \dots, w_m\}$ una base de autovectores de ψ_g con autovalores μ_1, \dots, μ_m . Cada $v_i \otimes w_j$ es autovectores de $\phi \otimes \psi$ de autovalor $\lambda_i \mu_j$ pues

$$g(v_i \otimes w_j) = gv_i \otimes gw_j = \lambda_i v_i \otimes \mu_j w_j = (\lambda_i \mu_j) v_i \otimes w_j.$$

Luego $\{v_i \otimes w_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ es base de autovectores y los $\lambda_i \mu_j$ son los autovalores de $\phi \otimes \psi$. Se concluye que

$$\chi_{V \otimes W}(g) = \sum_{i,j} \lambda_i \mu_j = \left(\sum_i \lambda_i \right) \left(\sum_j \mu_j \right) = \chi_V(g) \chi_W(g).$$

Demostremos la segunda afirmación. Sea $g \in G$, sea $\{v_1, \dots, v_n\}$ una base de autovectores de ϕ con autovalores $\lambda_1, \dots, \lambda_n$ y sea $\{f_1, \dots, f_n\}$ su base dual. Veamos que $\{f_1, \dots, f_n\}$ es base de autovectores con autovalores $\overline{\lambda_1}, \dots, \overline{\lambda_n}$. En efecto, si $gv_j = \lambda_j v_j$, entonces $g^{-1}v_j = \lambda_j^{-1}v_j = \overline{\lambda_j}v_j$ (observemos que como ϕ_g es inversible, los λ_j son no nulos). Luego

$$(gf_i)(v_j) = f_i(g^{-1}v_j) = \overline{\lambda_j} f_i(v_j) = \overline{\lambda_j} \delta_{ij}.$$

En conclusión

$$\chi_{V^*}(g) = \sum_{i=1}^n \overline{\lambda_i} = \overline{\chi_V(g)}.$$

\square

Como consecuencia, el producto de dos caracteres es un carácter. Esto nos permite demostrar que el conjunto de combinaciones lineales enteras de caracteres irreducibles es un anillo con las operaciones usuales.

Ejercicio 6.7. Demuestre que el carácter $\chi_{\text{Hom}_{\mathbb{C}}(U,V)}$ del módulo $\text{Hom}_{\mathbb{C}}(U,V)$ es igual a $\overline{\chi_U} \chi_V$.

exercise:cf(G)

Definición 6.8. Una $f: G \rightarrow \mathbb{C}$ se dice una **función de clases** (o funciones centrales) si $f(g) = f(hgh^{-1})$ para todo $g, h \in G$.

Vimos en la proposición 6.2 que los caracteres son funciones de clase.

Ejercicio 6.9.

- 1) Demuestre que el conjunto $\text{cf}(G)$ de funciones de clase $G \rightarrow \mathbb{C}$ es un subespacio vectorial de $L(G)$.
- 2) Demuestre que las funciones

$$\delta_K: G \rightarrow \mathbb{C}, \quad \delta_K(g) = \begin{cases} 1 & \text{si } g \in K, \\ 0 & \text{si } g \notin K, \end{cases}$$

donde $K \in \text{cl}(G)$, forman una base del conjunto $\text{cf}(G)$ de funciones de clases de G . En particular $\dim \text{cf}(G) = |\text{cl}(G)|$.

Proposición 6.10. *Los caracteres irreducibles forman una base del espacio de funciones de clases.*

Demostración. El conjunto $\text{Irr}(G)$ de caracteres irreducibles de G es linealmente independiente y además $|\text{Irr}(G)| = |\text{cl}(G)| = |\text{cf}(G)|$. \square

Si U es un $\mathbb{C}[G]$ -módulo, definimos

$$U^G = \{u \in U : g \cdot u = u \text{ para todo } g \in G\}.$$

lem:invariantes

Lema 6.11. $\dim U^G = \frac{1}{|G|} \sum_{x \in G} \chi_U(x)$.

Demostración. Sea $\alpha = \frac{1}{|G|} \sum_{x \in G} \rho_x: U \rightarrow U$. Primero vemos que $\alpha^2 = \alpha$. Como $\rho_g \circ \alpha = \frac{1}{|G|} \sum_{x \in G} \rho_{gx} = \alpha$, pues gx recorre todo G si x recorre todo G , entonces

$$\alpha(\alpha(u)) = \frac{1}{|G|} \sum_{g \in G} \rho_g(\alpha(u)) = \alpha(u)$$

para todo $u \in U$. En particular, α tiene autovalores 0 y 1. Sea V el autoespacio correspondiente al autovalor 1. Afirmamos que $V = U^G$. Si $v \in V$, entonces

$$\rho_g(v) = \rho_g(\alpha(v)) = \frac{1}{|G|} \sum_{x \in G} \rho_g \rho_x(v) = \frac{1}{|G|} \sum_{y \in G} \rho_y(v) = \alpha(v) = v,$$

pues si x recorre todo G , también lo hace gx . Recíprocamente, si $u \in U^G$ entonces $\rho_g(u) = u$ para todo $g \in G$. En particular,

$$\alpha(u) = \frac{1}{|G|} \sum_{x \in G} \rho_x(u) = \frac{1}{|G|} \sum_{x \in G} u = u.$$

En consecuencia, $\dim V = \text{traza}(\alpha) = \frac{1}{|G|} \sum_{g \in G} \text{traza}(\rho_g) = \frac{1}{|G|} \sum_g \chi_U(g)$. \square

Sea G un grupo finito. En el espacio de funciones $G \rightarrow \mathbb{C}$ definimos la operación

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}, \quad f, g: G \rightarrow \mathbb{C}.$$

Es fácil verificar que esta operación es un producto interno.

Teorema 6.12. Si U y V son $\mathbb{C}[G]$ -módulos, entonces

$$\langle \chi_U, \chi_V \rangle = \dim \text{Hom}_{\mathbb{C}[G]}(U, V).$$

Demostración. Primero observamos que $\text{Hom}_{\mathbb{C}[G]}(U, V)$ es un subespacio del conjunto $\text{Hom}_{\mathbb{C}}(U, V)$ de transformaciones lineales $U \rightarrow V$.

Veamos ahora $\text{Hom}_{\mathbb{C}[G]}(U, V) = \text{Hom}_{\mathbb{C}}(U, V)^G$. En efecto, si $f \in \text{Hom}_{\mathbb{C}[G]}(U, V)$, entonces

$$(g \cdot f)(u) = g \cdot f(g^{-1} \cdot u) = g \cdot (g^{-1} \cdot f(u)) = (gg^{-1}) \cdot f(u) = 1 \cdot f(u) = f(u)$$

para todo $g \in G$ y $u \in U$. Recíprocamente, si $f: U \rightarrow V$ es una transformación lineal tal que $g \cdot f = f$ para todo $g \in G$, entonces, en particular, $g^{-1} \cdot f = f$ y luego $(g^{-1} \cdot f)(u) = f(u)$ para todo $g \in G$ y $u \in U$, que es equivalente a $g \cdot f(u) = f(g \cdot u)$.

Luego

$$\begin{aligned} \dim \text{Hom}_{\mathbb{C}}(U, V)^G &= \dim \text{Hom}_{\mathbb{C}[G]}(U, V) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\text{Hom}_{\mathbb{C}[G]}(U, V)}(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_U(g)} \chi_V(g) = \langle \chi_V, \chi_U \rangle. \end{aligned}$$

Para terminar la demostración solamente hay que observar que

$$\langle \chi_U, \chi_V \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_U(g) \overline{\chi_V(g)} = \overline{\langle \chi_V, \chi_U \rangle}. \quad \square$$

Sea G un grupo finito y sean χ_1, \dots, χ_k los representantes de caracteres irreducibles de G . Para abreviar, simplemente diremos que χ_1, \dots, χ_k son los caracteres irreducibles de G y escribiremos

$$\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}.$$

Sean g_1, \dots, g_k los representantes de las clases de conjugación de G . Se define la **matriz de caracteres** (irreducibles) de G como la matriz $X \in \mathbb{C}^{k \times k}$ dada por

$$X_{ij} = \chi_i(g_j), \quad 1 \leq i, j \leq k.$$

Veremos a continuación dos resultados muy importantes. El primero es sobre la ortogonalidad de las filas de la matriz de caracteres.

Ejemplo 6.13. En este ejemplo veremos cómo calcular computacionalmente la tabla de caracteres de un grupo. Sabemos que \mathbb{S}_3 tiene tres clases de conjugación, por lo que $\text{Irr}(\mathbb{S}_3)$ tendrá tres elementos:

```
gap> S3 := SymmetricGroup(3);;
gap> irr := Irr(S3);;
gap> Size(irr);
3
gap> NrConjugacyClasses(S3);
```

Teorema 6.14 (Schur). Sea G un grupo finito. Si $\chi, \psi \in \text{Irr}(G)$, entonces

$$\langle \chi, \psi \rangle = \begin{cases} 1 & \text{si } \chi = \psi, \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración. Si S_1, \dots, S_k los $\mathbb{C}[G]$ -módulos simples, entonces

$$\langle \chi_i, \chi_j \rangle = \dim \text{Hom}_{\mathbb{C}[G]}(S_i, S_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{en otro caso,} \end{cases}$$

ya que, como los S_j son módulos simples, sabemos por el lema de Schur que $\text{Hom}_{\mathbb{C}[G]}(S_i, S_i) \simeq \mathbb{C}$ y $\text{Hom}_{\mathbb{C}[G]}(S_i, S_j) = \{0\}$ si $i \neq j$. \square

Ejemplo 6.15. Verifiquemos computacionalmente las relaciones de ortogonalidad de Schur en el caso del grupo simétrico \mathbb{S}_3 .

```
gap> S3 := SymmetricGroup(3);;
gap> irr := Irr(S3);
[ Character( CharacterTable( Sym( [ 1 .. 3 ] ) ), [ 1, -1, 1 ] ),
  Character( CharacterTable( Sym( [ 1 .. 3 ] ) ), [ 2, 0, -1 ] ),
  Character( CharacterTable( Sym( [ 1 .. 3 ] ) ), [ 1, 1, 1 ] ) ]
gap> Display(irr);
[ [ 1, -1, 1 ],
  [ 2, 0, -1 ],
  [ 1, 1, 1 ] ]
gap> ScalarProduct(irr[1], irr[1]);
1
gap> ScalarProduct(irr[1], irr[2]);
0
gap> ScalarProduct(irr[1], irr[3]);
0
gap> ScalarProduct(irr[2], irr[2]);
1
gap> ScalarProduct(irr[2], irr[3]);
0
gap> ScalarProduct(irr[3], irr[3]);
1
```

El teorema de Schur tiene muchas aplicaciones. Por ejemplo:

- 1) $\text{Irr}(G)$ es una base ortonormal del espacio $\text{cf}(G)$ de funciones de clases de G .
- 2) Si $\alpha = \sum_{i=1}^k a_i \chi_i$ y $\beta = \sum_{i=1}^k b_i \chi_i$, entonces $\langle \alpha, \beta \rangle = \sum_{i=1}^k a_i b_i$.
- 3) Si $\alpha = \sum_{i=1}^k a_i \chi_i$, entonces $\alpha = \sum_{i=1}^k \langle \alpha, \chi_i \rangle \chi_i$.

Corolario 6.16. Si G es un grupo finito y S_1, \dots, S_k son las clases de isomorfismos de módulos simples, entonces

$$\mathbb{C}[G] \simeq (\dim S_1)S_1 \oplus \dots \oplus (\dim S_k)S_k.$$

Demostración. Sabemos que la representación regular puede escribirse como

$$\mathbb{C}[G] \simeq a_1 S_1 \oplus \cdots \oplus a_k S_k,$$

para ciertos enteros no negativos a_1, \dots, a_k unívocamente determinados. Supongamos que $G = \{g_1, \dots, g_n\}$. Sea L la representación regular (a izquierda) de G , es decir $L_g(g_j) = gg_j$ para todo $j \in \{1, \dots, n\}$. La matriz de L_g en la base g_1, \dots, g_n es

$$(L_g)_{ij} = \begin{cases} 1 & \text{si } g_i = gg_j, \\ 0 & \text{en otro caso.} \end{cases}$$

En particular, el caracter χ_L de la representación regular cumple

$$\chi_L(g) = \begin{cases} |G| & \text{si } g = 1, \\ 0 & \text{en otro caso.} \end{cases}$$

La primera relación de ortogonalidad de Schur implica que $a_i = \langle \chi_L, \chi_i \rangle$ para todo i , es decir $\chi_L = \sum_{i=1}^k \langle \chi_L, \chi_i \rangle \chi_i$. Como para cada j se tiene

$$\langle \chi_L, \chi_j \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_L(g) \overline{\chi_j(g)} = \overline{\chi_j(1)} = \chi_j(1) = \dim S_j,$$

se concluye que $\mathbb{C}[G] \simeq \bigoplus_{i=1}^k (\dim S_i) S_i$. □

Ejercicio 6.17. Sea α un caracter de G y sea $n \in \{1, 2, 3\}$. Demuestre que α es suma de n irreducibles si y sólo si $\langle \alpha, \alpha \rangle = n$.

Veamos ahora la segunda relación de ortogonalidad de Schur.

Teorema 6.18. Sean G un grupo finito y $g, h \in G$. Entonces

$$\sum_{\chi \in \text{Irr}(G)} \chi(g) \overline{\chi(h)} = \begin{cases} |C_G(g)| & \text{si } g \text{ y } h \text{ son conjugados,} \\ 0 & \text{en otro caso.} \end{cases}$$

En particular, las columnas de X son ortogonales y la matriz X es inversible.

Demostración. Supongamos que g_1, \dots, g_r son los representantes de las clases de conjugación de G y que $\text{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. Entonces

$$\langle \chi_i, \chi_j \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \frac{1}{|G|} \sum_{k=1}^r c_k \chi_i(g_k) \overline{\chi_j(g_k)},$$

donde cada c_k es el tamaño de la clase de conjugación de g_k . Matricialmente,

$$I = \frac{1}{|G|} XDX^*,$$

donde I es la matriz identidad de $r \times r$, D es la matriz diagonal que tiene a c_1, \dots, c_r en la diagonal principal y $X^* = \overline{X}^T$. Entonces¹

$$I = \frac{1}{|G|} X^* X D,$$

es decir $|G|D^{-1} = X^* X$. Luego

$$\sum_{k=1}^r \overline{\chi_k(g_i)} \chi_k(g_j) = \begin{cases} |C_G(g_j)| & \text{si } i = j, \\ 0 & \text{en otro caso,} \end{cases}$$

que es lo que queríamos demostrar. \square

Ejercicio 6.19. Sea G un grupo finito. Si χ es un caracter irreducible de G y ϕ es un caracter de grado uno, entonces $\chi \otimes \phi$ es un caracter irreducible de G .

theorem:Solomon

Teorema 6.20 (Solomon). Sean G un grupo finito, $\text{Irr}(G) = \{\chi_1, \dots, \chi_r\}$ y g_1, \dots, g_r los representantes de las clases de conjugación de G . Si $i \in \{1, \dots, r\}$, entonces

$$\sum_{j=1}^r \chi_i(g_j) \in \mathbb{N}_0.$$

Demostración. Sea V el espacio vectorial con base $\{e_g : g \in G\}$. Hagamos actuar a G en G por conjugación y sea $\rho : G \rightarrow \mathbf{GL}(V)$, $\rho_g(e_h) = e_{ghg^{-1}}$. Observemos que en la base $\{e_g : g \in G\}$ la matriz de ρ_g es

$$(\rho_g)_{ij} = \begin{cases} 1 & \text{si } g_i g = g g_j, \\ 0 & \text{en otro caso.} \end{cases}$$

Sea χ el caracter de la representación ρ . Entonces

$$\chi(g) = \text{traza } \rho_g = \sum_k (\rho_g)_{kk} = |\{k : g_k g = g g_k\}| = |C_G(g)|.$$

Sean $m_1, \dots, m_r \in \mathbb{N}_0$ tales que

$$\chi = \sum_{i=1}^r m_i \chi_i.$$

Entonces, si c_j es el tamaño de la clase de conjugación de g_j , la cantidad m_i de veces que la representación irreducible con caracter χ_i aparece en ρ es igual a

$$m_i = \langle \chi, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi_i(g)} = \frac{1}{|G|} \sum_{j=1}^r c_j |C_G(g_j)| \overline{\chi_i(g_j)} = \sum_{j=1}^r \overline{\chi_i(g_j)}.$$

Luego $\sum_{j=1}^r \chi_i(g_j) = \overline{m_i} = m_i \in \mathbb{N}_0$. \square

¹ Si $A, B \in \mathbb{C}^{s \times s}$ son tales que $AB = I$ entonces $BA = I$.

Capítulo 7

El grado de un caracter

Nuestro objetivo ahora es demostrar el teorema de Frobenius, que afirma que el grado de una representación irreducible es un divisor del orden del grupo.

Definición 7.1. Sea $\alpha \in \mathbb{C}$. Se dice que α es un **entero algebraico** si α es raíz de un polinomio mónico con coeficientes en \mathbb{Z} .

Escribiremos \mathbb{A} para denotar al conjunto de enteros algebraicos.

Toda raíz n -ésima de la unidad es un entero algebraico. Los autovalores de una matriz $A \in \mathbb{Z}^{n \times n}$ son enteros algebraicos.

pro:Z

Proposición 7.2. $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$.

Demostración. Sea $m/n \in \mathbb{Q}$ con $\text{mcd}(m, n) = 1$ y $n > 0$. Supongamos que m/n es raíz del polinomio $t^k + a_{k-1}t^{k-1} + \dots + a_1t + a_0 \in \mathbb{Z}[t]$. Entonces

$$0 = (m/n)^k + a_{k-1}(m/n)^{k-1} + \dots + a_1m/n + a_0.$$

Al multiplicar por n^k ,

$$0 = m^k + a_{k-1}m^{k-1}n + \dots + a_1mn^{k-1} + a_0n^k,$$

y entonces n divide a m^k pues podemos escribir

$$m^k = -n(a_{k-1}m^{k-1} + \dots + a_1mn^{k-2} + a_0n^{k-1}).$$

Como m y n son coprimos se concluye así que $m/n \in \mathbb{Z}$ pues $n \in \{-1, 1\}$. □

lem:matriz_entera

Lema 7.3. Sea $x \in \mathbb{C}$. Entonces $x \in \mathbb{A}$ si y sólo si x es autovalor de una matriz entera.

Demostración. Supongamos que $x \in \mathbb{A}$, digamos que x es raíz de

$$f = t^n + a_{n-1}t^{n-1} + \dots + a_1t + a_0 \in \mathbb{Z}[t].$$

Entonces x es autovalor de la matriz compañera de f :

$$C(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Recíprocamente, si x es autovalor de una matriz $A \in \mathbb{Z}^{n \times n}$, entonces x es raíz del polinomio mónico $f(t) = \det(tI - A) \in \mathbb{Z}^{n \times n}$. \square

theorem:subanillo

Teorema 7.4. \mathbb{A} es un subanillo de \mathbb{C} .

Demostración. Sean $\alpha, \beta \in \mathbb{A}$. Gracias el lema anterior podemos suponer que α es autovalor de $A \in \mathbb{Z}^{n \times n}$ y que β es autovalor de $B \in \mathbb{Z}^{m \times m}$, digamos $Av = \alpha v$ y $Bw = \beta w$. Como

$$(A \otimes I_{m \times m} + I_{n \times n} \otimes B)(v \otimes w) = (\alpha + \beta)(v \otimes w), \quad (A \otimes B)(v \otimes w) = \alpha\beta(v \otimes w),$$

se concluye que $\alpha + \beta \in \mathbb{A}$ y que $\alpha\beta \in \mathbb{A}$. \square

theorem:chi(g) in A

Teorema 7.5. Si χ es un caracter de un grupo finito G , entonces $\chi(g) \in \mathbb{A}$ para todo $g \in G$.

Demostración. Sea ρ una representación con caracter χ . Sabemos que ρ_g es diagonalizable con autovalores $\lambda_1, \dots, \lambda_k$. Los λ_j son enteros algebraicos por ser raíces de la unidad. Luego $\chi(g) = \text{traza } \rho_g = \lambda_1 + \cdots + \lambda_k \in \mathbb{A}$. \square

lem:combinacion_lineal

Lema 7.6. Sea $x \in \mathbb{C}$. Entonces $x \in \mathbb{A}$ si y sólo si existen $z_1, \dots, z_k \in \mathbb{C}$ no todos cero tales que $xz_i = \sum_{j=1}^k a_{ij}z_j$, $a_{ij} \in \mathbb{Z}$, para todo $i \in \{1, \dots, k\}$.

Demostración. Supongamos que $x \in \mathbb{A}$ es raíz del polinomio

$$t^k + a_{k-1}t^{k-1} + \cdots + a_1t + a_0 \in \mathbb{Z}[t].$$

Sean $z_i = x^{i-1}$, $i \in \{1, \dots, k\}$. Entonces $xz_i = x^i = z_{i+1}$ para todo $i \in \{1, \dots, k-1\}$ y $xz_k = x^k = -a_0 - \cdots - a_{k-1}x^{k-1}$.

Demostremos la otra implicación. Sean $A = (a_{ij})$ y $Z = (z_1, \dots, z_k)^T$. Entonces $AZ = xZ$ pues para cada $i \in \{1, \dots, k\}$ se tiene

$$(AZ)_i = \sum_{j=1}^k a_{ij}z_j = xz_i = (xZ)_i.$$

Como $Z \neq 0$, x es autovalor de la matriz $A \in \mathbb{Z}^{k \times k}$. Luego $x \in \mathbb{A}$. \square

Necesitaremos la siguiente aplicación del lema de Schur.

Lema 7.7. Si V es un $\mathbb{C}[G]$ -módulo simple y $T: V \rightarrow V$ es un morfismo de $\mathbb{C}[G]$ -módulos, entonces $T = \lambda \text{id}$ para algún $\lambda \in \mathbb{C}$.

Demostración. Como estamos sobre los números complejos, existe un autovalor $\lambda \in \mathbb{C}$ de T . Luego $T - \lambda \text{id}$ no es inversible y entonces, como V es simple, el lema de Schur implica que $T - \lambda \text{id} = 0$. \square

theorem:algebraic

Teorema 7.8. Sean G un grupo finito, $g \in G$ y $\chi \in \text{Irr}(G)$. Si K es la clase de conjugación de g en G , entonces

$$\frac{|K|\chi(g)}{\chi(1)} \in \mathbb{A}.$$

Demostración. Sea ϕ una representación con caracter χ . Sean C_1, \dots, C_r las clases de conjugación de G . Para cada $i \in \{1, \dots, r\}$ definimos

$$T_i = \sum_{x \in C_i} \phi_x.$$

Vamos a demostrar que $T_i = \left(\frac{|C_i|\chi(C_i)}{\chi(1)} \right) \text{id}$, donde $\chi(C_i)$ denota el valor de χ en la clase de conjugación C_i . Cada T_i es un morfismo de representaciones, pues

$$\phi_g \circ T_i \circ \phi_{g^{-1}} = \sum_{x \in C_i} \phi_g = \sum_{x \in C_i} \phi_{gxg^{-1}} = \sum_{x \in C_i} \phi_x = T_i,$$

y entonces el lema de Schur implica que $T_i = \lambda \text{id}$ para algún $\lambda \in \mathbb{C}$.

Calculemos ahora λ :

$$\chi(1)\lambda = \text{traza}(\lambda \text{id}) = \text{traza}(T_i) = \sum_{x \in C_i} \text{traza}(\phi_x) = \sum_{x \in C_i} \chi(x) = \chi(C_i)|C_i|.$$

Veamos ahora que $T_i T_j = \sum_{k=1}^r a_{ijk} T_k$, donde $a_{ijk} \in \mathbb{N}_0$. Calculamos

$$T_i T_j = \sum_{x \in C_i} \sum_{y \in C_j} \phi_x \phi_y = \sum_{\substack{x \in C_i \\ y \in C_j}} \phi_{xy} = \sum_{g \in G} a_{ijg} \phi_g,$$

donde a_{ijg} es la cantidad de veces que g puede escribirse como $g = xy$ con $x \in C_i$, $y \in C_j$. Veamos que los a_{ijg} dependen únicamente de la clase de conjugación de g . En efecto, sea

$$X_g = \{(x, y) \in C_i \times C_j : xy = g\}.$$

Si $h = kgk^{-1}$, entonces la función

$$X_g \rightarrow X_h, \quad (x, y) \mapsto (kxk^{-1}, kyk^{-1})$$

está bien definida y es biyectiva con inversa $X_h \rightarrow X_g, (a, b) \mapsto (k^{-1}ak, k^{-1}bk)$. En particular, $|X_g| = |X_h|$.

Como los a_{ijg} dependen de la clase de conjugación de g ,

$$T_i T_j = \sum_{g \in G} a_{ijg} \phi_g = \sum_{k=1}^r \sum_{g \in C_k} a_{ijg} \phi_g = \sum_{k=1}^r a_{ijk} \sum_{g \in C_k} \phi_g = \sum_{k=1}^r a_{ijk} T_k,$$

tal como queríamos demostrar. De esta igualdad obtenemos:

$$\left(\frac{|C_i|}{\chi(1)}\chi(C_i)\right)\left(\frac{|C_j|}{\chi(1)}\chi(C_j)\right) = \sum_{k=1}^s a_{ijk} \left(\frac{|C_k|}{\chi(1)}\chi(C_k)\right), \quad (7.1) \quad \boxed{\text{eq:omega}}$$

y se concluye que $|C_i|\chi(C_i)/\chi(1) \in \mathbb{A}$ gracias al lema 7.6. \square

`theorem:chi(1) || G|`

Teorema 7.9 (Frobenius). *Sean G un grupo finito y $\chi \in \text{Irr}(G)$. Entonces $\chi(1)$ divide al orden de G .*

Demostración. Sea ϕ una representación irreducible con caracter χ . Como χ es irreducible, $1 = \langle \chi, \chi \rangle$ y entonces

$$\frac{|G|}{\chi(1)} = \frac{|G|}{\chi(1)} \langle \chi, \chi \rangle = \sum_{g \in G} \frac{\chi(g)}{\chi(1)} \overline{\chi(g)},$$

Sean C_1, \dots, C_r las clases de conjugación de G . Entonces

$$\frac{|G|}{\chi(1)} = \sum_{i=1}^r \sum_{g \in C_i} \frac{\chi(g)}{\chi(1)} \overline{\chi(g)} = \sum_{i=1}^r \left(\frac{|C_i|}{\chi(1)}\chi(C_i)\right) \overline{\chi(C_i)} \in \mathbb{A},$$

por los teoremas 7.4, 7.5 y 7.8. Luego $|G|/\chi(1) \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$ (proposición 7.2). En particular, $\chi(1)$ divide al orden de G . \square

`xca:p2_abeliano`

Ejercicio 7.10. Sea p un primo. Demuestre que todo grupo de orden p^2 es abeliano.

`xca:pq`

Ejercicio 7.11. Sean $p < q$ primos tales que $q \not\equiv 1 \pmod{p}$. Demuestre que todo grupo de orden pq es abeliano.

Veamos una aplicación.

Teorema 7.12. *Si G es un grupo finito simple, $\chi(1) \neq 2$ para todo $\chi \in \text{Irr}(G)$.*

Demostración. Sea $\chi \in \text{Irr}(G)$ tal que $\chi(1) = 2$ y sea $\rho: G \rightarrow \mathbf{GL}_2(\mathbb{C})$ una representación de G con caracter χ . Como G es simple y $\ker \rho$ es normal en G , $\ker \rho = \{1\}$, es decir ρ es inyectiva.

Como G tiene un caracter irreducible de grado dos, G es no abeliano, entonces $[G, G] = G$ pues $[G, G] \neq \{1\}$. Sabemos que G tiene exactamente $(G : [G, G])$ caracteres irreducibles de grado uno, entonces el único caracter irreducible de G de grado uno es el trivial. La función

$$G \rightarrow \mathbb{C}^\times, \quad g \mapsto \det(\rho_g),$$

es un morfismo de grupos, luego es un caracter de grado uno. Como tiene que ser el caracter trivial, $\det(\rho_g) = 1$ para todo $g \in G$.

Por el teorema de Frobenius, $\chi(1)$ divide al orden de G y luego G tiene orden par. Sea $x \in G$ un elemento de orden dos. Como ρ es inyectiva, ρ_x tiene orden dos en $\mathbf{GL}_2(\mathbb{C})$. Como ρ_x es diagonalizable, existe $C \in \mathbf{GL}_2(\mathbb{C})$ tal que

$$C\rho_x C^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix},$$

donde $\lambda, \mu \in \{-1, 1\}$ pues ρ_x^2 es la matriz identidad. Como $1 = \det(\rho_g) = \lambda\mu$, entonces $\lambda = \mu = -1$, lo que implica que la matriz ρ_x es central en $\mathbf{GL}_2(\mathbb{C})$. Como ρ es inyectiva, x es también central en G , es decir $xg = gx$ para todo $g \in G$. Luego $\langle x \rangle$ es un subgrupo propio normal no trivial de G . \square

Vamos a demostrar una mejora del teorema de Frobenius.

Proposición 7.13. Sean G y G_1 dos grupos finitos. Si ρ es una representación irreducible de G y ρ_1 es una representación irreducible de G_1 , entonces $\rho \otimes \rho_1$ es una representación irreducible de $G \times G_1$.

Demostración. Sea χ el caracter de ρ y χ_1 el caracter de ρ_1 . Como ρ y ρ_1 son irreducibles, $\langle \chi, \chi \rangle = \langle \chi_1, \chi_1 \rangle = 1$. Entonces

$$\begin{aligned} \langle \chi \otimes \chi_1, \chi \otimes \chi_1 \rangle &= \frac{1}{|G \times G_1|} \sum_{(g, g_1) \in G \times G_1} \chi(g) \chi_1(g_1) \overline{\chi(g) \chi_1(g_1)} \\ &= \left(\frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi(g)} \right) \left(\frac{1}{|G_1|} \sum_{g_1 \in G_1} \chi_1(g_1) \overline{\chi_1(g_1)} \right) \\ &= \langle \chi, \chi \rangle \langle \chi_1, \chi_1 \rangle = 1. \end{aligned}$$

Luego $\rho \otimes \rho_1$ es irreducible. \square

Ejercicio 7.14. Sean G y G_1 grupos finitos. Demuestre que toda representación irreducible de $G \times G_1$ es de la forma $\rho \otimes \rho_1$, donde ρ es una representación irreducible de G y ρ_1 es una representación irreducible de G_1 .

Teorema 7.15 (Schur). Sean G un grupo finito y $\chi \in \text{Irr}(G)$. Entonces $\chi(1)$ divide al índice $(G : Z(G))$.

Demostración. Sea $\rho : G \rightarrow \mathbf{GL}(V)$, $g \mapsto \rho_g$, una representación con caracter χ . Si $z \in Z(G)$, entonces ρ_z conmuta con ρ_g para todo $g \in G$. Por el lema de Schur, $\rho_z(v) = \lambda(z)v$ para todo $v \in V$. Sea $\lambda : Z(G) \rightarrow \mathbb{C}^\times$, $z \mapsto \lambda(z)$. Como

$$\lambda(z_1 z_2)v = \rho_{z_1 z_2}(v) = \rho_{z_1} \rho_{z_2}(v) = \lambda(z_1) \lambda(z_2)v$$

para todo $v \in V$, λ es morfismo de grupos.

Para $n \in \mathbb{N}$ sea $G^n = G \times \cdots \times G$ (n -veces) y sea

$$\sigma : G^n \rightarrow \mathbf{GL}(V^{\otimes n}), \quad (g_1, \dots, g_n) \mapsto \rho_{g_1} \otimes \cdots \otimes \rho_{g_n}.$$

La representación σ tiene caracter χ^n y es irreducible. Si $z_1, \dots, z_n \in Z(G)$, entonces, como

$$\begin{aligned}
\sigma(z_1, \dots, z_n)(v_1 \otimes \dots \otimes v_n) &= z_1 \cdot v_1 \otimes \dots \otimes z_n \cdot v_n \\
&= \lambda(z_1) \dots \lambda(z_n)(v_1 \otimes \dots \otimes v_n) \\
&= \lambda(z_1 \dots z_n)(v_1 \otimes \dots \otimes v_n),
\end{aligned}$$

el subgrupo

$$H = \{(z_1, \dots, z_n) \in Z(G) \times \dots \times Z(G) : z_1 \dots z_n = 1\}$$

de G^n actúa trivialmente en $V^{\otimes n}$, lo que nos da una representación

$$\tau: G^n/H \rightarrow \mathbf{GL}(V^{\otimes n}),$$

es decir una estructura de $\mathbb{C}[G^n/H]$ -módulo sobre $V^{\otimes n}$. Como $V^{\otimes n}$ es un $\mathbb{C}[G^n]$ -módulo simple, $V^{\otimes n}$ también es simple como $\mathbb{C}[G^n/H]$ -módulo. Por el teorema de Frobenius aplicado al $\mathbb{C}[G]$ -módulo V sabemos que el grado $\chi(1)$ divide a $|G|$, digamos $|G| = \chi(1)s$ para algún $s \in \mathbb{Z}$. Ese mismo teorema, ahora aplicado al $\mathbb{C}[G^n/H]$ -módulo $V^{\otimes n}$, nos dice que el grado $\chi(1)^n$ de τ divide al entero $(G^n : H) = (G : Z(G))^{n-1} |G|$, digamos $|G|(G : Z(G))^{n-1} = \chi(1)^n r$ para algún $r \in \mathbb{Z}$. Sean $a, b \in \mathbb{Z}$ tales que $\text{mcd}(a, b) = 1$ y

$$\frac{a}{b} = \frac{(G : Z(G))}{\chi(1)}.$$

Como

$$s \frac{a^{n-1}}{b^{n-1}} = s \frac{(G : Z(G))^{n-1}}{\chi(1)^{n-1}} = \frac{|G|(G : Z(G))^{n-1}}{\chi(1)^n} \in \mathbb{Z},$$

Luego b^{n-1} divide a s . Como n es arbitrario, se sigue que $b = 1$. \square

La demostración anterior fue descubierta por Tate y está basada en el "truco del producto tensorial". Para más información sobre este truco referimos al blog de Terence Tao: <https://terrytao.wordpress.com>. Allí encontraremos una entrada dedicada exclusivamente muchas de las aplicaciones de este poderoso truco.

El teorema de Schur también puede generalizarse. En 1951 Itô demostró el siguiente resultado:

Teorema 7.16 (Itô). *Si G es un grupo finito y $\chi \in \text{Irr}(G)$, entonces $\chi(1)$ divide a $(G : A)$ para todo subgrupo normal abeliano A .*

La demostración, que no es más difícil que la demostración del teorema de Frobenius o del teorema de Schur que vimos en este capítulo, puede consultarse por ejemplo en [30, §8.1].

Para terminar con el capítulo vamos a mencionar algunas de las conjeturas de conteo más famosas. En 1971 McKay hizo la siguiente conjetura:

Conjetura 7.17 (McKay). Sea p un primo. Si G es un grupo finito y $P \in \text{Syl}_p(G)$, entonces

$$|\{\chi \in \text{Irr}(G) : p \nmid \chi(1)\}| = |\{\psi \in \text{Irr}(N_G(P)) : p \nmid \psi(1)\}|.$$

En la versión original de McKay el grupo G es simple y el primo es $p = 2$. La versión general de la conjetura fue en realidad formulada por Alperin en [1] e independientemente por Isaacs en [18].

La conjetura de McKay permanece abierta y es uno de los problemas abiertos más importantes en la teoría de representaciones de grupos finitos sobre los números complejos.

Se sabe que la conjetura de McKay es verdadera para varias clases de grupos. Isaacs la demostró para grupos resolubles, ver por ejemplo [18, 20]. Malle y Späth demostraron que la conjetura de McKay es cierta para el primo $p = 2$.

Teorema 7.18 (Malle–Späth). *Si G es un grupo finito y $P \in \text{Syl}_2(G)$, entonces*

$$|\{\chi \in \text{Irr}(G) : 2 \nmid \chi(1)\}| = |\{\psi \in \text{Irr}(N_G(P)) : 2 \nmid \psi(1)\}|.$$

La demostración aparece en [26] y utiliza la clasificación de grupos simples finitos. Se basa en demostrar que todo grupo simple cumple con ciertas propiedades bastante más complicadas que la conjetura de McKay, un resultado de Isaacs, Malle y Navarro [21].

Podemos verificar computacionalmente algunos casos pequeños de la conjetura de McKay con la siguiente función:

```
gap> McKay := function(G, p)
> local N, n, m;
> N := Normalizer(G, SylowSubgroup(G, p));
> n := Number(Irr(G), x->Degree(x) mod p <> 0);
> m := Number(Irr(N), x->Degree(x) mod p <> 0);
> if n = m then
> return true;
> else
> return false;
> fi;
> end;
function( G, p ) ... end
```

Como ejemplo vamos a verificar computacionalmente la conjetura de McKay para el grupo de Mathieu M_{11} . Se sabe que M_{11} es un grupo simple de orden 7920.

```
gap> M11 := MathieuGroup(11);;
gap> PrimeDivisors(Order(M11));
[ 2, 3, 5, 11 ]
gap> McKay(M11, 2);
true
gap> McKay(M11, 3);
true
gap> McKay(M11, 5);
true
gap> McKay(M11, 11);
true
```

La siguiente conjetura es un refinamiento de la conjetura de McKay y fue formulada por Isaacs y Navarro a principios del siglo XXI:

Conjetura 7.19 (Isaacs–Navarro). Sean p un primo y $k \in \mathbb{Z}$. Si G es un grupo finito y $P \in \text{Syl}_p(G)$, entonces

$$\begin{aligned} & |\{\chi \in \text{Irr}(G) : p \nmid \chi(1) \text{ y } \chi(1) \equiv \pm k \pmod{p}\}| \\ &= |\{\psi \in \text{Irr}(N_G(P)) : p \nmid \psi(1) \text{ y } \psi(1) \equiv \pm k \pmod{p}\}|. \end{aligned}$$

Aunque la conjetura de Isaacs–Navarro en general permanece abierta, se sabe que es verdadera para varias clases de grupos, por ejemplo para grupos resolubles, para los 26 grupos simples esporádicos y para el grupo simétrico, ver por ejemplo [22].

Para verificar la conjetura de Isaacs–Navarro en ejemplos de orden pequeño podemos utilizar el siguiente código:

```
gap> IsaacsNavarro := function(G, k, p)
> local mG, mN, N;
> N := Normalizer(G, SylowSubgroup(G, p));
> mG := Number(Filtered(Irr(G), x->Degree(x) \
> mod p <> 0), x->Degree(x) mod p in [-k,k] mod p);
> mN := Number(Filtered(Irr(N), x->Degree(x) \
> mod p <> 0), x->Degree(x) mod p in [-k,k] mod p);
> if mG = mN then
> return mG;
> else
> return false;
> fi;
> end;
function( G, k, p ) ... end
```

Dejamos como ejercicio verificar la conjetura de Isaacs–Navarro por ejemplo para el grupo de Mathieu M_{11} .

Capítulo 8

Ejemplos de tablas de caracteres

Sea G un grupo finito y sean χ_1, \dots, χ_r los caracteres irreducibles de G . Sin pérdida de generalidad podemos suponer que χ_1 es el carácter trivial. Sabemos que r es igual a la cantidad de clases de conjugación de G . Como además cada χ_j es constante en las clases de conjugación de G , los caracteres de G quedan completamente determinados si conocemos el valor de cada χ_j en los representantes de las r clases de conjugación de G . Consideramos entonces la **tabla de caracteres** de G

	1	k_2	\cdots	k_r
	1	g_2	\cdots	g_r
χ_1	1	1	\cdots	1
χ_2	n_2	$\chi_2(g_2)$	\cdots	$\chi_2(g_r)$
\vdots	\vdots	\vdots	\ddots	\vdots
χ_r	n_r	$\chi_r(g_2)$	\cdots	$\chi_r(g_r)$

donde los n_j son los grados de las representaciones irreducibles de G y k_j es el tamaño de la clase de conjugación del elemento g_j en G para todo $j \in \{1, \dots, r\}$.

Ejemplo 8.1. Sea $G = \langle g \rangle$ el grupo cíclico de n elementos. Sea λ una raíz primitiva n -ésima de la unidad. Para cada i sea V_i un espacio vectorial de dimensión uno con base $\{v\}$. Cada V_i es un $\mathbb{C}[G]$ -módulo con

$$g \cdot v = \lambda^{i-1} v.$$

Además cada V_i es simple pues $\dim V_i = 1$. El carácter χ_i de V_i está dado por $\chi_i(g^m) = \lambda^{m(i-1)}$ para todo $m \in \{1, \dots, n\}$. Como los χ_1, \dots, χ_n son todos distintos y G admite n representaciones irreducibles, los χ_j son los caracteres de todas las representaciones irreducibles de G . La tabla de caracteres es fácil de calcular:

	1	1	1	...	1
	1	g	g^2	...	g^{n-1}
χ_1	1	1	1	...	1
χ_2	1	λ	λ^2	...	λ^{n-1}
χ_3	1	λ^2	λ^4	...	λ^{n-2}
\vdots	\vdots	\vdots	\vdots	\ddots	\vdots
χ_n	1	λ^{n-1}	λ^{n-2}	...	λ

Para dar un ejemplo computacional concreto expondremos la tabla de caracteres del grupo cíclico de orden cuatro.

```
gap> C4 := CyclicGroup(4);;
gap> T := CharacterTable(C4);;
gap> Display(T);
CT1
```

```
      2      2      2      2      2
      1a 4a 2a 4b
```

```
X.1      1      1      1      1
X.2      1     -1      1     -1
X.3      1      A     -1     -A
X.4      1     -A     -1      A
```

```
A = E(4)
   = Sqrt(-1) = i
```

Hay varias observaciones que debemos hacer:

- 1) El símbolo $E(4)$ denota a una raíz cuarta primitiva de la unidad.
- 2) Si bien la función `CharacterTable` se usa para calcular la tabla de caracteres de un grupo, esta función calcula algunas otras cosas. Por ejemplo:

```
gap> OrdersClassRepresentatives(T);
[ 1, 4, 2, 4 ]
gap> SizesCentralizers(T);
[ 4, 4, 4, 4 ]
gap> SizesConjugacyClasses(T);
[ 1, 1, 1, 1 ]
```

Como todo grupo abeliano finito es producto directo de grupos abelianos finitos y vimos que todo caracter irreducible de un producto directo es producto de caracteres irreducibles, es posible calcular tablas de caracteres de grupos abelianos finitos.

Ejemplo 8.2. Calculemos ahora la tabla de caracteres de $C_2 \times C_2 = \{1, a, b, ab\}$:

	1	1	1	1
	1	a	b	ab
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

Computacionalmente:

```
gap> Display(CharacterTable(AbelianGroup([2,2])));
CT2
```

```

      2      2      2      2      2
      1a 2a 2b 2c
X.1      1      1      1      1
X.2      1     -1      1     -1
X.3      1      1     -1     -1
X.4      1     -1     -1      1
```

Obviamente la forma en la que **GAP** ordena a los caracteres irreducibles de un grupo no tiene por qué coincidir con la forma en la que nosotros los ordenamos.

Ejemplo 8.3. Vimos que el grupo simétrico \mathbb{S}_3 tiene tres clases de conjugación con representantes id , (12) y (123) . La tabla de caracteres es entonces

	1	3	2
	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

¿Cómo fue que calculamos esta tabla de caracteres? Los caracteres de grado uno fueron muy fáciles de calcular. Para calcular la tercera fila de la tabla podemos utilizar la representación irreducible

$$(12) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

pues es irreducible y además

$$\chi_3((12)) = \text{traza} \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = 0,$$

$$\chi_3((123)) = \chi_3((12)(23)) = \text{traza} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = -1.$$

Es importante mencionar que podríamos haber calculado la tercera fila de la tabla sin conocer explícitamente la representación irreducible. Podríamos por ejemplo

usar la representación regular. Sabemos que el carácter de la representación regular L está dado por

$$\chi_L(g) = \begin{cases} 6 & \text{si } g = \text{id}, \\ 0 & \text{si } g \neq \text{id}. \end{cases}$$

Luego la ecuación $0 = \chi_L((12)) = 1 - 1 + 2\chi_3((12))$ nos dice que $\chi_3((12)) = 0$ y la ecuación $0 = \chi_L((123)) = 1 + 1 + 2\chi_3((123))$ nos dice que $\chi_3((123)) = -1$.

Alternativamente podríamos haber usado alguna de las relaciones de ortogonalidad. Por ejemplo si $\chi_3((12)) = a$ y $\chi_3((123)) = b$, entonces obtenemos $a = 0$ y $b = -1$ al resolver

$$0 = \langle \chi_3, \chi_1 \rangle = \frac{1}{6}(2 + 3a + 2b),$$

$$0 = \langle \chi_3, \chi_2 \rangle = \frac{1}{6}(2 - 3a + 2b).$$

Para ver qué es lo que puede obtenerse con la función `CharacterTable` hacemos lo siguiente:

```
gap> S3 := SymmetricGroup(3);
gap> T := CharacterTable(S3);
gap> Display(T);
CT3
```

```
2  1  1  .
3  1  .  1
```

```
1a 2a 3a
2P 1a 1a 3a
3P 1a 2a 1a
```

```
X.1    1 -1  1
X.2    2  . -1
X.3    1  1  1
```

Tal como hicimos antes, podemos extraer otra información de la tabla de caracteres calculada:

```
gap> SizesConjugacyClasses(T);
[ 1, 3, 2 ]
gap> SizesCentralizers(T);
[ 6, 2, 3 ]
gap> SizesConjugacyClasses(T);
[ 1, 3, 2 ]
gap> OrdersClassRepresentatives(T);
[ 1, 2, 3 ]
```

Ejemplo 8.4. Vamos a calcular la tabla de caracteres de \mathbb{S}_4 . Sabemos que \mathbb{S}_4 tiene orden 24 y cinco clases de conjugación

representante	id	(12)	(12)(34)	(123)	(1234)
tamaño	1	6	3	8	6

Como el conmutador $[\mathbb{S}_4, \mathbb{S}_4] \simeq \mathbb{A}_4$ entonces $\mathbb{S}_4/[\mathbb{S}_4, \mathbb{S}_4]$ tiene dos elementos y luego \mathbb{S}_4 tiene solamente dos representaciones de grado uno: una es el signo y la otra es la representación trivial. Tenemos entonces dos filas de la tabla de caracteres:

	id	(12)	(12)(34)	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1

Sabemos que existen $n_3, n_4, n_5 \in \{2, 3, 4\}$ tales que $24 = 1 + 1 + n_3^2 + n_4^2 + n_5^2$. Es fácil ver que $(n_3, n_4, n_5) = (2, 3, 3)$ es la única solución con $n_3 \leq n_4 \leq n_5$.

Encontraremos otra representación al usar la acción de \mathbb{S}_4 en el espacio vectorial

$$V = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 : x_1 + x_2 + x_3 + x_4 = 0\},$$

es decir: $g \cdot (x_1, x_2, x_3, x_4) = (x_{g^{-1}(1)}, x_{g^{-1}(2)}, x_{g^{-1}(3)}, x_{g^{-1}(4)})$. Sean

$$v_1 = (1, 0, 0, -1), \quad v_2 = (0, 1, 0, -1), \quad v_3 = (0, 0, 1, -1).$$

Entonces $\{v_1, v_2, v_3\}$ es base de V y

$$\begin{aligned} (12) \cdot v_1 &= v_2, & (12) \cdot v_2 &= v_1, & (12) \cdot v_3 &= v_3, \\ (1432) \cdot v_1 &= -v_3, & (1432) \cdot v_2 &= v_1 - v_3, & (1432) \cdot v_3 &= v_2 - v_3. \end{aligned}$$

Como $\mathbb{S}_4 = \langle (12), (1432) \rangle$ esto es suficiente para conocer la acción de cualquier $g \in \mathbb{S}_4$ en cualquier $v \in V$. Esta acción nos da una representación ρ de \mathbb{S}_4 en V :

$$\rho_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_{(1432)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix}.$$

Calculemos el carácter χ de ρ . Tenemos hasta ahora que $\chi(\text{id}) = 3$, $\chi((12)) = 1$, $\chi((1234)) = -1$. Para calcular el valor de χ es los 3-ciclos hacemos por ejemplo

$$\chi((234)) = \chi((12)(1234)) = \text{traza}(\rho_{(12)}\rho_{(1234)}) = \text{traza} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & -1 & -1 \end{pmatrix} = 0.$$

Similarmemente, para calcular el valor de χ en el producto de dos trasposiciones alcanza con observar que

$$\chi((13)(24)) = \chi((1234)(1234)) = \text{traza}(\rho_{(1234)}^2) = \text{traza} \begin{pmatrix} 0 & 0 & 1 \\ 1 & -1 & -1 \\ -1 & 2 & 0 \end{pmatrix} = -1.$$

Veamos que χ es un carácter irreducible:

$$\langle \chi, \chi \rangle = \frac{1}{24}(3^2 + 6 + 0 + 6 + 3) = 1.$$

Con lo que tenemos es fácil construir el caracter de otra representación irreducible pues $\text{signo} \otimes \chi$ es irreducible:

$$\langle \text{signo} \otimes \chi, \text{signo} \otimes \chi \rangle = \frac{1}{24}(3^2 + (-1)^2 6 + (-1)^2 3 + 6) = 1.$$

Tenemos así cuatro de los cinco caracteres irreducibles de G . Nos falta uno, digamos χ_5 . Para calcular χ_5 usamos el carácter de la representación regular L :

$$\begin{aligned} 0 &= \chi_L((12)) = 1 + (-1) + 3 + 3(-1) + 2\chi_5((12)), \\ 0 &= \chi_L((12)(34)) = 1 + 1 + 3(-1) + 3(-1) + 2\chi_5((12)(34)), \\ 0 &= \chi_L((123)) = 1 + 1 + 0 + 0 + 2\chi_5((123)), \\ 0 &= \chi_L((1234)) = 1 + (-1) + 3(-1) + 3 + 2\chi_5((1234)) = 0, \end{aligned}$$

de donde obtenemos los valores de χ_5 . Nos queda así la siguiente tabla:

	id	(12)	(12)(34)	(123)	(1234)
χ_1	1	1	1	1	1
signo	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\text{signo} \otimes \chi$	3	-1	-1	0	1
χ_5	2	0	2	-1	0

Dejamos como ejercicio calcular computacionalmente la tabla de caracteres de S_4 y compararla con el resultado obtenido en el ejemplo anterior.

Ejemplo 8.5. Calculemos ahora la tabla de caracteres de A_4 . Este grupo tiene orden 12 y cuatro clases de conjugación:

representante	id	(123)	(132)	(123)
tamaño	1	4	4	3

Como $[\mathbb{A}_4, \mathbb{A}_4] = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$, $\mathbb{A}_4/[\mathbb{A}_4, \mathbb{A}_4]$ tiene tres elementos. Luego \mathbb{A}_4 tiene tres caracteres irreducibles de grado uno y uno de grado tres. Sea $\omega = \exp(2\pi i/3)$ una raíz cúbica primitiva de la unidad. Si χ es un carácter no trivial de grado uno, $\chi((123)) = \omega^j$ para algún $j \in \{1, 2\}$ y $\chi((132)) = \omega^{2j}$. Como $(132)(134) = (12)(34)$ y además las permutaciones (134) y (123) son conjugadas, entonces

$$\chi_i((12)(34)) = \chi_i((132)(134)) = \chi_i((132))\chi_i((134)) = \omega^3 = 1$$

para todo $i \in \{1, 2\}$.

Para calcular χ_4 usamos el truco de la representación regular L ,

$$\begin{aligned} 0 &= \chi_L((12)(34)) = 1 + 1 + 1 + 3\chi_4((12)(34)), \\ 0 &= \chi_L((123)) = 1 + \omega + \omega^2 + 3\chi_4((123)), \\ 0 &= \chi_L((132)) = 1 + \omega + \omega^2 + 3\chi_4((132)), \end{aligned}$$

de donde obtenemos que $\chi_4((123)) = \chi_4((132)) = 0$ y $\chi_4((12)(34)) = -1$. Logramos así calcular la tabla de caracteres del grupo \mathbb{A}_4 :

	id	(123)	(132)	(12)(34)
χ_1	1	1	1	1
χ_2	1	ω	ω^2	1
χ_3	1	ω^2	ω	1
χ_4	3	0	0	-1

Si bien ya sabemos cómo calcular computacionalmente una tabla de caracteres, el caso del grupo \mathbb{A}_4 involucra raíces cúbicas de la unidad. Por eso conviene ver qué obtendremos al utilizar la computadora:

```
gap> A4 := AlternatingGroup(4);;
gap> T := CharacterTable(A4);;
gap> Display(T);
CT5
```

```
      2  2  2  .  .
      3  1  .  1  1
```

```
      1a 2a 3a 3b
2P 1a 1a 3b 3a
3P 1a 2a 1a 1a
```

```
X.1      1  1  1  1
X.2      1  1  A /A
X.3      1  1 /A  A
X.4      3 -1  .  .
```

```
A = E(3)^2
    = (-1-Sqrt(-3))/2 = -1-b3
```

Como imaginamos, el símbolo $E(3)$ denota una raíz cubica primitiva de la unidad ω . Para ahorrar espacio se utiliza la variable A para denotar al complejo ω^2 (que vemos escrito como el símbolo $E(3)^2$) y el símbolo $/A$ para denotar al complejo ω , el inverso multiplicativo de ω^2 .

Ejemplo 8.6. Vamos a calcular la tabla de caracteres de los grupos no abelianos de orden 8. (Salvo isomorfismo hay dos grupos no abelianos de ocho elementos, el grupo de cuaterniones y el diedral, pero no vamos a utilizar esta información.) Sea G un grupo no abeliano tal que $|G| = 8$. Como $Z(G) \neq 1$ y $G/Z(G)$ no es cíclico (pues G no es abeliano), $|Z(G)| = 2$. Como además $G/Z(G)$ es abeliano (porque $|G/Z(G)| = 4$), tenemos que $1 \neq [G, G] \subseteq Z(G)$ y luego $[G, G] = Z(G)$. Como $|G/[G, G]| = 4$, G admite exactamente cuatro representaciones de grado uno. Como además $8 = 1 + 1 + 1 + 1 + n_5^2 + \dots + n_r^2$, se concluye que $r = 5$ y $n_5 = 2$. Sabemos entonces que G tiene cinco clases de conjugación, digamos con representantes $1, x, a, b, c$, donde $[G, G] = Z(G) = \langle x \rangle$. La ecuación de clases nos dice que las clases de conjugación de a, b y c tienen dos elementos.

Sabemos que $G/[G, G] \simeq C_2 \times C_2$. Por la proposición 5.20, toda representación de grado uno de G es de la forma $\chi_j \circ \pi$, donde χ_j es una representación de grado uno

de $C_2 \times C_2$ y $\pi: G \rightarrow G/[G, G]$ es el morfismo canónico. Esto nos permite calcular gran parte de los valores de los caracteres de grado uno:

	1	x	a	b	c
χ_1	1	1	1	1	1
χ_2	1	?	-1	1	-1
χ_3	1	?	1	-1	-1
χ_4	1	?	-1	-1	1

Como $0 = \langle \chi_1, \chi_2 \rangle = \frac{1}{8}(1 + x + 2 + 2(-1) + 2(-1))$, se concluye que $\chi_2(x) = 1$. De la misma forma probamos que $\chi_j(x) = 1$ para todo $j \in \{3, 4\}$.

Nos falta calcular el valor del caracter de grado dos. Para eso usamos la representación regular L . Al resolver el sistema

$$\begin{aligned} 0 &= \chi_L(x) = 1 + 1 + 1 + 1 + 2\chi_5(x), \\ 0 &= \chi_L(a) = 1 + 1 + -1 - 1 + 2\chi_5(a), \\ 0 &= \chi_L(b) = 1 - 1 + 1 - 1 + 2\chi_5(b), \\ 0 &= \chi_L(c) = 1 - 1 - 1 + 1 + 2\chi_5(c), \end{aligned}$$

obtenemos $\chi_5(x) = -2$ y $\chi_5(a) = \chi_5(b) = \chi_5(c) = 0$. Luego la tabla de caracteres de G es

	1	x	a	b	c
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	-2	0	0	0

Para terminar con los ejemplos, primero listamos la tabla de caracteres del grupo de cuaterniones:

```
gap> Q8 := QuaternionGroup(8);;
gap> Display(CharacterTable(Q8));
CT6
```

```

      2   3   2   2   3   2
      1a 4a 4b 2a 4c
2P 1a 2a 2a 1a 2a
3P 1a 4a 4b 2a 4c

X.1      1   1   1   1   1
X.2      1  -1  -1   1   1
X.3      1  -1   1   1  -1
X.4      1   1  -1   1  -1
X.5      2   .   .  -2   .
```

Ahora listamos la tabla de caracteres del grupo diedral de ocho elementos. Es importante observar que la notación utilizada por **GAP** no coincide con nuestra notación, ya que para nosotros \mathbb{D}_n es el diedral de $2n$ elementos.

```
gap> D4 := DihedralGroup(8);;
gap> Display(CharacterTable(D8));
CT7
```

	2	3	2	2	3	2
	1a	2a	4a	2b	2c	
X.1	1	1	1	1	1	
X.2	1	-1	1	1	-1	
X.3	1	1	-1	1	-1	
X.4	1	-1	-1	1	1	
X.5	2	.	.	-2	.	

Capítulo 9

Conmutadores

Sea G un grupo finito y sean C_1, \dots, C_s sus clases de conjugación. Vimos en el teorema 7.8 que

$$\omega_{\chi}(C_i) = \frac{|C_i|\chi(C_i)}{\chi(1)}$$

es un número algebraico para todo $\chi \in \text{Irr}(G)$ y todo $i \in \{1, \dots, s\}$. Vimos además en la fórmula (7.1) que

$$\left(\frac{|C_i|}{\chi(1)} \chi(C_i) \right) \left(\frac{|C_j|}{\chi(1)} \chi(C_j) \right) = \sum_{k=1}^s a_{ijk} \left(\frac{|C_k|}{\chi(1)} \chi(C_k) \right),$$

es decir

$$\omega_{\chi}(C_i) \omega_{\chi}(C_j) = \sum_{k=1}^s a_{ijk} \omega_{\chi}(C_k),$$

donde a_{ijk} es la cantidad de soluciones de la ecuación $xy = z$ con $x \in C_i$, $y \in C_j$ y $z \in C_k$.

Teorema 9.1 (Burnside). *Si G es un grupo finito y C_1, \dots, C_s son sus clases de conjugación, entonces*

$$a_{ijk} = \frac{|C_i||C_j|}{|G|} \sum_{\chi \in \text{Irr}(G)} \frac{\chi(C_i)\chi(C_j)\overline{\chi(C_k)}}{\chi(1)}.$$

Demostración. Sabemos que

$$\left(\frac{|C_i|}{\chi(1)} \chi(C_i) \right) \left(\frac{|C_j|}{\chi(1)} \chi(C_j) \right) = \sum_{k=1}^s a_{ijk} \left(\frac{|C_k|}{\chi(1)} \chi(C_k) \right),$$

que puede reescribirse como

$$\frac{|C_i||C_j|\chi(C_i)\chi(C_j)}{\chi(1)} = \sum_{k=1}^s a_{ijk}|C_k|\chi(C_k).$$

Al multiplicar esta igualdad por $\overline{\chi(C_l)}$ y luego sumar sobre todos los $\chi \in \text{Irr}(G)$ tenemos

$$\begin{aligned} |C_i||C_j| \sum_{\chi \in \text{Irr}(G)} \frac{\overline{\chi(C_l)}}{\chi(1)} \chi(C_i) \chi(C_j) &= \sum_{\chi \in \text{Irr}(G)} \sum_{k=1}^s a_{ijk} |C_k| \chi(C_k) \overline{\chi(C_l)} \\ &= \sum_{k=1}^s a_{ijk} |C_k| \sum_{\chi \in \text{Irr}(G)} \chi(C_k) \overline{\chi(C_l)} \\ &= a_{ijl} |G|, \end{aligned}$$

ya que, gracias a la segunda relación de ortogonalidad de Schur, sabemos que

$$\sum_{\chi \in \text{Irr}(G)} \chi(C_k) \overline{\chi(C_l)} = \begin{cases} \frac{|G|}{|C_l|} & \text{si } k = l, \\ 0 & \text{en otro caso.} \end{cases} \quad \square$$

Veamos ahora algunos corolarios sobre conmutadores.

Teorema 9.2 (Burnside). *Sea G un grupo finito y sean $g, x \in G$. Entonces g y $[x, y]$ son conjugados para algún $y \in G$ si y sólo si*

$$\sum_{\chi \in \text{Irr}(G)} \frac{|\chi(x)|^2 \chi(g)}{\chi(1)} > 0.$$

Demostración. Sean C_1, \dots, C_s las clases de conjugación de G . Supongamos que $x \in C_i$ y que $g \in C_k$. Para $i \in \{1, \dots, s\}$ sea $C_i^{-1} = \{z^{-1} : z \in C_i\}$. El teorema de Burnside en el caso $C_j = C_i^{-1}$ implica entonces que

$$a_{ijk} = \frac{|C_i|^2}{|G|} \sum_{\chi \in \text{Irr}(G)} \frac{|\chi(C_i)|^2 \overline{\chi(C_k)}}{\chi(1)}.$$

Para cada $i \in \{1, \dots, s\}$ sea $g_i \in C_i$.

Demostremos primero la implicación \Leftarrow . Como en este caso $a_{ijk} > 0$, existen $u \in C_i$ y $v \in C_j$ tales que $g = uv$. Si x y u son conjugados, entonces x^{-1} y v también, digamos

$$u = zxz^{-1}, \quad v = z_1 x^{-1} z_1^{-1}$$

para ciertos $z, z_1 \in G$. Si $y = z^{-1} z_1$, entonces $y^{-1} z^{-1} = z_1^{-1}$ y luego g y $[x, y]$ son conjugados, pues

$$g = uv = (zxz^{-1})(z_1 x^{-1} z_1^{-1}) = zxyx^{-1} y^{-1} z^{-1}.$$

Demostremos ahora la implicación \Rightarrow . Si existe $y \in G$ tal que g y $[x, y]$ son conjugados, entonces $g = z(xy x^{-1} y^{-1}) z^{-1}$ para algún $z \in G$. Si $v = yxy^{-1}$, entonces $v^{-1} = yx^{-1} y^{-1}$ y luego g y $[x, y] = xyx^{-1} y^{-1} = xv^{-1}$ son conjugados. En particular, $g \in C_i C_i^{-1} = C_i C_j$ y luego $a_{ijk} > 0$. \square

Ejercicio 9.3. Si G es un grupo finito, $g, h \in G$ y $\chi \in \text{Irr}(G)$, entonces

$$\chi(g)\chi(h) = \frac{\chi(1)}{|G|} \sum_{z \in G} \chi(zgz^{-1}h).$$

Ejercicio 9.4. Si G es un grupo finito, $g, h \in G$ y $\chi \in \text{Irr}(G)$, entonces

$$\sum_{h \in G} \chi([g, h]) = \frac{|G|}{\chi(1)} |\chi(g)|^2.$$

Sea G un grupo finito. Para $g \in G$ sea

$$\tau(g) = |\{(x, y) \in G \times G : [x, y] = g\}|.$$

Vamos a demostrar una fórmula descubierta por Frobenius que nos permite calcular el valor de $\tau(g)$ a partir de la tabla de caracteres de G .

Teorema 9.5 (Frobenius). Si G es un grupo finito, entonces

$$\tau(g) = |G| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)}.$$

Demostración. Si χ es irreducible, entonces

$$\begin{aligned} 1 = \langle \chi, \chi \rangle &= \frac{1}{|G|} \sum_{z \in G} \chi(z) \overline{\chi(z)} \\ &= \frac{1}{|G|} \sum_C |C| \chi(C) \chi(C^{-1}), \end{aligned} \tag{9.1} \quad \boxed{\text{eq:chi}}$$

donde la última suma se hace sobre todas las clases de conjugación de G .

Sea $g \in G$ y sea C una clase de conjugación de G . Sabemos que la ecuación $xu^{-1} = g$, donde $x \in C$ y $u \in C^{-1}$ tiene

$$\frac{|C||C^{-1}|}{|G|} \sum_{\chi \in \text{Irr}(G)} \frac{\chi(C)\chi(C^{-1})\chi(g^{-1})}{\chi(1)}.$$

Si (x, u) es una solución, entonces existen $|C_G(x)|$ elementos y tales que $yxy^{-1} = u$. La ecuación $[x, y] = g$ tiene entonces

$$|C| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(C)\chi(C^{-1})\chi(g^{-1})}{\chi(1)}.$$

soluciones. Al sumar sobre todas las clases de conjugación y utilizar la fórmula (9.1) obtenemos

$$\begin{aligned} \sum_C |C| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(C) \chi(C^{-1}) \chi(g^{-1})}{\chi(1)} &= \sum_{\chi \in \text{Irr}(G)} \left(\sum_C |C| \chi(C) \chi(C^{-1}) \right) \frac{\chi(g^{-1})}{\chi(1)} \\ &= |G| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g^{-1})}{\chi(1)}. \end{aligned}$$

Como este número es un entero (pues cuenta la cantidad de soluciones de una cierta ecuación), es en particular un número real. En consecuencia, al conjugar obtenemos el resultado que queríamos demostrar. \square

El teorema de Frobenius obviamente implica el siguiente resultado demostrado en forma independiente por Burnside: Si G es un grupo finito y $g \in G$, entonces g es un conmutador si y sólo si

$$\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0.$$

En 1951 Ore conjeturó que todo elemento de un grupo simple finito no abeliano es un conmutador. El resultado fue demostrado en 2010:

Teorema 9.6 (Liebeck–O’Brien–Shalev–Tiep). *Todo elemento de un grupo simple finito no abeliano es un conmutador.*

La demostración puede consultarse en [24]. Ocupa unas 70 páginas y utiliza la clasificación de grupos simples finitos y teoría de caracteres, en particular los teoremas que presentamos en este capítulo. Para más información sobre el teorema de Liebeck–O’Brien–Shalev–Tiep referimos a [25]. Sin embargo, podemos dar una demostración computacional para algunos casos particulares:

Proposición 9.7. *La conjetura de Ore es verdadera para todo grupo simple esporádico.*

Demostración. Sea G un grupo simple finito. Sabemos que $g \in G$ es un conmutador si y sólo si $\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0$. La función que exponemos a continuación nos permite determinar si todo elemento de un grupo es un conmutador. La función recibe como parámetro una tabla de caracteres y devuelve **true** si todo elemento del grupo es un conmutador o **false** en caso contrario.

```
gap> Ore := function(char)
> local s, f, k;
> for k in [1..NrConjugacyClasses(char)] do
> s := 0;
> for f in Irr(char) do
> s := s+f[k]/Degree(f);
> od;
> if s<=0 then
> return false;
> fi;
> od;
```

```

> return true;
> end;
function( char ) ... end

```

Verificamos entonces la conjetura de Ore para los cinco grupos de Mathieu y para el monstruo M :

```

gap> Ore(CharacterTable("M11"));
true
gap> Ore(CharacterTable("M12"));
true
gap> Ore(CharacterTable("M22"));
true
gap> Ore(CharacterTable("M23"));
true
gap> Ore(CharacterTable("M24"));
true
gap> Ore(CharacterTable("M"));
true

```

Dejamos como ejercicio demostrar la conjetura de Ore para el resto de los grupos esporádicos: $HS, J_1, J_2, J_3, J_4, Co_1, Co_2, Co_3, McL, Ru, Ly, Suz, He, HN, Th, Fi_{22}, Fi_{23}, Fi'_{24}, B, M$ □

Para otras aplicaciones de la teoría de caracteres a los grupos simples finitos referiremos a [23].

Capítulo 10

El teorema de Cauchy-Frobenius-Burnside

El siguiente resultado se atribuye incorrectamente a Burnside. Se sabe que fue demostrado independientemente por Cauchy y por Frobenius, para más información puede consultarse en [27].

Teorema 10.1 (Cauchy–Frobenius–Burnside). *Supongamos que el grupo finito G actúa en un conjunto finito X . Si m es la cantidad de órbitas de la acción, entonces*

$$m = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|,$$

donde $\text{Fix}(g) = \{x \in X : g \cdot x = x\}$.

Demostración. Sea V el espacio vectorial con base en $\{x : x \in X\}$. Como G actúa en X , tenemos un morfismo $\rho : G \rightarrow \mathbf{GL}(V)$, $g \mapsto \rho_g$. Observemos que para cada $g \in G$ la matriz de ρ_g en la base $\{x : x \in X\}$ es

$$(\rho_g)_{ij} = \begin{cases} 1 & \text{si } g \cdot x_j = x_i, \\ 0 & \text{en otro caso.} \end{cases}$$

En particular,

$$(\rho_g)_{ii} = \begin{cases} 1 & \text{si } x_i \in \text{Fix}(g), \\ 0 & \text{en otro caso.} \end{cases}$$

Si χ es el caracter de ρ , entonces

$$\chi(g) = \text{traza}(\rho_g) = \sum_{i=1}^k (\rho_g)_{ii} = |\text{Fix}(g)|.$$

Vimos en el lema 6.11 que $\langle \chi, \chi_1 \rangle = \dim V^G$, donde χ_1 denota al caracter trivial.

Para demostrar el teorema tenemos necesitamos $\dim V^G = m$.

Sean x_1, \dots, x_m los representantes de las órbitas de la acción de G en X . Para cada $i \in \{1, \dots, m\}$ sea $v_i = \sum_{x \in G \cdot x_i} x$. Veamos que $\{v_1, \dots, v_m\}$ es una base de V .

Primero vemos que $\{v_1, \dots, v_m\} \subseteq V^G$, pues para cada $g \in G$, tenemos

$$g \cdot v_i = \sum_{x \in G \cdot x_i} g \cdot x = \sum_{y \in G \cdot y} y = v_i,$$

ya que si x recorre una órbita, también lo hace $g \cdot x$.

El conjunto $\{v_1, \dots, v_m\}$ es linealmente independiente, pues los v_1, \dots, v_m son ortogonales no nulos. De hecho,

$$\langle v_i, v_j \rangle = \begin{cases} |G \cdot x_i| & \text{si } i = j, \\ 0 & \text{en otro caso.} \end{cases}$$

Veamos que V está generado por el conjunto $\{v_1, \dots, v_m\}$. Si $v \in V^G$, escribimos $v = \sum_{x \in X} \lambda_x x$ para $\lambda_x \in \mathbb{C}$. Afirmamos que si existe $g \in G$ tal que $g \cdot y = z$, entonces $\lambda_y = \lambda_z$. En efecto, como $v \in V^G$, tenemos

$$\sum_{x \in X} \lambda_x x = v = g \cdot v = \sum_{x \in X} \lambda_x (g \cdot x),$$

de donde obtenemos $\lambda_z = \lambda_y$ al comparar el coeficiente de z en ambos miembros de la igualdad. Podemos escribir entonces

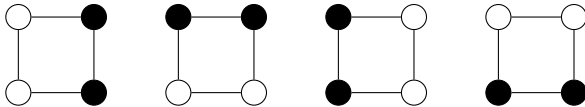
$$v = \sum_{x \in X} \lambda_x x = \sum_{i=1}^m \lambda_{x_i} \sum_{y \in G \cdot x_i} y = \sum_{i=1}^m (\lambda_{x_i} |G \cdot x_i|) v_i. \quad \square$$

En [31] encontramos una demostración alternativa muy sencilla. Hagamos el caso en que G actúa transitivamente en X :

$$\sum_{g \in G} |\text{Fix}(g)| = \sum_{g \in G} \sum_{\substack{x \in X \\ g \cdot x = x}} 1 = \sum_{x \in X} \sum_{\substack{g \in G \\ g \cdot x = x}} 1 = \sum_{x \in X} |G_x| = |G_x| |X| = |G|.$$

El teorema de Cauchy–Frobenius–Burnside tiene muchas aplicaciones.

Ejemplo 10.2. Vamos a calcular de cuántas formas pueden colorearse con dos colores –negro y blanco– los vértices de un cuadrado. Vamos a contar la cantidad de coloreos salvo simetrías. Eso significa, por ejemplo, que los coloreos

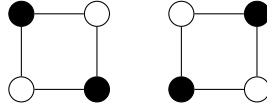

(10.1)

eq:orbita

serán considerados equivalentes. Sea $G = \langle g \rangle$ el grupo cíclico de orden cuatro y sea X el conjunto de coloreos del cuadrado.

Obviamente $|X| = 16$.

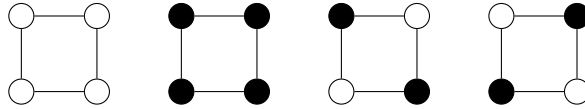
Hacemos actuar a G en X por rotaciones de 90° en sentido antihorario. Los coloreos que vimos en (10.1) están todos en una misma órbita. Otra de las órbitas del conjunto X está formada por



La fórmula de Cauchy–Frobenius–Burnside nos dice que la cantidad de órbitas en X es igual a

$$\frac{1}{|G|} \sum_{x \in G} |\text{Fix}(x)|.$$

Para cada $x \in G = \{1, g, g^2, g^3\}$ calculemos entonces $\text{Fix}(x)$. La identidad fija a los 16 puntos de X , g y g^3 fijan solamente dos puntos de X y g^2 fija cuatro puntos de X . Por ejemplo, los puntos de X fijados por g^2 son



Luego X es unión de

$$\frac{1}{|G|} \sum_{x \in G} |\text{Fix}(x)| = \frac{1}{4} (16 + 2 + 4 + 2) = 6$$

órbitas.

Ejercicio 10.3. Calcule la cantidad de formas (salvo simetrías) en las que pueden ubicarse ocho torres en un tablero de ajedrez sin que se ataquen mutuamente. Las simetrías de este problema están dadas por la acción del grupo diedral \mathbb{D}_4 de ocho elementos.

Si G es un grupo finito, se define $\text{cp}(G)$ como la probabilidad de que dos elementos de G elegidos al azar conmuten. Como aplicación de la fórmula de Cauchy–Frobenius–Burnside vamos a demostrar que $\text{cp}(G) = k/|G|$, donde k es la cantidad de clases de conjugación de G .

Teorema 10.4 (Erdős–Turan). Si G es un grupo finito no abeliano, entonces $\text{cp}(G) \leq 5/8$.

Demostración. Sea $C = \{(x, y) \in G \times G : xy = yx\}$. Veamos que la probabilidad que queremos calcular es

$$\text{cp}(G) = \frac{|C|}{|G|^2} = \frac{k}{|G|}.$$

En efecto, si hacemos actuar a G en G por conjugación. Gracias a la fórmula de Cauchy–Frobenius–Burnside,

$$k = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| = \frac{1}{|G|} \sum_{g \in G} |C_G(g)| = \frac{|C|}{|G|},$$

pues $\text{Fix}(g) = \{x \in G : gxg^{-1} = x\} = C_G(g)$ y además $\sum_{g \in G} |C_G(g)| = |G|$.

Vamos a demostrar ahora que $k/|G| \leq 5/8$ si G es no abeliano.

Sean y_1, \dots, y_m representantes de las clases de conjugación de G de tamaño ≥ 2 . Por la ecuación de clases,

$$|G| = |Z(G)| + \sum_{i=1}^m (G : C_G(y_i)) \geq |Z(G)| + 2m.$$

Luego $m \leq (1/2)(|G| - |Z(G)|)$ y entonces

$$k = |Z(G)| + m \leq |Z(G)| + \frac{1}{2}(|G| - |Z(G)|) = \frac{1}{2}(|Z(G)| + |G|).$$

Como G es no abeliano, el cociente $G/Z(G)$ no es cíclico y entonces, en particular, $(G : Z(G)) \geq 4$. En consecuencia,

$$k \leq \frac{1}{2}(|Z(G)| + |G|) \leq \frac{1}{2} \left(\frac{1}{4} + 1 \right) |G|,$$

es decir $k/|G| \leq 5/8$. □

Ejercicio 10.5. Demuestre que la probabilidad de que dos elementos elegidos al azar de Q_8 conmuten es exactamente $5/8$.

Ejercicio 10.6. Si G es un grupo no abeliano y p es el menor primo que divide al orden de G , entonces $\text{cp}(G) \leq (p^2 + p - 1)/p^3$. Vale además la igualdad si y sólo si $(G : Z(G)) = p^2$.

Ejercicio 10.7. Sea G un grupo finito y sea H un subgrupo de G .

- 1) $\text{cp}(G) \leq \text{cp}(H)$.
- 2) Si H es normal en G , entonces $\text{cp}(G) \leq \text{cp}(G/H) \text{cp}(H)$.

Los grados de las representaciones irreducibles nos dan una cota inferior:

Proposición 10.8. Si G es un grupo finito, entonces

$$\text{cp}(G) \geq \left(\frac{\sum_{\chi \in \text{Irr}(G)} \chi(1)}{|G|} \right)^2.$$

Demostración. Supongamos que G tiene k clases de conjugación. Al usar la desigualdad de Cauchy-Schwarz,

$$\left(\sum_{\chi \in \text{Irr}(G)} \chi(1) \right)^2 \leq \left(\sum_{\chi \in \text{Irr}(G)} \chi(1)^2 \right) \left(\sum_{\chi \in \text{Irr}(G)} 1 \right) = \left(\sum_{\chi \in \text{Irr}(G)} \chi(1)^2 \right) k = |G|k,$$

de donde se obtiene inmediatamente la desigualdad que queríamos demostrar. □

Teorema 10.9 (Dixon). Si G es un grupo finito simple, entonces $\text{cp}(G) \leq 1/12$.

El teorema anterior fue propuesto por Dixon como problema en el volumen 13 del *Canadian Math. Bulletin* de 1970, la solución apareció en 1973. Demostraremos el teorema de Dixon cuando estudiemos grupos transitivos.

Ejercicio 10.10. Verifique que $\text{cp}(\mathbb{A}_5) = 1/12$.

El grupo alternado \mathbb{A}_5 juega un papel especial:

Teorema 10.11 (Guralnick–Robinson). *Si G es un grupo finito no resoluble y tal que $\text{cp}(G) > 3/40$, entonces $G \simeq \mathbb{A}_5 \times T$ para algún grupo abeliano T y además $\text{cp}(G) = 1/12$.*

La demostración puede consultarse en [14].

Veamos otras direcciones hacia donde pueden generalizarse resultados sobre la probabilidad de que dos elementos elegidos al azar conmuten.

En una serie de trabajos monumentales [34, 35, 36, 37], Thompson demostró el siguiente resultado:

Teorema 10.12 (Thompson). *Si G es un grupo finito tal que todo par de elementos de G genera un grupo resoluble, entonces G es resoluble.*

Una demostración mucho más sencilla y que no depende de la clasificación de grupos simples finitos puede consultarse en [10]. El siguiente resultado de [15] depende de la clasificación de grupos simples, puede interpretarse como una versión probabilística del teorema de Thompson.

Teorema 10.13 (Guralnick–Wilson). *Sea G un grupo finito.*

- 1) *Si la probabilidad de que dos elementos de G elegidos al azar generen un grupo resoluble es $> 11/30$, entonces G es resoluble.*
- 2) *Si la probabilidad de que dos elementos de G elegidos al azar generen un grupo nilpotente es $> 1/2$, entonces G es nilpotente.*
- 3) *Si la probabilidad de que dos elementos de G elegidos al azar generen un grupo de orden impar es $> 11/30$, entonces G es de orden impar.*

La fórmula de Cauchy–Frobenius–Burnside es útil para determinar caracteres.

Supongamos que el grupo G actúa en el conjunto finito X . Podemos definir entonces una acción de G en el conjunto $X \times X$:

$$g \cdot (x, y) = (g \cdot x, g \cdot y).$$

Las órbitas de esta acción se llaman **orbitales** de G en X . Se define el **rango** de G en X como la cantidad de orbitales de G en X . Observemos que el conjunto de puntos fijos de la acción de $g \in G$ en $X \times X$ es $\text{Fix}(g) \times \text{Fix}(g)$ pues

$$\begin{aligned} g \cdot (x, y) = (x, y) &\iff (g \cdot x, g \cdot y) = (x, y) \\ &\iff g \cdot x = x, g \cdot y = y \iff (x, y) \in \text{Fix}(g) \times \text{Fix}(g). \end{aligned}$$

Por el teorema de Cauchy–Frobenius–Burnside, el rango de G en X es igual a

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|^2.$$

Diremos que G actúa **2-transitivamente** en X si dados $x, y \in X$ con $x \neq y$ y $x_1, y_1 \in X$ con $x_1 \neq y_1$ existe $g \in G$ tal que $g \cdot x = y$ y $g \cdot x_1 = y_1$.

Ejemplo 10.14. El grupo simétrico \mathbb{S}_n actúa 2-transitivamente en $\{1, 2, \dots, n\}$.

Ejemplo 10.15. Si G es 2-transitivo en X , entonces el rango de G en X es dos. En efecto, un orbital es

$$\Delta = \{(x, x) : x \in X\}.$$

Veamos que el complemento de Δ es el otro orbital. Si $x, y \in X$ y $x_1, y_1 \in X$ con $x \neq y$ y $x_1 \neq y_1$, existe $g \in G$ tal que $g \cdot x = y$ y $g \cdot x_1 = y_1$, es decir $g \cdot (x, x_1) = (y, y_1)$.

Proposición 10.16. Si G actúa 2-transitivamente en X con caracter $\chi(g) = |\text{Fix}(g)|$, entonces el caracter $\chi - \chi_1$ es irreducible.

Demostración. Como G actúa 2-transitivamente en X , el grupo G es transitivo en X . Como el caracter trivial χ_1 es irreducible, $\langle \chi_1, \chi_1 \rangle = 1$. Por el teorema de Cauchy-Frobenius-Burnside, el rango de G en X es

$$2 = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|^2 = \langle \chi, \chi \rangle.$$

Luego

$$\langle \chi - \chi_1, \chi - \chi_1 \rangle = \langle \chi, \chi \rangle - 1 - 1 + 1 = 1. \quad \square$$

Ejemplo 10.17. El grupo simétrico \mathbb{S}_n actúa 2-transitivamente en $\{1, \dots, n\}$. También lo hace el grupo alternado \mathbb{A}_n para $n \geq 4$. Luego estos grupos poseen un caracter irreducible χ dado por $\chi(g) = |\text{Fix}(g)| - 1$.

Ejemplo 10.18. Sean p un primo y $q = p^m$. Sea V el espacio vectorial de dimensión m sobre el cuerpo finito de q elementos. El grupo $G = \mathbf{GL}_2(q)$ actúa 2-transitivamente en el conjunto X de subespacios de V de dimensión uno. En efecto, si $\langle v \rangle \neq \langle v_1 \rangle$ y $\langle w \rangle \neq \langle w_1 \rangle$, entonces $\{v, v_1\}$ y $\{w, w_1\}$ son bases de V . La matriz g que corresponde a la transformación lineal $v \mapsto w$, $v_1 \mapsto w_1$, es inversible y luego $g \in \mathbf{GL}_2(q)$. La proposición anterior nos da el caracter $\chi(g) = |\text{Fix}(g)| - 1$.

Nos basaremos en [31] y veremos otras aplicaciones del teorema de Cauchy-Frobenius-Burnside.

Teorema 10.19 (Jordan). Sea G un grupo finito no trivial. Si G actúa transitivamente en un conjunto finito X y $|X| > 1$, entonces existe $g \in G$ sin puntos fijos.

Demostración. El teorema de Cauchy-Frobenius-Burnside implica que

$$1 = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| = \frac{1}{|G|} \left(|X| + \sum_{g \neq 1} |\text{Fix}(g)| \right).$$

Si todo $g \in G \setminus \{1\}$ contiene al menos un punto fijo, entonces

$$1 = \frac{1}{|G|} \left(|X| + \sum_{g \neq 1} |\text{Fix}(g)| \right) \geq \frac{1}{|G|} (|X| + |G| - 1) = 1 + \frac{|X| - 1}{|G|}$$

y luego $|X| \leq 1$, una contradicción. \square

Corolario 10.20. *Sea G un grupo finito y H un subgrupo propio de G . Entonces $G \neq \cup_{g \in G} gHg^{-1}$.*

Demostración. El grupo G actúa transitivamente en $X = G/H$ por multiplicación a izquierda. El estabilizador de xH es

$$G_{xH} = \{g \in G : gxH = xH\} = xHx^{-1}.$$

Como $H \neq G$, entonces $|X| = |G/H| > 1$. El teorema de Jordan implica entonces que existe $g \in G$ sin puntos fijos, es decir que existe $g \in G$ tal que $g \notin \cup_{x \in G} xHx^{-1}$. \square

Sea G un grupo finito. Diremos que dos clases de conjugación C y D **conmutan** si existen $c \in C$ y $d \in D$ tales que $[c, d] = 1$. Observemos que C y D conmutan si y sólo si para todo $c \in C$ existe $d \in D$ tal que $[c, d] = 1$.

Corolario 10.21 (Wildon). *Sea G un grupo finito y sea C una clase de conjugación de G . Entonces $|C| = 1$ si y sólo si C conmuta con cualquier clase de conjugación de G .*

Demostración. Si $C = \{c\}$, entonces $c \in Z(G)$ y luego C conmuta con cualquier clase de conjugación de G . Recíprocamente, supongamos que C conmuta con cualquier clase de conjugación de G . Si $c \in C$ y $H = C_G(c)$, entonces $H \cap D \neq \emptyset$ para toda clase de conjugación D . Afirmamos que entonces $G = \cup_{g \in G} gHg^{-1}$. En efecto, sea $x \in G$. Entonces $x \in D$ para alguna clase de conjugación D . Sea $h \in H \cap D$. Existe $y \in G$ tal que $h = yxy^{-1}$, es decir $x = y^{-1}hy \in \cup_{g \in G} gHg^{-1}$. Por el teorema de Jordan, $H = G$. Luego c es central, es decir $C = \{c\}$. \square

La clasificación de grupos simples finitos permite demostrar un teorema similar al teorema de Jordan [8].

Teorema 10.22 (Fein–Kantor–Schacher). *Sea G un grupo finito no trivial. Si G actúa transitivamente en un conjunto finito X y $|X| > 1$, entonces existe un primo p y un elemento $g \in G$ sin puntos fijos cuyo orden es una potencia de p .*

No veremos la demostración en este curso.

Supongamos que G es un grupo finito que actúa fiel y transitivamente en un conjunto X , digamos $G \leq \mathbb{S}_n$, donde $X = \{1, 2, \dots, n\}$. Sea G_0 el conjunto de $g \in G$ sin puntos fijos, es decir $g(x) \neq x$ para todo $x \in X$. Tales permutaciones se conocen como **desarreglos**. Sea $c_0 = |G_0|/|G|$.

Teorema 10.23 (Cameron–Cohen). *Si G es un subgrupo de \mathbb{S}_n que actúa transitivamente en $\{1, \dots, n\}$, entonces $c_0 \geq \frac{1}{n}$.*

Demostración. Sea $X = \{1, \dots, n\}$. El rango de G es, por definición, la cantidad de orbitales de G en X . Luego el rango de G es ≥ 2 , pues $X \times X$ puede descomponerse como $X \times X = \Delta \cup ((X \times X) \setminus \Delta)$. Sean $\chi(g) = |\text{Fix}(g)|$ y $G_0 = \{g \in G : \chi(g) = 0\}$. Si $g \notin G_0$, entonces $1 \leq \chi(g) \leq n$. Como $(\chi(g) - 1)(\chi(g) - n) \leq 0$, se tiene que

$$\frac{1}{|G|} \sum_{g \in G \setminus G_0} (\chi(g) - 1)(\chi(g) - n) \leq 0.$$

Por un lado,

$$\begin{aligned} \frac{1}{|G|} \sum_{g \in G} (\chi(g) - 1)(\chi(g) - n) \\ &= \frac{1}{|G|} \left\{ \sum_{g \in G_0} + \sum_{g \in G \setminus G_0} \right\} (\chi(g) - 1)(\chi(g) - n) \\ &\leq n \frac{|G_0|}{|G|} = nc_0. \end{aligned}$$

Por otro lado, como el rango de G es ≥ 2 , tenemos

$$2 - \frac{n+1}{|G|} \sum_{g \in G} \chi(g) + n \leq \frac{1}{|G|} \sum_{g \in G} (\chi(g) - 1)(\chi(g) - n) \leq nc_0. \quad (10.2) \quad \boxed{\text{eq:CameronCohen}}$$

Por hipótesis, G es transitivo en X . El teorema de Cauchy–Frobenius–Burnside implica entonces que $\sum_{g \in G} \chi(g) = |G|$. Se sigue que $2 - (n+1) + n \leq nc_0$ y luego $1/n \leq c_0$. \square

El teorema de Cameron–Cohen tiene una segunda parte: Si n no es potencia de un primo, entonces $c_0 > 1/n$. Daremos la demostración en el capítulo 13, donde estudiaremos grupos de Frobenius.

La cota del teorema de Cameron–Cohen puede mejorarse si se utiliza la clasificación de grupos simples finitos [12].

Teorema 10.24 (Guralnick–Wan). *Sea G un grupo finito transitivo de grado $n \geq 2$. Si n no es potencia de un número primo y además $G \neq \mathbb{S}_n$ para $n \in \{2, 4, 5\}$, entonces $c_0 \geq 2/n$.*

La demostración utiliza la clasificación de grupos finitos 2-transitivos, que depende de la clasificación de grupos simples finitos.

Capítulo 11

El teorema de Brauer–Fowler

En este capítulo vamos a demostrar el teorema de Brauer–Fowler.

El resultado es fundamental en la clasificación de grupos simples finitos. Daremos dos demostraciones, una basada en teoría de caracteres y una demostración alternativa completamente elemental.

Comenzaremos con la demostración que usa teoría de caracteres.

Sea $\rho: G \rightarrow \mathbf{GL}(V)$ una representación con caracter χ . Vimos que el $\mathbb{C}[G]$ -módulo $V \otimes V$ tiene caracter χ^2 . Sea v_1, \dots, v_n una base de V y sea

$$T: V \rightarrow V, \quad v_i \otimes v_j \mapsto v_j \otimes v_i.$$

Dejamos como ejercicio verificar que $T(v \otimes w) = w \otimes v$ para todo $v, w \in V$. Luego la transformación lineal T no depende de la base elegida. Observemos que además T es morfismo de $\mathbb{C}[G]$ -módulos, pues

$$T(g \cdot (v \otimes w)) = T((g \cdot v) \otimes (g \cdot w)) = (g \cdot w) \otimes (g \cdot v) = g \cdot T(w \otimes v)$$

para todo $g \in G$ y $v, w \in V$. En particular, la **parte simétrica**

$$S(V \otimes V) = \{x \in V \otimes V : T(x) = x\}$$

la **parte antisimétrica**

$$A(V \otimes V) = \{x \in V \otimes V : T(x) = -x\}$$

de $V \otimes V$ son ambas $\mathbb{C}[G]$ -submódulos de $V \otimes V$. Estos nombres están motivados por la siguiente observación

$$V \otimes V = S(V \otimes V) \oplus A(V \otimes V).$$

En efecto, $S(V \otimes V) \cap A(V \otimes V) = \{0\}$ pues si $x \in S(V \otimes V) \cap A(V \otimes V)$, entonces $x = T(x)$ y $x = -T(x)$ y luego $x = 0$. Además $V \otimes V = S(V \otimes V) + A(V \otimes V)$ pues todo $x \in V \otimes V$ puede escribirse como

$$x = \frac{1}{2}(x + T(x)) + \frac{1}{2}(x - T(x))$$

con $\frac{1}{2}(x + T(x)) \in S(V \otimes V)$ y $\frac{1}{2}(x - T(x)) \in A(V \otimes V)$.

Veamos que el conjunto $\{v_i \otimes v_j + v_j \otimes v_i : 1 \leq i, j \leq n\}$ es base de $S(V \otimes V)$ y que el conjunto

$$\{v_i \otimes v_j - v_j \otimes v_i : 1 \leq i < j \leq n\}$$

es base de $A(V \otimes V)$. Como ambos conjuntos son linealmente independientes, entonces $\dim S(V \otimes V) \geq n(n+1)/2$ y también $\dim A(V \otimes V) \geq n(n-1)/2$. Como además

$$n^2 = \dim(V \otimes V) = \dim S(V \otimes V) + \dim A(V \otimes V),$$

se concluye que $\dim S(V \otimes V) = n(n+1)/2$ y que $\dim A(V \otimes V) = n(n-1)/2$.

Proposición 11.1. *Sea G un grupo finito y sea V un $\mathbb{C}[G]$ -módulo de dimensión finita con caracter χ . Si el módulo $S(V \otimes V)$ tiene caracter χ_S y el módulo $A(V \otimes V)$ tiene caracter χ_A , entonces*

$$\begin{aligned}\chi_S(g) &= \frac{1}{2}(\chi^2(g) + \chi(g^2)), \\ \chi_A(g) &= \frac{1}{2}(\chi^2(g) - \chi(g^2)).\end{aligned}$$

Demostración. Sea $g \in G$. Sea $\rho : G \rightarrow \mathbf{GL}(V)$ la representación asociada al módulo V , es decir $\rho(g)(v) = \rho_g(v) = g \cdot v$. Sabemos que ρ_g es diagonalizable. Sea $\{e_1, \dots, e_n\}$ una base de autovectores de ρ_g , digamos $g \cdot e_i = \lambda_i e_i$ con $\lambda_i \in \mathbb{C}$ para $i \in \{1, \dots, n\}$. En particular, $\chi(g) = \sum_{i=1}^n \lambda_i$.

Como $\{e_i \otimes e_j - e_j \otimes e_i : 1 \leq i < j \leq n\}$ es base de $A(V \otimes V)$ y además

$$g \cdot (e_i \otimes e_j - e_j \otimes e_i) = \lambda_i \lambda_j (e_i \otimes e_j - e_j \otimes e_i),$$

tenemos $\chi_A(g) = \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j$. Por otro lado, como $g^2 \cdot e_i = \lambda_i^2 e_i$ para todo i , $\chi(g^2) = \sum_{i=1}^n \lambda_i^2$. Luego

$$\chi^2(g) = \chi(g)^2 = \sum_{i=1}^n \sum_{j=1}^n \lambda_i \lambda_j = 2 \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j + \sum_{i=1}^n \lambda_i^2 = 2\chi_A(g) + \chi(g^2).$$

Como además $V \otimes V = S(V \otimes V) \oplus A(V \otimes V)$, se tiene $\chi^2(g) = \chi_S(g) + \chi_A(g)$, es decir $\chi_S(g) = \frac{1}{2}(\chi^2(g) + \chi(g^2))$. \square

Una **involución** en un grupo es un elemento $x \neq 1$ tal que $x^2 = 1$. Es posible la cantidad de involuciones con la tabla de caracteres:

Proposición 11.2. *Si G es un grupo finito con t involuciones, entonces*

$$1 + t = \sum_{\chi \in \text{Irr}(G)} \langle \chi_S - \chi_A, \chi_1 \rangle \chi(1).$$

Demostración. Supongamos que $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$, donde χ_1 es el carácter trivial de G . Para $x \in G$ sea

$$\theta(x) = |\{y \in G : y^2 = x\}|.$$

Como θ es una función de clases θ puede escribirse como combinación lineal de los χ_j , digamos

$$\theta = \sum_{\chi \in \text{Irr}(G)} \langle \theta, \chi \rangle \chi.$$

Calculamos

$$\begin{aligned} \langle \chi_S - \chi_A, \chi_1 \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g^2) \\ &= \frac{1}{|G|} \sum_{x \in G} \sum_{\substack{g \in G \\ g^2 = x}} \chi(g^2) = \frac{1}{|G|} \sum_{x \in G} \theta(x) \chi(x) = \langle \theta, \chi \rangle. \end{aligned}$$

Luego $\theta(x) = \sum_{\chi \in \text{Irr}(G)} \langle \chi_S - \chi_A, \chi_1 \rangle \chi$ y el resultado se obtiene al evaluar esta expresión en $x = 1$. \square

Necesitamos un lema:

Lema 11.3. *Sea G un grupo finito con k clases de conjugación. Si t es la cantidad de involuciones de G , entonces $t^2 \leq (k-1)(|G|-1)$.*

Demostración. Supongamos que $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$, donde χ_1 es el carácter trivial de G . Si $\chi \in \text{Irr}(G)$, entonces

$$\langle \chi^2, \chi_1 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \chi(g) = \langle \chi, \bar{\chi} \rangle = \begin{cases} 1 & \text{si } \chi = \bar{\chi}, \\ 0 & \text{en otro caso.} \end{cases}$$

Como $\chi^2 = \chi_S + \chi_A$, si $\langle \chi^2, \chi_1 \rangle = 1$, entonces el carácter trivial o bien es χ_1 es parte de χ_S o bien es parte de χ_A , pero no de ambos. Esto implica que

$$\langle \chi_S - \chi_A, \chi_1 \rangle \in \{-1, 1, 0\}.$$

Vamos a demostrar ahora que $t \leq \sum_{i=2}^k \chi_i(1)$. En efecto, como $|\langle \chi_S - \chi_A, \chi_1 \rangle| \leq 1$, entonces

$$\begin{aligned} 1 + t = \theta(1) &= \left| \sum_{\chi \in \text{Irr}(G)} \langle \chi_S - \chi_A, \chi_1 \rangle \chi(1) \right| \\ &\leq \sum_{\chi \in \text{Irr}(G)} |\langle \chi_S - \chi_A, \chi_1 \rangle| \chi(1) \leq \sum_{\chi \in \text{Irr}(G)} \chi(1), \end{aligned}$$

de donde se obtiene inmediatamente que $t \leq \sum_{i=2}^k \chi_i(1)$. Si utilizamos ahora la desigualdad de Cauchy–Schwartz,

$$t^2 \leq \left(\sum_{i=2}^k \chi_i(1) \right)^2 \leq (k-1) \sum_{i=2}^k \chi_i(1)^2 = (k-1)(|G|-1). \quad \square$$

Ahora sí estamos en condiciones de dar la primera demostración del teorema de Brauer–Fowler.

Teorema 11.4 (Brauer–Fowler). *Sea G un grupo finito y simple y sea x una involución. Si $|C_G(x)| = n$, entonces $|G| \leq (n^2)!$*

Demostración. Supongamos primero que existe un subgrupo propio H de G tal que $(G:H) \leq n^2$. En ese caso, hacemos actuar a G en G/H por multiplicación a izquierda y tenemos un morfismo de grupos $\rho: G \rightarrow \mathbb{S}_{n^2}$. Como G es un grupo simple, $\ker \rho = \{1\}$ o bien $\ker \rho = G$. Si $\ker \rho = G$, entonces $\rho(g)(yH) = yH$ para todo $g \in G$ e $y \in G$, lo que implica que $g \in H$, una contradicción. Luego ρ es inyectiva y entonces G es isomorfo a un subgrupo de \mathbb{S}_{n^2} . En particular, $|G|$ divide a $(n^2)!$

Sea $m = (|G|-1)/t$. Como $|C_G(x)| = n$, el grupo G tiene al menos $|G|/n$ involuciones (pues la clase de conjugación de x tiene tamaño $|G|/n$ y todos sus elementos son involuciones), es decir $t \geq |G|/n$. Luego $m = (|G|-1)/t < n$. Basta demostrar entonces que G contiene un subgrupo de índice $\leq m^2$.

Sean C_1, \dots, C_k las clases de conjugación de G , donde $C_1 = \{1\}$. Como G es simple, $|C_i| > 1$ para todo $i \in \{2, \dots, k\}$. Notar que

$$|G|-1 \leq \frac{(k-1)(|G|-1)^2}{t^2} \iff t^2 \leq (k-1)(|G|-1),$$

que vale gracias al lema anterior. Si $|C_i| > m$ para todo $i \in \{2, \dots, k\}$, entonces, como

$$|G|-1 \leq \frac{(k-1)(|G|-1)^2}{t^2} = (k-1)m^2,$$

tendríamos

$$|G|-1 = \sum_{i=2}^k |C_i| > (k-1)m^2,$$

una contradicción. Luego existe una clase de conjugación C de G tal que $|C| \leq m^2$. Si $g \in C$, entonces $C_G(g)$ es un subgrupo de G de índice $|C| \leq m^2$. \square

La cota del teorema de Brauer–Fowler no es importante, ya que para considerar una forma posible de atacar la clasificación de grupos simples solamente es necesario saber que existen finitos grupos simples finitos con un cierto centralizador de involuciones.

Corolario 11.5. *Sea $n \in \mathbb{N}$. Existe (a lo sumo) una cantidad finita de grupos simples finitos con una involución con centralizador de orden n .*

Veamos un ejemplo sencillo que da una idea de cómo es que pueden clasificarse grupos simples una vez que se tiene fija la estructura del centralizador de una involución.

Ejercicio 11.6. Si G es un grupo simple finito y x es una involución con centralizador de orden dos, entonces $G \simeq \mathbb{Z}/2$.

Una demostración elemental del teorema de Brauer–Fowler

Tal como hicimos en el primer párrafo de la demostración del teorema de Brauer–Fowler, alcanza con encontrar un subgrupo de índice $\leq 2n^2$. Sea X la clase de conjugación de x . Para $g \in G$ definimos

$$J(g) = \{z \in X : zgz^{-1} = g^{-1}\}.$$

Primero veamos que $|J(g)| \leq |C_G(g)|$. La función $J(g) \rightarrow C_G(g)$, $z \mapsto gz$, está bien definida, pues

$$(gz)g(gz)^{-1} = g(xgx^{-1})g^{-1} = g^{-1} \in C_G(g),$$

y es inyectiva, pues $gz = gz_1$ implica $z = z_1$.

Sea $\{(g, z) \in G \times X : zgz^{-1} = g^{-1}\}$. Como la función $X \times X \rightarrow J$, $(y, z) \mapsto (yz, z)$, está bien definida, pues $z(yz)z^{-1} = zy = (yz)^{-1}$, y es trivialmente una función inyectiva, tenemos entonces que

$$|X|^2 \leq |J| = \sum_{(g,z) \in J} 1 \leq \sum_{g \in G} |J(g)| = \sum_{g \in G} |C_G(g)| = k|G|,$$

donde k es la cantidad de clases de conjugación de G , pues $(g, z) \in J$ si y sólo si $z \in J(g)$. Luego $|G| \leq kn^2$, pues

$$\left(\frac{|G|}{|C_G(x)|} \right)^2 = |X|^2 = \frac{|G|}{n^2} \leq k|G|.$$

Afirmación. Existe alguna clase de conjugación que tiene $\leq 2n^2$ elementos.

De lo contrario, si C_1, \dots, C_k son las clases de conjugación de G , donde $C_1 = \{1\}$ y $|C_i| > 2n^2$ para todo $i \in \{2, \dots, k\}$, entonces

$$|G| = 1 + \sum_{i=2}^k |C_i| > 1 + \sum_{i=2}^k n^2 = 1 + (k-1)2n^2 \geq |G|,$$

una contradicción.

Afirmación. Existe un subgrupo H de G tal que $(G : H) \leq 2n^2$.

Sea C alguna clase de conjugación de G tal que $|C| \leq 2n^2$ y sea $g \in C$. Entonces $H = C_G(g)$ es un subgrupo de G tal que $(G : H) \leq 2n^2$. \square

Este resultado es uno de los primeros pasos hacia la clasificación de grupos simples finitos.

Capítulo 12

Inducción y restricción

Sea N es un subgrupo normal de G y sea $\pi: G \rightarrow G/N$, $g \mapsto gN$, el morfismo canónico. Si $\tilde{\chi}$ es un caracter de G/N , sea $\tilde{\rho}: G/N \rightarrow \mathbf{GL}(V)$ una representación de G/N con caracter $\tilde{\chi}$.

La composición $\rho = \tilde{\rho} \circ \pi: G \rightarrow \mathbf{GL}(V)$, $\rho(g) = \tilde{\rho}(gN)$, es un morfismo de grupos, luego es una representación de G . Entonces

$$\chi(g) = \text{traza } \rho(g) = \text{traza } (\tilde{\chi}(gN)) = \tilde{\chi}(gN).$$

En particular, $\chi(1) = \tilde{\chi}(1)$. El caracter χ es el **levantado** a G del caracter $\tilde{\chi}$ de G/N .

Lema 12.1. Si $\chi \in \text{Irr}(G)$, entonces

$$\ker \chi = \{g \in G : \chi(g) = \chi(1)\}$$

es un subgrupo normal de G .

Demostración. Sea $\rho: G \rightarrow \mathbf{GL}_n(\mathbb{C})$ una representación con caracter χ . Es claro que $\ker \rho \subseteq \ker \chi$, pues si $\rho_g = \text{id}$, entonces $\chi(g) = \text{traza}(\rho_g) = n = \chi(1)$. Demostremos que $\ker \chi \subseteq \ker \rho$. Si $g \in G$ es tal que $\chi(g) = \chi(1)$, como ρ_g es diagonalizable, existen autovalores $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ tales que

$$n = \chi(1) = \chi(g) = \sum_{i=1}^n \lambda_i.$$

Como los λ_i son raíces de la unidad, $\lambda_1 = \dots = \lambda_n = 1$. Luego $\rho_g = \text{id}$. □

El subgrupo $\ker \chi$ es el **núcleo** del caracter irreducible χ .

Teorema 12.2. Sea N un subgrupo normal de G . Existe una correspondencia biyectiva entre los caracteres de G/N y los caracteres χ de G tales que $N \subseteq \ker \chi$. Bajo esta correspondencia, caracteres irreducibles se corresponden con caracteres irreducibles.

Demostración. Si $\tilde{\chi} \in \text{Char}(G/N)$, sea χ el levantado de $\tilde{\chi}$ al grupo G . Si $n \in N$, entonces

$$\chi(n) = \tilde{\chi}(nN) = \tilde{\chi}(N) = \chi(1)$$

y luego $N \subseteq \ker \chi$.

Si $\chi \in \text{Char}(G)$ es tal que $N \subseteq \ker \chi$, sea $\rho: G \rightarrow \mathbf{GL}(V)$ una representación con caracter χ . Sea $\tilde{\rho}: G/N \rightarrow \mathbf{GL}(V)$, $gN \mapsto \rho(g)$. Veamos que $\tilde{\rho}$ está bien definida:

$$gN = hN \iff h^{-1}g \in N \iff \rho(h^{-1}g) = \text{id} \iff \rho(h) = \rho(g).$$

Además $\tilde{\rho}$ es una representación, pues

$$\tilde{\rho}((gN)(hN)) = \tilde{\rho}(ghN) = \rho(gh) = \rho(g)\rho(h) = \tilde{\rho}(gN)\tilde{\rho}(hN).$$

Si $\tilde{\chi}$ es el caracter de $\tilde{\rho}$, entonces $\tilde{\chi}(gN) = \chi(g)$.

Veamos que χ es irreducible si y sólo si $\tilde{\chi}$ es irreducible. Si U es un subespacio de V , entonces

$$\begin{aligned} U \text{ es un } \mathbb{C}[G]\text{-submódulo} &\iff g \cdot U \subseteq U \text{ para todo } g \in G \\ &\iff \rho(g)(U) \subseteq U \text{ para todo } g \in G \\ &\iff \tilde{\rho}(gN)(U) \subseteq U \text{ para todo } g \in G. \end{aligned}$$

Luego

$$\begin{aligned} \chi \text{ es irreducible} &\iff \rho \text{ es irreducible} \\ &\iff \tilde{\rho} \text{ es irreducible} \iff \tilde{\chi} \text{ es irreducible}. \quad \square \end{aligned}$$

Ejemplo 12.3. Sea $G = \mathbb{S}_4$ y sea $N = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$. Sabemos que N es normal en G y que $G/N = \langle a, b \rangle \simeq \mathbb{S}_3$, donde $a = (123)N$ y $b = (12)N$. La tabla de caracteres de G/N es entonces

	1	(12)N	(123)N
$\tilde{\chi}_1$	1	1	1
$\tilde{\chi}_2$	1	-1	1
$\tilde{\chi}_3$	2	0	-1

Para cada $i \in \{1, 2, 3\}$ vamos a calcular el levantado χ_i al grupo G del caracter $\tilde{\chi}_i$ de G/N . Como $(12)(34) \in N$ y $(13)(1234) = (12)(34) \in N$, entonces

$$\chi((12)(34)) = \tilde{\chi}(N), \quad \chi((1234)) = \tilde{\chi}((13)N) = \tilde{\chi}((12)N).$$

Como $\tilde{\chi}_i$ son irreducibles, también lo serán sus levantados χ_i . Al levantar los caracteres irreducibles del cociente G/N conseguimos los siguientes caracteres irreducibles del grupo G :

	1	(12)	(123)	(12)(34)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0

La tabla de caracteres de un grupo finito permite detectar los subgrupos normales del grupo y las inclusiones entre esos distintos subgrupos normales. Empezamos con un lema:

Lema 12.4. *Sea G un grupo finito y sean $g, h \in G$. Entonces g y h son conjugados si y sólo si $\chi(g) = \chi(h)$ para todo $\chi \in \text{Char}(G)$.*

Demostración. Si g y h son conjugados, entonces $\chi(g) = \chi(h)$, pues ya vimos que los caracteres son funciones de clases de G . Recíprocamente, si $\chi(g) = \chi(h)$ para todo $\chi \in \text{Char}(G)$, entonces $f(g) = f(h)$ para toda función de clases f de G , pues los caracteres de G generan el espacio de funciones de clases de G . En particular, $\delta(g) = \delta(h)$, donde δ es la función de clases

$$\delta(x) = \begin{cases} 1 & \text{si } x \text{ y } g \text{ son conjugados,} \\ 0 & \text{en otro caso,} \end{cases}$$

lo que implica que g y h son conjugados. □

Observemos ahora que

$$\bigcap_{\chi \in \text{Irr}(G)} \ker \chi = \{1\}. \quad (12.1) \quad \boxed{\text{eq:kernels}}$$

En efecto, si $g \in \ker \chi$ para todo $\chi \in \text{Irr}(G)$, entonces $g = 1$ pues el lema anterior nos dice que g y 1 son conjugados ya que $\chi(g) = \chi(1)$ para todo $\chi \in \text{Irr}(G)$.

Proposición 12.5. *Sea G un grupo finito. Si N es un subgrupo normal de G , entonces existen caracteres $\chi_1, \dots, \chi_k \in \text{Irr}(G)$ tales que*

$$N = \bigcap_{i=1}^k \ker \chi_i.$$

Demostración. La observación anterior para el grupo G/N nos dice que

$$\bigcap_{\tilde{\chi} \in \text{Irr}(G/N)} \ker \tilde{\chi} = \{N\}.$$

Supongamos que $\text{Irr}(G/N) = \{\tilde{\chi}_1, \dots, \tilde{\chi}_k\}$. Levantamos los caracteres irreducibles de G/N al grupo G y tenemos algunos caracteres irreducibles χ_1, \dots, χ_k del grupo G tales que $N \subseteq \ker \chi_1 \cap \dots \cap \ker \chi_k$. Si $g \in \ker \chi_i$ para todo $i \in \{1, \dots, k\}$, entonces

$$\tilde{\chi}_i(N) = \chi_i(1) = \chi_i(g) = \tilde{\chi}_i(gN)$$

para todo $i \in \{1, \dots, k\}$, lo que nos dice que

$$gN \in \bigcap_{i=1}^k \ker \tilde{\chi}_i = \{N\},$$

es decir $g \in N$. □

Como corolario tenemos un criterio para detectar la simplicidad de un grupo solamente con mirar la tabla de caracteres.

Proposición 12.6. *Sea G un grupo finito. Entonces G no es simple si y sólo si existe algún caracter no trivial χ tal que $\chi(g) = \chi(1)$ para algún $g \in G \setminus \{1\}$.*

Demostración. Supongamos que G no es simple, es decir que existe un subgrupo normal N propio y no trivial. Por la proposición anterior, existen $\chi_1, \dots, \chi_k \in \text{Irr}(G)$ tales que $N = \ker \chi_1 \cap \dots \cap \ker \chi_k$. En particular, existe algún caracter no trivial χ_i tal que $\ker \chi_i \neq \{1\}$, lo que nos dice que algún $g \in G \setminus \{1\}$ cumple con $\chi_i(g) = \chi_i(1)$.

Supongamos ahora que existe algún caracter irreducible no trivial χ tal que $\chi(g) = \chi(1)$ para algún $g \in G \setminus \{1\}$. En particular, $g \in \ker \chi$ y luego $\ker \chi \neq \{1\}$. Como χ es no trivial, $\ker \chi \neq G$. Luego $\ker \chi$ es un subgrupo normal propio y no trivial de G . \square

Ejemplo 12.7. Si existe un grupo G con una tabla de caracteres de la forma

χ_1	1	1	1	1	1	1
χ_2	1	1	1	-1	1	-1
χ_3	1	1	1	1	-1	-1
χ_4	1	1	1	-1	-1	1
χ_5	2	-2	2	0	0	0
χ_6	8	0	-1	0	0	0

entonces G no es simple.

De existir, este grupo G tiene que tener orden $\sum_{i=1}^6 \chi_i(1)^2 = 72$. El grupo de Mathieu M_9 tiene la tabla de caracteres.

Ejemplo 12.8. Sea $\alpha = \frac{1}{2}(-1 + \sqrt{7}i)$. Si existe un grupo G con una tabla de caracteres de la forma

χ_1	1	1	1	1	1	1
χ_2	7	-1	-1	1	0	0
χ_3	8	0	0	-1	1	1
χ_4	3	-1	1	0	α	$\bar{\alpha}$
χ_5	3	-1	1	0	$\bar{\alpha}$	α
χ_6	6	2	0	0	0	0

entonces G es simple.

De existir, este grupo G tiene que tener orden $\sum_{i=1}^6 \chi_i(1)^2 = 168$. De hecho,

$$\text{PSL}(2, 7) = \text{SL}(2, 7) / Z(\text{SL}(2, 7))$$

es un grupo que tiene esa tabla de caracteres.

Definición 12.9. Si U es un $K[G]$ -módulo y H es un subgrupo de G , podemos pensar a U como $K[H]$ -módulo al restringir la acción al subgrupo H . Este módulo será denotado por $\text{Res}_H^G U$ y se conoce como la **restricción** de U a H .

La restricción de un módulo irreducible puede no ser irreducible.

Ejemplo 12.10. Sea $G = \mathbb{D}_4 = \langle r, s : r^4 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diedral de ocho elementos. Sea V un espacio vectorial con base $\{v_1, v_2\}$. Entonces V es un $\mathbb{C}[\mathbb{D}_4]$ -módulo con

$$r \cdot v_1 = v_2, \quad r \cdot v_2 = -v_1, \quad s \cdot v_1 = v_1, \quad s \cdot v_2 = -v_2.$$

El caracter de V es

$$\chi(g) = \begin{cases} 2 & \text{si } g = 1, \\ -2 & \text{si } g = r^2, \\ 0 & \text{en otro caso.} \end{cases}$$

Observemos que χ es irreducible, pues $\langle \chi, \chi \rangle = 1$. Sea $H = \langle r^2, s \rangle = \{1, r^2, s, r^2s\}$. Entonces $\text{Res}_H^G V$ es V como $\mathbb{C}[H]$ -módulo con

$$r^2 \cdot v_1 = -v_1, \quad r^2 \cdot v_2 = -v_2, \quad s \cdot v_1 = -v_1, \quad s \cdot v_2 = -v_2.$$

El caracter de $\text{Res}_H^G V$ es

$$\chi_H(h) = \chi|_H(h) = \begin{cases} 2 & \text{si } h = 1, \\ -2 & \text{si } h = r^2, \\ 0 & \text{en otro caso.} \end{cases}$$

El carater χ_H no es irreducible ya que $\langle \chi_H, \chi_H \rangle = 0$.

Sea H un subgrupo de G y supongamos que $\text{Irr}(H) = \{\phi_1, \dots, \phi_l\}$. Si $\chi \in \text{Char}(G)$, entonces

$$\chi|_H = \sum_{i=1}^l d_i \phi_i$$

para ciertos enteros $d_1, \dots, d_l \geq 0$. Cada ϕ_i tal que $d_i = \langle \chi|_H, \phi_i \rangle \neq 0$ es una **parte irreducible** del caracter $\chi|_H$ y esos ϕ_i son las **partes irreducibles que constituyen** al caracter $\chi|_H$.

Proposición 12.11. Si H es un subgrupo de G y $\phi \in \text{Char}(H)$, entonces $\chi \in \text{Irr}(G)$ tal que $\langle \chi|_H, \phi \rangle_H \neq 0$.

Demostración. Supongamos que $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. Sabemos que si L es la representación regular de G , entonces

$$\chi_L(g) = \begin{cases} |G| & \text{si } g = 1, \\ 0 & \text{en otro caso.} \end{cases}$$

Si escribimos $\chi_L = \sum_{i=1}^k \chi_i(1) \chi_i$, entonces, como

$$0 \neq \frac{|G|}{|H|} \phi(1) = \langle \chi_L|_H, \phi \rangle_H = \sum_{i=1}^k \chi_i(1) \langle \chi_i|_H, \phi \rangle_H,$$

existe algún $i \in \{1, \dots, k\}$ tal que $\langle \chi_i|_H, \phi \rangle_H \neq 0$. \square

Proposición 12.12. Sean H un subgrupo de G y $\chi \in \text{Irr}(G)$. Si $\text{Irr}(H) = \{\phi_1, \dots, \phi_l\}$, entonces

$$\chi|_H = \sum_{i=1}^l d_i \phi_i,$$

donde $\sum_{i=1}^l d_i^2 \leq (G : H)$. Más aún, $\sum_{i=1}^l d_i^2 = (G : H)$ si y sólo si $\chi(g) = 0$ para todo $g \in G \setminus H$.

Demostración. Como

$$\sum_{i=1}^l d_i^2 = \langle \chi|_H, \chi|_H \rangle_H = \frac{1}{|H|} \sum_{h \in H} \chi(h) \overline{\chi(h)}.$$

Además, como χ es irreducible,

$$\begin{aligned} 1 = \langle \chi, \chi \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi(g)} \\ &= \frac{1}{|G|} \sum_{h \in H} \chi(h) \overline{\chi(h)} + \frac{1}{|G|} \sum_{g \in G \setminus H} \chi(g) \overline{\chi(g)} \\ &= \frac{|H|}{|G|} \sum_{i=1}^l d_i^2 + \frac{1}{|G|} \sum_{g \in G \setminus H} \chi(g) \overline{\chi(g)}. \end{aligned}$$

Como $\sum_{g \in G \setminus H} \chi(g) \overline{\chi(g)} \geq 0$, se concluye que $\sum_{i=1}^l d_i^2 \leq (G : H)$. Además vale la igualdad si y sólo si $\sum_{g \in G \setminus H} \chi(g) \overline{\chi(g)} = 0$, es decir si sólo si $\chi(g) = 0$ para todo $g \in G \setminus H$. \square

Discutiremos ahora la inducción de módulos. Para eso, repasaremos algunas nociones básicas sobre **bimódulos** y **producto tensorial de bimódulos**. Si R y S son anillos, un grupo abeliano M se dirá un (R, S) -bimódulo si M es un R -módulo a izquierda, M es un S -módulo a derecha y además

$$r \cdot (m \cdot s) = (r \cdot m) \cdot s$$

para todo $r \in R, s \in S$ y $m \in M$.

Ejemplos 12.13.

- 1) Un R -módulo a izquierda es un (R, \mathbb{Z}) -bimódulo.
- 2) Un S -módulo a derecha es un (\mathbb{Z}, S) -bimódulo.
- 3) Todo anillo R es un (R, R) -bimódulo.

Ejemplo 12.14. Si M es un (R, S) -bimódulo y N es un R -módulo, entonces el conjunto $\text{Hom}_R(M, N)$ de morfismos de R -módulos $M \rightarrow N$ es un S -módulo con

$$(s \cdot \varphi)(m) = \varphi(m \cdot s), \quad s \in S, \varphi \in \text{Hom}_R(M, N), m \in M.$$

Sean M un (R, S) -bimódulo, N un S -módulo y U un R -módulo. Diremos que una función $f: M \times N \rightarrow U$ es **balanceada** si

$$\begin{aligned} f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n), \\ f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2), \\ f(m \cdot s, n) &= f(m, s \cdot n), \\ f(r \cdot m, n) &= r \cdot f(m, n) \end{aligned}$$

para todo $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $r \in R$ y $s \in S$.

Ejemplo 12.15. Si M es un R -módulo, la función $f: R \times M \rightarrow M$, $(r, m) \mapsto r \cdot m$, es balanceada.

Sean M un (R, S) -bimódulo, N un S -módulo y U un R -módulo. Se define el **producto tensorial** $M \otimes_S N$ es un R -módulo provisto con una función balanceada $\eta: M \times N \rightarrow M \otimes_S N$ que cumple con la siguiente propiedad universal:

Si $f: M \times N \rightarrow U$ es una función balanceada, entonces existe un único morfismo de R -módulos $\alpha: M \otimes_S N \rightarrow U$ tal que $f = \alpha \circ \eta$.

Notación: $m \otimes n = \eta(m, n)$ para $m \in M$ y $n \in N$. El producto tensorial existe y puede demostrarse que es único salvo isomorfismos. Más precisamente, $M \otimes_S N$ se define como el R -módulo generado por el conjunto $\{m \otimes n : m \in M, n \in N\}$, donde los $m \otimes n$ satisfacen las siguientes identidades:

$$(m + m_1) \otimes n = m \otimes n + m_1 \otimes n \quad m, m_1 \in M, n \in N, \quad (12.2)$$

$$m \otimes (n + n_1) = m \otimes n + m \otimes n_1 \quad m \in M, n, n_1 \in N, \quad (12.3)$$

$$(ms) \otimes n = m \otimes (sn) \quad m \in M, n \in N, s \in S, \quad (12.4)$$

$$(rm) \otimes n = r(m \otimes n) \quad m \in M, n \in N, r \in R. \quad (12.5)$$

Un elemento arbitrario de $M \otimes_S N$ es una suma finita de la forma $\sum_{i=1}^k m_i \otimes n_i$, donde $m_1, \dots, m_k \in M$ y $n_1, \dots, n_k \in N$, y no necesariamente un tensor elemental $m \otimes n$.

Ejemplo 12.16. $M \simeq R \otimes_R M$ como R -módulos. Como la función $R \times M \rightarrow M$, $(r, m) \mapsto r \cdot m$, es balanceada, induce un morfismo $R \otimes_R M \rightarrow M$, $r \otimes m \mapsto r \cdot m$ con inversa $M \rightarrow R \otimes_R M$, $m \mapsto 1 \otimes m$.

Ejemplo 12.17. Si M_1, \dots, M_k son (R, S) -bimódulos y N es un S -módulo, entonces

$$(M_1 \oplus \dots \oplus M_k) \otimes_S N \simeq (M_1 \otimes_S N) \oplus \dots \oplus (M_k \otimes_S N).$$

Algunos ejercicios:

Ejercicio 12.18. Demuestre que $M \otimes_R N \simeq N \otimes_{R^{\text{op}}} M$.

Ejercicio 12.19. Demuestre que $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}$.

Ejercicio 12.20. Sean M un (R, S) -bimódulo y N un (S, T) -bimódulo. Demuestre que $M \otimes_S N$ es un (R, T) -bimódulo con $r(m \otimes n)t = (rm) \otimes (nt)$, donde $m \in M$, $n \in N$, $r \in R$, $t \in T$.

Ejercicio 12.21. Demuestre que $(M \otimes_R N) \otimes_R T \simeq M \otimes_R (N \otimes_R T)$.

Ejercicio 12.22. Enuncie y demuestre la asociatividad del producto tensorial de bimódulos.

Si G es un grupo finito, H es un subgrupo de G y V es un $K[H]$ -módulo, entonces $K[G]$ es un $(K[G], K[H])$ -bimódulo.

Definición 12.23. Sea G un grupo finito y sea H un subgrupo de G . Si V es un $K[H]$ -módulo de G , se define el $K[G]$ -módulo **inducido** de V como

$$\text{Ind}_H^G V = K[G] \otimes_{K[H]} V.$$

Si H es un subgrupo de G , un **transversal** (a izquierda) de H en G es un subconjunto T de G que contiene exactamente un elemento de cada coclase (a izquierda) de H en G .

Ejemplo 12.24. Si $G = \mathbb{S}_3$ y $H = \{\text{id}, (12)\}$, entonces $T = \{\text{id}, (123), (23)\}$ es un transversal de H en G . Podemos descomponer a G como

$$G = \{\text{id}, (12)\} \cup \{(123), (13)\} \cup \{(132), (23)\} = \bigcup_{t \in T} tH.$$

Como cada $g \in G$ se escribe en forma única como $g = th$ para $t \in T$ y $h \in H$, podemos definir una transformación lineal $\varphi: K[G] \rightarrow K[H] \oplus K[H] \oplus K[H] = |T|K[H]$, que para $g = th$ devuelve h en el lugar que corresponde a $t \in T$, es decir

$$\begin{aligned} \text{id} &\mapsto (\text{id}, 0, 0), & (12) &\mapsto ((12), 0, 0), & (123) &\mapsto (0, \text{id}, 0), \\ (23) &\mapsto (0, 0, \text{id}), & (13) &\mapsto (0, (12), 0), & (132) &\mapsto (0, 0, (12)). \end{aligned}$$

Por ejemplo,

$$\varphi(5(12) - 3(123) + 7\text{id}) = (7\text{id} + 5(12), -3\text{id}, 0).$$

Es importante observar que φ es un isomorfismo de $K[H]$ -módulos (a derecha).

La observación hecha en el ejemplo anterior es la clave del siguiente resultado.

Proposición 12.25. Sea G un grupo finito y sea H un subgrupo de G . Si V es un $K[H]$ -módulo de G , entonces

$$\text{Ind}_H^G(V) = \bigoplus_{t \in T} t \otimes V,$$

donde T es un transversal de H en G y $t \otimes V = \{t \otimes v : v \in V\}$. En particular, $\dim \text{Ind}_H^G V = (G : H) \dim V$.

Demostración. Descomponemos a G como unión disjunta de coclases de H con el transversal T , es decir

$$G = \bigcup_{t \in T} tH.$$

Cada $g \in G$ se escribe entonces unívocamente como $g = th$ con $t \in T$ y $h \in H$. Tal como hicimos en el ejemplo anterior, esto nos permite obtener un isomorfismo $\varphi: K[G] \rightarrow |T|K[H]$ de $K[H]$ -módulos (a derecha), donde $\varphi(g)$ es h en el sumando que corresponde a $t \in T$ y es cero en el resto de los sumandos. Luego

$$\text{Ind}_H^G V = K[G] \otimes_{K[H]} V \simeq (|T|K[H]) \otimes_{K[H]} V \simeq |T|(K[H] \otimes_{K[H]} V) \simeq |T|V$$

como $K[H]$ -módulos. En particular, $\dim \text{Ind}_H^G V = |T| \dim V$.

Si escribimos $g = th$ con $t \in T$ y $h \in H$, entonces $g \otimes v = (th) \otimes v = t \otimes h \cdot v \in t \otimes V$. Luego $K[G] \otimes_{K[H]} V \subseteq \bigoplus_{t \in T} t \otimes V$. La otra inclusión es trivial. Por definición, la suma sobre $t \in T$ de los $t \otimes V$ es directa. \square

Teorema 12.26 (Reciprocidad de Frobenius). *Sea G un grupo finito y H un subgrupo de G . Si U es un $K[G]$ -módulo y V es un $K[H]$ -módulo, entonces*

$$\text{Hom}_{K[H]}(V, \text{Res}_H^G U) \simeq \text{Hom}_{K[G]}(\text{Ind}_H^G V, U)$$

como espacios vectoriales.

Demostración. Si $\varphi \in \text{Hom}_{K[H]}(V, \text{Res}_H^G U)$, sea

$$f_\varphi: K[G] \times V \rightarrow U, \quad (g, v) \mapsto g \cdot \varphi(v).$$

Veamos que f_φ es balanceada. Un cálculo directo muestra que

$$f_\varphi(g + g_1, v) = f_\varphi(g, v) + f_\varphi(g_1, v), \quad f_\varphi(g, v + w) = f_\varphi(g, v) + f_\varphi(g, w).$$

Como φ es morfismo de $K[H]$ -módulos,

$$f_\varphi(gh, v) = (gh) \cdot \varphi(v) = g \cdot (h \cdot \varphi(v)) = g \cdot (h \cdot \varphi(v)) = g \cdot \varphi(h \cdot v) = f_\varphi(g, h \cdot v)$$

para todo $g \in G$, $h \in H$ y $v \in V$. Por último,

$$f_\varphi(gg_1, v) = (gg_1) \cdot \varphi(v) = g \cdot (g_1 \cdot \varphi(v)) = g \cdot f_\varphi(g_1, v)$$

para todo $g, g_1 \in G$ y $v \in V$. Para cada $\varphi \in \text{Hom}_{K[H]}(V, \text{Res}_H^G U)$ tenemos entonces un $\Gamma(\varphi) \in \text{Hom}_{K[G]}(\text{Ind}_H^G V, U)$ tal que $\Gamma(\varphi)(g \otimes v) = g \cdot \varphi(v)$. Tenemos así definida una función

$$\Gamma: \text{Hom}_{K[H]}(V, \text{Res}_H^G U) \rightarrow \text{Hom}_{K[G]}(\text{Ind}_H^G V, U), \quad \varphi \mapsto \Gamma(\varphi).$$

La función Γ es lineal e inyectiva, ambas afirmaciones fáciles de verificar.

Es también sobreyectiva, pues si $\theta \in \text{Hom}_{K[H]}(\text{Ind}_H^G V, U)$, entonces la función $\varphi(v) = \theta(1 \otimes v)$ es tal que $\varphi \in \text{Hom}_{K[H]}(V, \text{Res}_H^G U)$ y cumple

$$\Gamma(\varphi)(g \otimes v) = g \cdot \varphi(v) = g \cdot \theta(1 \otimes v) = \theta(g \otimes v). \quad \square$$

Supongamos ahora que $K = \mathbb{C}$.

Sea H un subgrupo de G . Si U es un $\mathbb{C}[G]$ -módulo con caracter χ , el caracter de $\text{Res}_H^G U$ se denota por $\chi|_H$ y vale que $\chi|_H(1) = \chi(1)$. Si V es un $\mathbb{C}[H]$ -módulo con caracter ϕ , el módulo $\text{Ind}_H^G V$ tiene caracter ϕ^G y vale que $\phi^G(1) = (G:H)\phi(1)$.

$$\langle \phi, \chi|_H \rangle_H = \dim \text{Hom}_{\mathbb{C}[H]}(V, \text{Res}_H^G U) = \dim \text{Hom}_{\mathbb{C}[G]}(\text{Ind}_H^G V, U) = \langle \phi^G, \chi \rangle_G,$$

donde $\langle \alpha, \beta \rangle_X = \sum_{x \in X} \alpha(x) \overline{\beta(x)}$ denota el producto interno del espacio de funciones $X \rightarrow \mathbb{C}$.

Definición 12.27. Si $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$ e $\text{Irr}(H) = \{\phi_1, \dots, \phi_l\}$, se define la **matriz de inducción-restricción** como la matriz $(c_{ij}) \in \mathbb{C}^{l \times k}$, donde

$$c_{ij} = \langle \phi_i^G, \chi_j \rangle_G = \langle \phi_i, \chi_j|_H \rangle_H.$$

La fila i -ésima de la matriz de inducción-restricción da la multiplicidad con que el caracter χ_j aparece en la descomposición de ϕ_i^G . La columna j -ésima da la multiplicidad con que el caracter ϕ_i aparece en la descomposición de $\chi_j|_H$.

Ejemplo 12.28. Sea $G = \mathbb{S}_3$. La tabla de caracteres de G es

	1	3	2
	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

La tabla de caracteres del subgrupo $H = \{\text{id}, (12)\}$ es

	1	1
	id	(12)
ϕ_1	1	1
ϕ_2	1	-1

A simple vista vemos que $\chi_1|_H = \phi_1$, $\chi_2|_H = \phi_2$ y que $\chi_3|_H = \phi_1 + \phi_2$. La matriz de inducción-restricción es entonces

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Observemos que además $\phi_1^G = \chi_1 + \chi_3$ y que $\phi_2^G = \chi_2 + \chi_3$.

Veamos cómo calcular explícitamente caracteres inducidos.

Proposición 12.29. Sea H un subgrupo de G y sea V es un $\mathbb{C}[H]$ -módulo con caracter χ . Si T es un transversal de H en G , entonces

$$\chi^G(g) = \sum_{\substack{t \in T \\ t^{-1}gt \in H}} \chi(t^{-1}gt)$$

para todo $g \in G$.

Demostración. Sabemos que $\text{Ind}_H^G V = \bigoplus_{t \in T} t \otimes V$. Supongamos que $T = \{t_1, \dots, t_m\}$ y sea $\{v_1, \dots, v_n\}$ una base de V . Entonces $\{t_i \otimes v_k : 1 \leq i \leq m, 1 \leq k \leq n\}$ es una base de $\text{Ind}_H^G V$ y la acción de g en $\text{Ind}_H^G V$ está dada por

$$\rho^G(g) = \begin{cases} \rho(t_j^{-1}gt_i) & \text{si } t_j^{-1}gt_i \in H, \\ 0 & \text{en otro caso.} \end{cases}$$

En efecto, si $gt_i = t_jh$ para $h \in H$ y ciertos i, j , entonces

$$g \cdot (t_i \otimes v_k) = gt_i \otimes v_k = t_jh \otimes v_k = t_j \otimes h \cdot v_k$$

y además $gt_i = t_jh$ si y sólo si $t_j^{-1}gt_i = h \in H$. Se concluye entonces que g actúa como $t^{-1}gt$ en V en caso en que $t^{-1}gt \in H$ y como la transformación nula en otro caso. \square

cor:inducccion

Corolario 12.30. Sea H un subgrupo de G y sea V es un $\mathbb{C}[H]$ -módulo con caracter χ . Si $g \in G$, entonces

$$\chi^G(g) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \chi(x^{-1}gx).$$

Demostración. Sea T un transversal de H en G . Si $x \in G$, escribimos $x = th$ para $t \in T$ y $h \in H$. Como $x^{-1}gx = h^{-1}(t^{-1}gt)h$, entonces $x^{-1}gx \in H \iff t^{-1}gt \in H$ y además, en ese caso, $\chi(x^{-1}gx) = \chi(t^{-1}gt)$ pues χ es una función de clases. Eso implica que existen $|H|$ elementos $x \in G$ tales que $x^{-1}gx \in H$. Para esos x , se tiene $\chi(x^{-1}gx) = \chi(t^{-1}gt)$, lo que implica el corolario. \square

Capítulo 13

El teorema de Frobenius

Frobenius

Recordemos que si p es un número primo, entonces las unidades $(\mathbb{Z}/p)^\times$ de \mathbb{Z}/p forman un grupo con la multiplicación. Más aún, $(\mathbb{Z}/p)^\times$ es un grupo cíclico de orden $p-1$.

Sean p y q números primos tales que q divide a $p-1$ y sea

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x \in (\mathbb{Z}/p)^\times, y \in \mathbb{Z}/p \right\}.$$

Es sencillo verificar que G es un grupo con la multiplicación usual de matrices y que $|G| = p(p-1)$. Sea $z \in \mathbb{Z}$ un elemento de orden q módulo p y sean

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} z & 1 \\ 0 & 1 \end{pmatrix}, \quad H = \langle a, b \rangle.$$

Un cálculo directo muestra que

$$a^p = b^q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad bab^{-1} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} = a^z. \quad (13.1) \quad \text{eq:pq}$$

Todo elemento de H es de la forma $a^i b^j$ para $i \in \{0, \dots, p-1\}$ y $j \in \{0, \dots, q-1\}$. Luego $|H| = pq$ y además las relaciones (13.1) nos permiten calcular completamente la tabla de multiplicación de G .

Ejercicio 13.1. Sean p y q dos primos tales que $q \mid p-1$. Sean $u, v \in \mathbb{Z}$ de orden q módulo p . Demuestre que

$$\langle a, b : a^p = b^q = 1, bab = a^u \rangle \simeq \langle a, b : a^p = b^q = 1, bab = a^v \rangle.$$

El grupo

$$F_{p,q} = \langle a, b : a^p = b^q = 1, bab = a^u \rangle,$$

donde $u \in \mathbb{Z}$ tiene orden q módulo p , es un caso particular de *grupo de Frobenius*.

Proposición 13.2. Sean p y q números primos tales que $p > q$ y sea G un grupo de orden pq . Entonces G es abeliano o bien $q \mid p-1$ y $G \simeq F_{p,q}$.

Demostración. Supongamos que G es no abeliano. Los teoremas de Sylow implican que q divide a $p-1$ y que además existe un único p -subgrupo de Sylow P de G . Sean $a, b \in G$ tales que $P = \langle a \rangle \simeq \mathbb{Z}/p$ y $G/P = \langle bP \rangle \simeq \mathbb{Z}/q$. Por el teorema de Lagrange, $G = \langle a, b \rangle$. Calculemos el orden de b^q . Como G no es cíclico (pues es no abeliano) y $b^q \in P$, se concluye que $|b^q| = q$. Como P es normal en G , $bab^{-1} \in P$ y entonces $bab^{-1} = a^z$ para algún $z \in \mathbb{Z}$. Luego $b^q ab^{-q} = a^{z^q}$, lo que implica que $z^q \equiv 1 \pmod{p}$. El orden de u en $(\mathbb{Z}/p)^\times$ divide entonces al primo q y luego es igual a q , pues de lo contrario, $u = 1$ y entonces $bab^{-1} = a$, lo que implicaría que G es abeliano. En conclusion, $G \simeq F_{p,q}$. \square

La proposición anterior nos permite demostrar, por ejemplo, que todo grupo de orden 15 es abeliano y que, salvo isomorfismos, $\mathbb{Z}/20$ y $F_{5,4}$ son los únicos grupos de orden 20.

Definición 13.3. Diremos que un grupo G es un **grupo de Frobenius** si G tiene un subgrupo propio no trivial H tal que $H \cap xHx^{-1} = \{1\}$ para todo $x \in G \setminus H$. En este caso, el subgrupo H se llama **complemento de Frobenius**.

theorem:Frobenius

Teorema 13.4 (Frobenius). Sea G un grupo de Frobenius con complemento H . Entonces

$$N = \left(G \setminus \bigcup_{x \in G} xHx^{-1} \right) \cup \{1\}$$

es un subgrupo normal de G .

Demostración. Para cada $\chi \in \text{Irr}(H)$, $\chi \neq 1_H$ definimos $\alpha = \chi - \chi(1)1_H \in \text{cf}(H)$, donde 1_H denota el caracter trivial de H .

Demostremos que $(\alpha^G)_H = \alpha$. Primero, $\alpha^G(1) = \alpha(1) = 0$. Si $h \in H \setminus \{1\}$, entonces, gracias al corolario 12.30,

$$\alpha^G(h) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}hx \in H}} \alpha(x^{-1}hx) = \frac{1}{|H|} \sum_{x \in H} \alpha(h) = \alpha(h),$$

pues si $x \notin H$, entonces, como $x^{-1}hx \in H$, se tiene que $h \in H \cap xHx^{-1} = \{1\}$.

Por la reciprocidad de Frobenius,

$$\langle \alpha^G, \alpha^G \rangle = \langle \alpha, (\alpha^G)_H \rangle = \langle \alpha, \alpha \rangle = 1 + \chi(1)^2. \quad (13.2)$$

eq:<a,a>=1+chi2

Nuevamente por la reciprocidad de Frobenius,

$$\langle \alpha^G, 1_G \rangle = \langle \alpha, (1_G)_H \rangle = \langle \alpha, 1_H \rangle = \langle \chi - \chi(1)1_H, 1_H \rangle = -\chi(1),$$

donde 1_G denota al caracter trivial de G . Si escribimos

$$\alpha^G = \sum_{\eta \in \text{Irr}(G)} \langle \alpha^G, \eta \rangle \eta = \langle \alpha^G, 1_G \rangle 1_G + \underbrace{\sum_{\substack{1_G \neq \eta \\ \eta \in \text{Irr}(G)}} \langle \alpha^G, \eta \rangle \eta}_{\phi}$$

entonces $\alpha^G = -\chi(1)1_G + \phi$, donde ϕ es una combinación lineal entera de caracteres irreducibles no triviales de G . Calculamos además

$$1 + \chi(1)^2 = \langle \alpha^G, \alpha^G \rangle = \langle \phi - \chi(1)1_G, \phi - \chi(1)1_G \rangle = \langle \phi, \phi \rangle + \chi(1)^2$$

y luego $\langle \phi, \phi \rangle = 1$.

Afirmación. Si $\eta \in \text{Irr}(G)$ es tal que $\eta \neq 1_G$, entonces $\langle \alpha^G, \eta \rangle \in \mathbb{Z}$.

En efecto, por la reciprocidad de Frobenius, $\langle \alpha^G, \eta \rangle = \langle \alpha, \eta_H \rangle$. Si descomponemos a η_H en irreducibles de H , digamos

$$\eta_H = m_1 1_H + m_2 \chi + m_3 \theta_3 + \cdots + m_t \theta_t$$

para ciertos $m_1, m_2, \dots, m_t \in \mathbb{N}_0$, entonces, como

$$\langle \alpha, 1_H \rangle = \langle \chi - \chi(1)1_H, 1_H \rangle = -\chi(1), \quad \langle \alpha, \chi \rangle = \langle \chi - \chi(1)1_H, \chi \rangle = 1,$$

y además

$$\langle \alpha, \theta_j \rangle = \langle \chi - \chi(1)1_H, \theta_j \rangle = 0$$

para todo $j \in \{3, \dots, t\}$, se concluye que

$$\langle \alpha^G, \eta \rangle = -m_1 \chi(1) + m_2 \in \mathbb{Z}.$$

Afirmación. $\phi \in \text{Irr}(G)$.

Como $\langle \alpha^G, \eta \rangle \in \mathbb{Z}$ para todo $\eta \in \text{Irr}(G)$ tal que $\eta \neq 1_G$ y además

$$1 = \langle \phi, \phi \rangle = \sum_{\substack{\eta, \theta \in \text{Irr}(G) \\ \eta, \theta \neq 1_G}} \langle \alpha^G, \eta \rangle \langle \alpha^G, \theta \rangle \langle \eta, \theta \rangle = \sum_{\substack{\eta \neq 1_G \\ \eta \in \text{Irr}(G)}} \langle \alpha^G, \eta \rangle^2,$$

entonces existe un único $\eta \in \text{Irr}(G)$ tal que $\langle \alpha^G, \eta \rangle^2 = 1$ y el resto de los productos es cero, es decir $\alpha^G = \pm \eta$ para un cierto $\eta \in \text{Irr}(G)$. Como además

$$\chi - \chi(1)1_H = \alpha = (\alpha^G)_H = (\phi - \chi(1)1_G)_H = \phi_H - \chi(1)1_H,$$

se tiene que $\phi(1) = \phi_H(1) = \chi(1) \in \mathbb{N}$. Luego $\phi \in \text{Irr}(G)$.

Observemos que hemos demostrado que si $\chi \in \text{Irr}(H)$ es tal que $\chi \neq 1_H$, entonces existe $\phi_\chi \in \text{Irr}(G)$ tal que $(\phi_\chi)_H = \chi$.

Vamos a demostrar que N es igual a

$$M = \bigcap_{\substack{\chi \in \text{Irr}(H) \\ \chi \neq 1_H}} \ker \phi_\chi.$$

Demostremos primero que $N \subseteq M$. Sea $n \in N \setminus \{1\}$ y sea $\chi \in \text{Irr}(H) \setminus \{1_H\}$. Como n no pertenece a ningún conjugado de H ,

$$\alpha^G(n) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}nx \in H}} \chi(x^{-1}nx) = 0$$

pues como $n \in N$ el conjunto $\{x \in G : x^{-1}nx \in H\}$ es vacío. Como entonces

$$0 = \alpha^G(n) = \phi_\chi(n) - \chi(1) = \phi_\chi(n) - \phi_\chi(1),$$

se concluye que $n \in \ker \phi_\chi$.

Demostremos ahora que $M \subseteq N$. Sea $h \in M \cap H$ y sea $\chi \in \text{Irr}(H) \setminus \{1_H\}$. Entonces

$$\phi_\chi(h) - \chi(1) = \alpha^G(h) = \alpha(h) = \chi(h) - \chi(1),$$

y luego $h \in \ker \chi$ pues

$$\chi(h) = \phi_\chi(h) = \phi_\chi(1) = \chi(1).$$

Por lo tanto $h \in \bigcap_\chi \ker \chi = \{1\}$, que vimos en la fórmula (12.1) que la intersección de los núcleos de los irreducibles es trivial. Demostremos ahora que $M \cap xHx^{-1} = \{1\}$ para todo $x \in G$. Sean $x \in G$ y $m \in M \cap xHx^{-1}$. Como $m = xhx^{-1}$ para algún $h \in H$, $x^{-1}mx \in H \cap M = \{1\}$. Esto implica que $m = 1$. \square

No se conoce una demostración del teorema de Frobenius que no use teoría de caracteres.

Definición 13.5. Sea G un grupo de Frobenius. El subgrupo normal N construido en el teorema de Frobenius se llama **núcleo de Frobenius**.

Corolario 13.6. Sea G un grupo de Frobenius con complemento H . Entonces existe un subgrupo normal N de G tal que $G = HN$, $H \cap N = \{1\}$.

Demostración. La existencia del subgrupo normal N está garantizada por el teorema de Frobenius. Demostremos que $H \subseteq N_H(H)$. Si $h \in H \setminus \{1\}$ y $g \in G$ son tales que $ghg^{-1} \in H$, entonces $h \in g^{-1}Hg \cap H$ y luego $g \in H$. Como entonces $H = N_G(H)$, el subgrupo H tiene $(G : H)$ conjugados y luego $|G| = |H||N|$ pues

$$|N| = |G| - (G : H)(|H| - 1) = (G : H).$$

Como $N \cap H = \{1\}$, entonces

$$|HN| = |N||H|/|H \cap N| = |N||H| = |G|$$

y luego $G = NH$. \square

Corolario 13.7 (Teorema de Frobenius, versión combinatoria). *Sea X un conjunto finito y sea G un grupo que actúa transitivamente en X . Supongamos que todo $g \in G \setminus \{1\}$ fija a lo sumo un punto de X . El conjunto N formado por la identidad y las permutaciones que mueven todos los puntos de X es un subgrupo de G .*

Demostración. Sea $x \in X$ y sea $H = G_x$. Veamos que si $g \in G \setminus H$ entonces $H \cap gHg^{-1} = 1$. Si $h \in H \cap gHg^{-1}$ entonces $h \cdot x = x$ y $g^{-1}hg \cdot x = x$. Como $g \cdot x \neq x$, entonces h fija dos puntos de X . Esto implica que $h = 1$ (pues todo elemento no trivial fija a lo sumo un punto de X).

Por el teorema 13.4, el conjunto

$$N = \left(G \setminus \bigcup_{g \in G} gHg^{-1} \right) \cup \{1\}$$

es un subgrupo de G . Veamos cómo son los elementos de N : Si $h \in \bigcup_{g \in G} gHg^{-1}$ entonces existe $g \in G$ tal que $g^{-1}hg \in H$, es decir $(g^{-1}hg) \cdot x = x$ o equivalentemente $h \in G_{g \cdot x}$. Luego, a excepción de la identidad, los elementos de N son los elementos de G que mueven algún punto de X . \square

Ejemplo 13.8. Sea F un cuerpo finito y sea G el grupo de funciones $f: G \rightarrow G$ de la forma $f(x) = ax + b$, $a, b \in F$ con $a \neq 0$. El grupo G actúa en F y toda $f \neq \text{id}$ fija a lo sumo un punto de F pues

$$x = f(x) = ax + b \implies x = 1 - (b/a).$$

En este caso, $N = \{f: f(x) = x + b, b \in F\}$ que es un subgrupo de G .

Ejercicio 13.9. Demuestre que el teorema 13.4 puede deducirse del corolario 13.7.

En su tesis doctoral Thompson demostró el siguiente resultado, que había sido conjeturado por Frobenius:

Teorema 13.10 (Thompson). *Sea G un grupo de Frobenius. Si N es el núcleo de Frobenius, entonces N es nilpotente.*

La demostración puede consultarse en el capítulo 6 de [19], más precisamente en el teorema 6.24.

Capítulo 14

Algunos teoremas de Burnside

Recordemos cómo actúa la representación natural del grupo simétrico. Sea $n \in \mathbb{N}$ y sea $\{e_1, \dots, e_n\}$ la base canónica de \mathbb{C}^n . La **representación natural** de \mathbb{S}_n es la representación

$$\rho: \mathbb{S}_n \rightarrow \mathbf{GL}(n, \mathbb{C}), \quad \sigma \mapsto \rho_\sigma,$$

donde $\rho_\sigma(e_j) = e_{\sigma(j)}$ para todo $j \in \{1, \dots, n\}$. La matriz de ρ_σ en la base canónica está dada por

$$(\rho_\sigma)_{ij} = \begin{cases} 1 & \text{si } i = \sigma(j), \\ 0 & \text{en otro caso.} \end{cases} \quad (14.1)$$

eq:Sn_natural

lem:permutaciones

Lema 14.1. Sea $n \in \mathbb{N}$ y sea $\rho: \mathbb{S}_n \rightarrow \mathbf{GL}(n, \mathbb{C})$ la representación natural del grupo simétrico. Si $A \in \mathbb{C}^{n \times n}$ y $\sigma \in \mathbb{S}_n$ entonces

$$A_{ij} = (\rho_\sigma A)_{\sigma(i)j} = (A \rho_\sigma)_{i\sigma^{-1}(j)}$$

para todo $i, j \in \{1, \dots, n\}$.

Demostración. Con la fórmula (14.1) calculamos

$$(A \rho_\sigma)_{ij} = \sum_{k=1}^n A_{ik} (\rho_\sigma)_{kj} = A_{i\sigma(j)}, \quad (\rho_\sigma A)_{ij} = \sum_{k=1}^n (\rho_\sigma)_{ik} A_{kj} = A_{\sigma^{-1}(i)j}. \quad \square$$

Definición 14.2. Sea G un grupo finito. Un caracter χ de G se dice **real** si $\chi = \overline{\chi}$, es decir si $\chi(g) \in \mathbb{R}$ para todo $g \in G$.

xca:chi_irreducible

Ejercicio 14.3. Demuestre que si χ es un carácter irreducible de un grupo finito G entonces $\overline{\chi}$ es irreducible.

Definición 14.4. Sea G un grupo. Una clase de conjugación C de G se dice **real** si para cada $g \in C$ se tiene $g^{-1} \in C$.

Utilizaremos la siguiente notación: si $C = \{xgx^{-1} : x \in G\}$ es una clase de conjugación de un grupo G , entonces $C^{-1} = \{xg^{-1}x^{-1} : x \in G\}$.

Teorema 14.5 (Burnside). *Sea G un grupo finito. La cantidad de clases de conjugación reales es igual a la cantidad de caracteres irreducibles reales.*

Demostración. Sea r la cantidad de clases de conjugación de G . Sean C_1, \dots, C_r las clases de conjugación de G y sean χ_1, \dots, χ_r los caracteres irreducibles de G . Sean $\alpha, \beta \in \mathbb{S}_r$ dados por $\bar{\chi}_i = \chi_{\alpha(i)}$ y $C_i^{-1} = C_{\beta(i)}$ para todo $i \in \{1, \dots, r\}$. Observar que χ_i es real si y sólo si $\alpha(i) = i$ y que C_i es real si y sólo si $\beta(i) = i$. La cantidad n de puntos fijos de α es igual a la cantidad de caracteres irreducibles de G y la cantidad m de puntos fijos de β es igual a la cantidad de clases reales.

Sea $\rho: \mathbb{S}_r \rightarrow \mathbf{GL}(r, \mathbb{C})$ la representación natural de \mathbb{S}_r . Entonces $\chi_\rho(\alpha) = n$ y $\chi_\rho(\beta) = m$. Veamos que $\text{traza } \rho_\alpha = \text{traza } \rho_\beta$. Sea $X \in \mathbf{GL}(r, \mathbb{C})$ la matriz de caracteres de G . Por el lema 14.1,

$$\rho_\alpha X = \bar{X} = X \rho_\beta.$$

Como X es una matriz inversible, $\rho_\alpha = X \rho_\beta X^{-1}$. Luego

$$n = \chi_\rho(\alpha) = \text{traza } \rho_\alpha = \text{traza } \rho_\beta = \chi_\rho(\beta) = m. \quad \square$$

corollary: $|G|$ impar

Corolario 14.6. *Sea G un grupo finito. Entonces $|G|$ es impar si y sólo si el único $\chi \in \text{Irr}(G)$ real es el caracter trivial.*

Demostración. Supongamos que G tiene una clase de conjugación C real no trivial y sea $g \in C$. Basta con demostrar que G tiene un elemento de orden par. Sea $h \in G$ tal que $hgh^{-1} = g^{-1}$. Entonces $h^2 \in C_G(g)$ (pues $h^2gh^{-2} = g$). Si $h \in \langle h^2 \rangle \subseteq C_G(g)$, g tiene orden par pues $g^{-1} = g$. Si $h \notin \langle h^2 \rangle$ entonces h^2 no es un generador de $\langle h \rangle$ y luego 2 divide a $|h|$ (pues $|h| \neq |h^2| = |h|/(|h|:2)$). Recíprocamente, si $|G|$ es par, existe $g \in G$ de orden dos y la clase de conjugación de g es real. \square

Teorema 14.7 (Burnside). *Sea G un grupo de orden impar y sea r el número de clases de conjugación de G . Entonces*

$$r \equiv |G| \pmod{16}.$$

Demostración. Como $|G|$ es impar, todo $\chi \in \text{Irr}(G)$ no trivial es no real por el corolario anterior. Los caracteres irreducibles de G son entonces

$$\chi_1, \chi_2, \bar{\chi}_2, \dots, \chi_k, \bar{\chi}_k, \quad r = 1 + 2k,$$

donde χ_1 representa al carácter trivial. Para cada $j \in \{2, \dots, k\}$ sea $d_j = \chi_j(1)$. Como cada d_j divide a $|G|$ por el teorema 7.9 de Frobenius y $|G|$ es impar, los d_j son números impares, digamos $d_j = 1 + 2m_j$. Entonces

$$\begin{aligned} |G| &= 1 + \sum_{j=2}^k 2d_j^2 = 1 + \sum_{j=2}^k 2(2m_j + 1)^2 \\ &= 1 + \sum_{j=2}^k 2(4m_j^2 + 4m_j + 1) = 1 + 2k + 8 \sum_{j=2}^k m_j(m_j + 1). \end{aligned}$$

Luego $|G| \equiv r \pmod{16}$ pues $r = 1 + 2k$ y cada $m_j(m_j + 1)$ es un número par. \square

Ejercicio 14.8. Demuestre que todo grupo de orden 15 es abeliano.

Capítulo 15

Grupos resolubles y teorema de Burnside

Si G es un grupo se define

$$G^{(0)} = G, \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad i \geq 0.$$

La **serie derivada** de G se define entonces como

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots$$

Cada $G^{(i)}$ es un subgrupo característico de G . Diremos que G es **resoluble** si existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$.

Ejemplo 15.1. Todo grupo abeliano es resoluble.

Ejemplo 15.2. El grupo $\mathrm{SL}_2(3)$ es resoluble. La serie derivada de $\mathrm{SL}_2(3)$ es

$$\mathrm{SL}_2(3) \supseteq Q_8 \supseteq C_4 \supseteq C_2 \supseteq 1.$$

Veamos el código:

```
gap> IsSolvable(SL(2,3));
true
gap> List(DerivedSeries(SL(2,3)), StructureDescription);
[ "SL(2,3)", "Q8", "C2", "1" ]
```

Ejemplo 15.3. Un grupo simple no abeliano no es resoluble.

theorem:resoluble

Teorema 15.4. Sea G un grupo.

- 1) Todo subgrupo H de G es resoluble.
- 2) Sea K es un subgrupo normal de G . Entonces G es resoluble si y sólo si K y G/K son resolubles.

Demostración. La primera afirmación es fácil pues $H^{(i)} \subseteq G^{(i)}$ para todo $i \geq 0$. Demostremos la segunda afirmación. Sean $Q = G/K$ y $\pi: G \rightarrow Q$ el morfismo canónico. Demostramos por inducción que $\pi(G^{(i)}) = Q^{(i)}$ para todo $i \geq 0$. El caso $i = 0$ es trivial pues π es sobreyectiva. Si el resultado es válido para algún $i \geq 0$ entonces

$$\pi(G^{(i+1)}) = \pi([G^{(i)}, G^{(i)}]) = [\pi(G^{(i)}), \pi(G^{(i)})] = [Q^{(i)}, Q^{(i)}] = Q^{(i+1)}.$$

Supongamos que Q y K son resolubles. Como Q es resoluble, existe n tal que $Q^{(n)} = 1$. Como $\pi(G^{(n)}) = Q^{(n)} = 1$, se tiene que $G^{(n)} \subseteq K$. Como K es resoluble, existe m tal que

$$G^{(n+m)} \subseteq (G^{(n)})^{(m)} \subseteq K^{(m)} = 1,$$

y luego G es resoluble.

Supongamos ahora que G es resoluble. Existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$. Luego Q es resoluble pues $Q^n = f(G^{(n)}) = f(1) = 1$. Además K es resoluble por ser un subgrupo de G . \square

Ejemplo 15.5. Sea $n \geq 5$. El grupo \mathbb{S}_n no es resoluble pues \mathbb{A}_n no es resoluble.

Ejemplo 15.6. Si H y K son grupos resolubles entonces $H \times K$ es resoluble.

Proposición 15.7. Sea p un número primo y sea G un p -grupo finito. Entonces G es resoluble.

Demostración. Procederemos por inducción en $|G|$. Supongamos que el resultado es válido para todos los p -grupos de orden $< |G|$. Como $Z(G) \neq 1$, por hipótesis inductiva $G/Z(G)$ es un p -grupo resoluble. Como $Z(G)$ es resoluble por ser un grupo abeliano, G es resoluble por el teorema 15.4. \square

Antes de demostrar el teorema de resolubilidad de Burnside vamos a demostrar un resultado auxiliar que resulta de interés. Necesitamos un resultado previo:

lem:4Burnside

Lema 15.8. Sean $\varepsilon_1, \dots, \varepsilon_n$ raíces de la unidad tales que $(\varepsilon_1 + \dots + \varepsilon_n)/n \in \mathbb{A}$. Entonces $\varepsilon_1 = \dots = \varepsilon_n$ o bien $\varepsilon_1 + \dots + \varepsilon_n = 0$.

Demostración. Sea $\alpha = (\varepsilon_1 + \dots + \varepsilon_n)/n$. Si los ε_j no son todos iguales, entonces $N(\alpha) < 1$. Además $N(\beta) < 1$ para todo conjugado algebraico β de α . Como el producto de los conjugados algebraicos de α es un entero de módulo < 1 , se concluye que es cero. \square

thm:Burnside_auxiliar

Teorema 15.9 (Burnside). Sea G un grupo finito. Sea $\phi: G \rightarrow \mathbf{GL}(n, \mathbb{C})$ una representación con carácter χ y sea C es una clase de conjugación de G tal que $(|C| : n) = 1$. Para cada $g \in C$ se tiene que $\chi(g) = 0$ o bien que ϕ_g es una matriz escalar.

Demostración. Sean $\varepsilon_1, \dots, \varepsilon_n$ los autovalores de ϕ_g . Como $(|C| : n) = 1$, existen $a, b \in \mathbb{Z}$ tales que $a|C| + bn = 1$. Como $|C|\chi(g)/n \in \mathbb{A}$, al multiplicar por $\chi(g)/n$ obtenemos

$$a|C|\frac{\chi(g)}{n} + b\chi(g) = \frac{\chi(g)}{n} = \frac{1}{n}(\varepsilon_1 + \dots + \varepsilon_n) \in \mathbb{A}.$$

El lema anterior nos dice que entonces hay dos posibilidades: $\varepsilon_1 = \dots = \varepsilon_n$ o bien $\varepsilon_1 + \dots + \varepsilon_n = 0$. En el primer caso, como ϕ_g es diagonalizable, ϕ_g es una matriz escalar. El segundo caso dice exactamente que $\chi(g) = 0$. \square

Teorema 15.10 (Burnside). *Sea p un número primo. Si G es un grupo finito y C es una clase de conjugación de G con $p^k > 1$ elementos, entonces G no es simple.*

Demostración. Sea $g \in C \setminus \{1\}$. Por la ortogonalidad de las columnas,

$$\begin{aligned} 0 &= \sum_{\chi \in \text{Irr}(G)} \chi(1)\chi(g) \\ &= \sum_{p|\chi(1)} \chi(1)\chi(g) + \sum_{p \nmid \chi(1)} \chi(1)\chi(g) + 1, \end{aligned} \quad (15.1) \quad \boxed{\text{eq:Burnside}}$$

donde el uno corresponde a la representación trivial de G .

Vamos a mirar esta ecuación módulo p . Más precisamente, si $\chi(g) = 0$ para todo $\chi \in \text{Irr}(G)$ tal que $\chi \neq \chi_1$ y $p \nmid \chi(1)$, entonces podemos escribir

$$-\frac{1}{p} = \sum \frac{\chi(1)}{p} \chi(g) \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z},$$

donde la suma se toma sobre todos los irreducibles no triviales de G de grado divisible por p , una contradicción. Luego existe una representación no trivial irreducible ϕ con carácter χ tal que p no divide a $\chi(1)$ y además $\chi(g) \neq 0$. Por el teorema anterior, ϕ_g es una matriz escalar. Si ϕ es fiel, entonces g es un elemento central no trivial, una contradicción pues $|C| > 1$. En caso contrario, G no es simple pues $\ker \phi$ es un subgrupo propio no trivial de G . \square

Teorema 15.11 (Burnside). *Sean p, q primos. Si G tiene orden $p^a q^b$ entonces G es resoluble.*

Demostración. Supongamos que el teorema no es cierto y sea G un grupo de orden $p^a q^b$ minimal con la propiedad de no ser resoluble. La minimalidad de $|G|$ implica que G es simple. Por el teorema anterior, G no tiene clases de conjugación de tamaño p^k ni clases de tamaño q^l con $k, l \geq 1$. El tamaño de toda clase de conjugación de G es entonces igual a uno o es divisible por pq . Pero entonces la ecuación de clases,

$$|G| = 1 + \sum_{C: |C| > 1} |C|,$$

donde la suma se hace sobre todas las clases de conjugación que tienen más de un elemento, da una contradicción. \square

Concluimos el capítulo con los enunciados de algunas generalizaciones del teorema de Burnside.

Teorema 15.12 (Kegel–Wielandt). *Si G es un grupo finito y existen subgrupos nilpotentes A y B de G tales que $G = AB$, entonces G es resoluble.*

La demostración del teorema de Kegel–Wielandt puede consultarse en el segundo capítulo del libro [2], más precisamente en el teorema 2.13.

Teorema 15.13 (Feit–Thompson). *Todo grupo finito de orden impar es resoluble.*

La demostración del teorema de Feit–Thompson es extremadamente difícil y ocupa un volumen completo del *Pacific Journal of Mathematics* [9]. En [11] se anunció haber verificado formalmente demostración del teorema de Feit–Thompson con el sistema de ayuda para la demostración de teoremas Coq.

En los sesenta se sabía que la demostración del teorema de Feit–Thomson iba a poder simplificarse si la conjetura de Feit–Thompson es verdadera:

No existen primos distintos p y q tales que $\frac{p^q-1}{p-1}$ divide a $\frac{q^p-1}{q-1}$.

Ya no es necesaria esa conjetura para simplificar la demostración, y la conjetura de Feit–Thompson permanece abierta. En [33] Stephens demostró que la versión fuerte de la conjetura no es cierta, ya que los enteros $\frac{p^q-1}{p-1}$ y $\frac{q^p-1}{q-1}$ podrían tener factores en común. De hecho, si $p = 17$ y $q = 3313$, entonces

$$\text{mcd}\left(\frac{p^q-1}{p-1}, \frac{q^p-1}{q-1}\right) = 112643.$$

Hoy podemos reproducir los cálculos de Stephens con casi cualquier computadora de escritorio:

```
gap> Gcd((17^3313-1)/16, (3313^17-1)/3312);
112643
```

Otra dirección en la que puede generalizarse el teorema de Burnside es con el uso de las funciones de palabra. Una *función de palabra* de un grupo G es una función

$$G^k \rightarrow G, \quad (x_1, \dots, x_k) \mapsto w(x_1, \dots, x_k)$$

para alguna palabra $w(x_1, \dots, x_k)$ en el grupo libre F_k de rango k . Algunas palabras son sobreyectivas en todo grupo o en cierta familia de grupos. Por ejemplo, la conjetura de Ore es la sobreyectividad de la función $(x, y) \mapsto [x, y] = xyx^{-1}y^{-1}$ en todo grupo finito simple no abeliano.

Teorema 15.14 (Guralnick–Liebeck–O’Brien–Shalev–Tiep). Sean p y q dos primos, $a, b \geq 0$ y $N = p^a q^b$. La función $(x, y) \mapsto x^N y^N$ es sobreyectiva en todo grupo simple.

El teorema fue demostrado en [13].

Veamos por qué implica el teorema de Burnside. Supongamos que G es un grupo de orden $N = p^a q^b$ y que G no es resoluble. Si fijamos una serie de composición de G , tenemos un factor S no abeliano de orden que divide a N . Como entonces S es simple y no abeliano y $s^N = 1$, se concluye que la función $(x, y) \mapsto x^N y^N$ tiene imagen trivial en S , una contradicción al teorema.

Capítulo 16

Un teorema de Hurwitz

En esta sección demostraremos un teorema de Hurwitz sobre el producto de sumas de cuadrados. Sabemos que $x^2y^2 = (xy)^2$ vale para todo $x, y \in \mathbb{C}$. Fibonnaci descubrió una identidad un poquito más interesante:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

Euler y Hamilton, de forma independiente, descubrieron una identidad similar para cuatro cuadrados:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

donde

$$\begin{aligned} z_1 &= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, & z_2 &= x_2y_1 + x_1y_2 - x_4y_3 + x_3y_4, \\ z_3 &= x_3y_1 + x_4y_2 + x_1y_3 - x_2y_4, & z_4 &= x_4y_1 - x_3y_2 + x_2y_3 - x_1y_4. \end{aligned} \quad (16.1) \quad \boxed{\text{eq:Hamilton}}$$

Cayley descubrió una identidad similar para sumas de ocho cuadrados. Es natural preguntarse si existen otras identidades de este estilo. Hurwitz demostró que esto no es posible. Veremos una demostración de Eckmann que utiliza representaciones de grupos. Vamos a necesitar estudiar algunas propiedades de un cierto grupo finito:

Lema 16.1. *Sea $n > 2$ un número par. Supongamos que existe un grupo G con generadores $\varepsilon, x_1, \dots, x_{n-1}$ y relaciones*

$$x_1^2 = \dots = x_{n-1}^2 = \varepsilon \neq 1, \quad \varepsilon^2 = 1, \quad [x_i, x_j] = \varepsilon \quad \text{si } i \neq j.$$

Entonces valen las siguientes afirmaciones:

- 1) $|G| = 2^n$.
- 2) $[G, G] = \{1, \varepsilon\}$.
- 3) Si $g \notin Z(G)$, entonces la clase de conjugación de g es $\{g, \varepsilon g\}$.
- 4) $Z(G) = \{1, \varepsilon, x_1 \dots x_{n-1}, \varepsilon x_1 \dots x_{n-1}\}$.
- 5) G tiene $2^{n-1} + 2$ clases de conjugación.

Demostración. Primero demostramos las dos primeras afirmaciones. Observemos que $\varepsilon \in Z(G)$ pues $\varepsilon = x_i^2$ para todo $i \in \{1, \dots, n-1\}$. Como $n-1 > 2$, $[x_1, x_2] = \varepsilon$ y luego $\varepsilon \in [G, G]$. Además $G/\langle \varepsilon \rangle$ es abeliano y luego $[G, G] = \langle \varepsilon \rangle$. Como $G/[G, G]$ es elemental abeliano de orden 2^{n-1} , se sigue que $|G| = 2^n$.

Demostremos ahora la tercera afirmación. Sea $g \in G \setminus Z(G)$ y sea $x \in G$ tal que $[x, g] \neq 1$. Entonces $[x, g] = \varepsilon$ y luego $xgx^{-1} = \varepsilon g$.

Demostremos la cuarta afirmación. Sea $g \in G$ y escribamos

$$g = \varepsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}},$$

donde $a_j \in \{0, 1\}$ para todo $j \in \{1, \dots, n-1\}$. Si $g \in Z(G)$ entonces $gx_i = x_i g$ para todo $i \in \{1, \dots, n-1\}$. Luego $g \in Z(G)$ si y sólo si

$$\varepsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}} = x_i (\varepsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}}) x_i^{-1}.$$

Como $x_i x_j^{a_j} x_i = \varepsilon^{a_j} x_j^{a_j}$ si $i \neq j$ y $\varepsilon \in Z(G)$, el elemento g es central si y sólo si

$$\sum_{\substack{j=1 \\ j \neq i}}^{n-1} a_j \equiv 0 \pmod{2}$$

para todo $i \in \{1, \dots, n-1\}$. En particular,

$$\sum_{j \neq i} a_j \equiv \sum_{j \neq k} a_j$$

para todo $k \neq i$, y en consecuencia $a_i \equiv a_k \pmod{2}$ para todo $i, k \in \{1, \dots, n-1\}$. Luego $a_1 = \cdots = a_{n-1}$ y entonces $Z(G) = \{1, x_1 \cdots x_{n-1}, \varepsilon, \varepsilon x_1 \cdots x_{n-1}\}$.

La última afirmación es entonces consecuencia de la ecuación de clases. Como

$$2^n = |G| = |Z(G)| + \sum_{i=1}^N 2 = 4 + 2N,$$

se concluye que G tiene $N + 4 = 2^{n-1} + 2$ clases de conjugación. \square

Ejemplo 16.2. Las fórmulas (16.1) dan una representación del grupo G del lema anterior. Escribamos a cada z_i como $z_i = \sum_{k=1}^4 a_{ik}(x_1, \dots, x_4)y_k$. Sea A la matriz tal que $A_{ij} = a_{ij}(x_1, \dots, x_4)$, es decir

$$A = \begin{pmatrix} x_1 & -x_2 & -x_3 & -x_4 \\ x_2 & x_1 & -x_4 & x_3 \\ x_3 & x_4 & x_1 & -x_2 \\ x_4 & -x_3 & x_2 & -x_1 \end{pmatrix}$$

La matriz A puede escribirse como $A = A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4$, donde $A_1 = I$ y

$$A_2 = \begin{pmatrix} & -1 \\ 1 & \\ & -1 \\ & & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} & -1 \\ & & 1 \\ 1 & \\ & -1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} & -1 \\ & & -1 \\ & 1 \\ 1 \end{pmatrix}.$$

Para cada $i \in \{1, \dots, 4\}$ sea $B_i = A_4^T A_i$. Entonces $B_i = -B_i^T$ y $B_i^2 = -I$ para todo i y además $B_i B_j = -B_j B_i$ para todo $i \neq j$. El grupo generado por B_1, B_2, B_3 está formado por elementos de la forma

$$\pm B_1^{k_1} B_2^{k_2} B_3^{k_3}$$

para $k_j \in \{0, 1\}$ y luego tiene orden 2^3 . La función $G \rightarrow \langle B_1, B_2, B_3 \rangle$,

$$x_1 \mapsto B_1, \quad x_2 \mapsto B_2, \quad x_3 \mapsto B_3$$

se extiende entonces a un isomorfismo de grupos.

Teorema 16.3 (Hurwitz). *Si existe una identidad*

$$(x_1^2 + \dots + x_n^2)(y_1^2 + \dots + y_n^2) = z_1^2 + \dots + z_n^2, \quad (16.2)$$

eq: Hurwitz

donde los x_j y los y_j son números complejos y las z_k son funciones bilineales en los x_j y los y_j , entonces $n \in \{1, 2, 4, 8\}$.

Demostración. Sin pérdida de generalidad podemos suponer que $n > 2$. Para cada $i \in \{1, \dots, n\}$ escribimos

$$z_i = \sum_{k=1}^n a_{ik}(x_1, \dots, x_n) y_k,$$

donde las a_{ik} son funciones lineales. Entonces

$$z_i^2 = \sum_{k,l=1}^n a_{ik}(x_1, \dots, x_n) a_{il}(x_1, \dots, x_n) y_k y_l$$

para todo $i \in \{1, \dots, n\}$. Si usamos estas expresiones para los z_i en (16.2) y comparamos coeficientes obtenemos

$$\sum_{i=1}^n a_{ik}(x_1, \dots, x_n) a_{il}(x_1, \dots, x_n) = \delta_{k,l}(x_1^2 + \dots + x_n^2), \quad (16.3)$$

eq: delta

donde $\delta_{k,l}$ es la función delta de Kronecker. Escribamos esta última expresión matricialmente. Para eso, sea A la matriz de $n \times n$ dada por

$$A_{ij} = a_{ij}(x_1, \dots, x_n).$$

Entonces

$$AA^T = (x_1^2 + \dots + x_n^2)I, \quad (16.4)$$

eq: AAT

donde I es la matriz identidad de $n \times n$ pues

$$(AA^T)_{kl} = \sum_{i=1}^n a_{ki}(x_1, \dots, x_n) a_{li}(x_1, \dots, x_n) = \delta_{kl}(x_1^2 + \dots + x_n^2)$$

por la fórmula (16.3). Como cada $a_{ki}(x_1, \dots, x_n)$ es una función lineal, existen escalares $\alpha_{ij1}, \dots, \alpha_{ijn} \in \mathbb{C}$ tales que

$$a_{ij}(x_1, \dots, x_n) = \alpha_{ij1}x_1 + \dots + \alpha_{ijn}x_n.$$

Podemos escribir entonces

$$A = A_1x_1 + \dots + A_nx_n,$$

donde cada A_k es la matriz $(A_k)_{ij} = \alpha_{ijk}$. La fórmula (16.4) queda entonces

$$\sum_{i=1}^n \sum_{j=1}^n A_i A_j^T x_i x_j = (x_1^2 + \dots + x_n^2)I.$$

Luego

$$A_i A_j^T + A_j A_i^T = 0 \quad i \neq j, \quad A_i A_i^T = I. \quad (16.5)$$

eq:condiciones

Queremos entonces encontrar n matrices complejas de $n \times n$ que cumplan las condiciones (16.5). Para cada $i \in \{1, \dots, n\}$ sea $B_i = A_n^T A_i$. Entonces (16.5) queda ahora

$$B_i B_j^T + B_j B_i^T = 0 \quad i \neq j, \quad B_i B_i^T = I, \quad B_n = I.$$

Al poner $j = n$ en la primera ecuación obtenemos que $B_i = -B_i^T$ vale para todo $i \in \{1, \dots, n-1\}$ y luego $B_i B_j = -B_j B_i$ para todo $i, j \in \{1, \dots, n-1\}$.

Afirmamos que n es par. De hecho, al calcular el determinante de $B_i B_j = -B_j B_i$ obtenemos $\det(B_i B_j) = (-1)^n \det(B_j B_i)$ y luego n es par pues $1 = (-1)^n$.

Si existe una solución a 16.2, entonces se tiene una representación fiel del grupo G del lema anterior (y en particular, este grupo existe). Como $G/[G, G]$ tiene orden 2^{n-1} , G admite 2^{n-1} representaciones de grado uno. Como G tiene $2^{n-1} + 2$ clases de conjugación, G admite dos representaciones irreducibles de grados $f_1 > 1$ y $f_2 > 1$ respectivamente. Además

$$2^n = |G| = \underbrace{1 + \dots + 1}_{2^{n-1}} + f_1^2 + f_2^2 = 2^{n-1} + f_1^2 + f_2^2$$

implica que $f_1 = f_2 = 2^{\frac{n-2}{2}} > 1$. Nuestra representación de G no contiene subrepresentaciones de grado uno (pues en esta representación ε debería representarse como $-I$ y en las representaciones de grado uno ε es trivial porque $\varepsilon \in [G, G]$). Luego $2^{\frac{n-2}{2}}$ divide a n . Al escribir $n = 2^a b$ con $a \geq 1$ y b un número impar, tenemos que $\frac{n-2}{2} \leq a$ y luego $n \in \{4, 8\}$ pues $2^a \leq n \leq 2a + 2$. \square

Veamos una aplicación.

Teorema 16.4. *Sea V un espacio vectorial real con producto interno tal que $\dim V = n \geq 3$. Si existe una función $V \times V \rightarrow \mathbb{R}$, $(v, w) \mapsto v \times w$, bilineal tal que $v \times w$ es ortogonal a v y a w y además*

$$\|v \times w\|^2 = \|v\|^2 \|w\|^2 - \langle v, w \rangle^2,$$

donde $\|v\|^2 = \langle v, v \rangle$, entonces $n \in \{3, 7\}$.

Demostración. Sea $W = V \oplus \mathbb{R}$ con el producto escalar

$$\langle (v_1, r_1), (v_2, r_2) \rangle = \langle v_1, v_2 \rangle + r_1 r_2.$$

Primero observemos que

$$\begin{aligned} & \langle v_1 \times v_2 + r_1 v_2 + r_2 v_1, v_1 \times v_2 + r_1 v_2 + r_2 v_1 \rangle \\ &= \|v_1 \times v_2\|^2 + r_1^2 \|v_2\|^2 + 2r_1 r_2 \langle v_1, v_2 \rangle + r_2^2 \|v_1\|^2. \end{aligned}$$

Luego

$$\begin{aligned} & (\|v_1\|^2 + r_1^2)(\|v_2\|^2 + r_2^2) \\ &= \|v_1\|^2 \|v_2\|^2 + r_1^2 \|v_1\|^2 + r_1^2 \|v_2\|^2 + r_1^2 r_2^2 \\ &= \|v_1 \times v_2 + r_1 v_1 + r_2 v_2\|^2 - 2r_1 r_2 \langle v_1, v_2 \rangle + \langle v_1, v_2 \rangle^2 + r_1^2 r_2^2 \\ &= \|v_1 \times v_2 + r_1 v_1 + r_2 v_2\|^2 + (\langle v_1, v_2 \rangle - r_1 r_2)^2 \\ &= z_1^2 + \cdots + z_{n+1}^2, \end{aligned}$$

donde las z_k son funciones bilineales en (v_1, r_1) y (v_2, r_2) . El teorema de Hurwitz implica entonces que $n+1 \in \{4, 8\}$ y luego $n \in \{3, 7\}$. \square

Si en el teorema anterior $\dim V = 3$, el resultado nos da el producto vectorial usual. Si en cambio $\dim V = 7$, sea

$$W = \{(v, k, w) : v, w \in V, k \in \mathbb{R}\}$$

con el producto interno dado por

$$\langle (v_1, k_1, w_1), (v_2, k_2, w_2) \rangle = \langle v_1, v_2 \rangle + k_1 k_2 + \langle w_1, w_2 \rangle.$$

Queda como ejercicio demostrar que la operación

$$\begin{aligned} & (v_1, k_1, w_1) \times (v_2, k_2, w_2) \\ &= (k_1 w_2 - k_2 w_1 + v_1 \times v_2 - w_1 \times w_2, \\ & \quad - \langle v_1, w_2 \rangle + \langle v_2, w_1 \rangle, k_2 v_1 - k_1 v_2 - v_1 \times w_2 - w_1 \times v_2) \end{aligned}$$

cumple las propiedades del teorema.

Parte III
Teoría de grupos

Capítulo 17

El teorema de Itô

Definición 17.1. Un grupo G se dice **metabeliano** si $[G, G]$ es abeliano.

Ejercicio 17.2. Demuestre que un grupo G es metabeliano si y sólo si existe un subgrupo normal K de G tal que K y G/K son abelianos.

Ejercicio 17.3. Sea G un grupo metabeliano.

- 1) Si H es un subgrupo de G entonces H es metabeliano.
- 2) Si $f: G \rightarrow H$ es un morfismo entonces $f(H)$ es metabeliano.

Lema 17.4. En un grupo valen las siguientes fórmulas:

- 1) $[a, bc] = [a, b]b[a, c]b^{-1}$.
- 2) $[ab, c] = a[b, c]a^{-1}[a, c]$.

Demostración. Es un cálculo directo:

$$\begin{aligned} [a, b]b[a, c]b^{-1} &= aba^{-1}b^{-1}baca^{-1}c^{-1}b^{-1} = abca^{-1}c^{-1}b^{-1} = [a, bc], \\ a[b, c]a^{-1}[a, c] &= abcb^{-1}c^{-1}a^{-1}aca^{-1}c^{-1} = abcb^{-1}a^{-1}c^{-1} = [ab, c]. \quad \square \end{aligned}$$

Ejemplo 17.5. El grupo \mathbb{S}_3 es metabeliano pues $\mathbb{A}_3 \simeq C_3$ es un subgrupo normal de \mathbb{S}_3 tal que $\mathbb{S}_3/\mathbb{A}_3 \simeq C_2$ es abeliano.

Ejemplo 17.6. El grupo \mathbb{A}_4 es metabeliano pues el subgrupo

$$K = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$$

es abeliano y normal en \mathbb{A}_4 y el cociente $\mathbb{A}_4/K \simeq C_3$ es abeliano.

Ejemplo 17.7. El grupo $\mathbf{SL}_2(3)$ no es metabeliano pues $[\mathbf{SL}_2(3), \mathbf{SL}_2(3)] \simeq Q_8$ no es un grupo abeliano. En efecto:

```
gap> IsAbelian(DerivedSubgroup(SL(2,3)));
false
gap> StructureDescription(DerivedSubgroup(SL(2,3)));
"Q8"
```

theorem:Itô

Teorema 17.8 (Itô). Sea $G = AB$ una factorización de G con A y B subgrupos de G abelianos. Entonces G es metabeliano.

Demostración. Como $G = AB$ entonces $AB = BA$. Veamos primero que $[A, B]$ es un subgrupo normal de G . Sean $a, \alpha \in A, b, \beta \in B$. Sean $a_1, a_2 \in A, b_1, b_2 \in B$ tales que $\alpha b \alpha^{-1} = b_1 a_1, \beta a \beta^{-1} = a_2 b_2$. Entonces, como

$$\begin{aligned}\alpha[a, b]\alpha^{-1} &= a(\alpha b \alpha^{-1})a^{-1}(\alpha b^{-1}\alpha^{-1}) = ab_1 a_1 a^{-1} a_1^{-1} b_1^{-1} = [a, b_1] \in [A, B] \\ \beta[a, b]\beta^{-1} &= (\beta a \beta^{-1})\beta b \beta^{-1}(\beta a^{-1}\beta^{-1})b^{-1} = a_2 b_2 b b_2^{-1} a_2^{-1} b^{-1} = [a_2, b] \in [A, B],\end{aligned}$$

se concluye que $[A, B]$ es normal en G .

Veamos ahora que $[A, B]$ es abeliano. Como

$$\begin{aligned}\beta \alpha[a, b]\alpha^{-1} \beta^{-1} &= \beta[a, b_1]\beta^{-1} = (\beta a \beta^{-1})b_1(\beta a^{-1}\beta^{-1})b_1^{-1} = [a_2, b_1], \\ \alpha \beta[a, b]\beta^{-1} \alpha^{-1} &= \alpha[a_2, b]\alpha^{-1} = a_2(\alpha b \alpha^{-1})a_2^{-1}(\alpha b^{-1}\alpha^{-1}) = [a_2, b_1],\end{aligned}$$

un cálculo directo muestra que

$$[\alpha^{-1}, \beta^{-1}][a, b][\alpha^{-1}, \beta^{-1}]^{-1} = [a, b].$$

Como dos generadores arbitrarios de $[A, B]$ conmutan, el grupo $[A, B]$ es abeliano.

Para completar la demostración observamos $[G, G] = [A, B]$ pues

$$[a_1 b_1, a_2 b_2] = a_1 [a_2, b_1]^{-1} a_1^{-1} a_2 [a_1, b_2] a_2^{-1} \subseteq [A, B],$$

ya que $[A, B]$ es normal en G . □

Capítulo 18

El teorema del matrimonio de Hall

Supongamos que tenemos un conjunto finito de personas p_1, p_2, \dots, p_n y cada uno de esas personas, digamos la persona p_i , se postuló en varios trabajos, digamos T_i . Nos interesa saber bajo qué condiciones todas las personas podrán obtener un trabajo al que se postularon.

Teorema 18.1 (Hall). *El problema tiene solución si y sólo si para cada $k \in \{1, \dots, n\}$ cada conjunto de k personas se postula en al menos k trabajos.*

Demostración. Demostremos primero la implicación fácil. Si existe un conjunto de k personas que se postuló a menos de k trabajos, entonces alguna de esas personas no podrá conseguir trabajo.

Para demostrar la afirmación recíproca procederemos por inducción en n , la cantidad de personas. El caso $n = 1$ es trivial. Supongamos entonces que el teorema es válido si hay $< n$ personas. Si hay n personas, hay dos casos a considerar.

Si todo conjunto de k personas, $k < n$, se postula colectivamente al menos a $k + 1$ trabajos, entonces la condición de Hall se verifica (y sobrarán un trabajo). Elegimos cualquier persona para que trabaje donde se haya postulado. Como la condición de Hall vale para las $n - 1$ personas restantes, esas personas conseguirán un trabajo al que se postularon gracias a la hipótesis inductiva.

Si, en cambio, existe un conjunto de k personas que se postula colectivamente a exactamente k trabajos, estas k personas, por hipótesis inductiva, podrán conseguir trabajo. Quedan ahora $n - k$ personas sin trabajo. Para cada $l \leq n - k$, toda colección de l de estas personas se postula al menos a l trabajos (pues de lo contrario, estas l personas junto con las k personas anteriores se hubieran postulado colectivamente a $< l + k$ trabajos, una contradicción). Podemos aplicar entonces la hipótesis inductiva a esas $n - k$ personas y vemos que también podrán conseguir trabajo. \square

El teorema fue demostrado por Hall en 1935, aunque con una prueba distinta. La demostración que presentamos es básicamente la de Halmos y Vaughan [?], aunque allí el teorema se presenta en términos de hombres, mujeres y matrimonios.

Teorema 18.2 (Hall). *Sea G un grupo finito y $H \leq G$ tal que $(G : H) = n$. Existen $g_1, \dots, g_n \in G$ tales que $\{g_1H, \dots, g_nH\} = \{Hg_1, \dots, Hg_n\}$.*

Demostración. Supongamos que $\{x_1, \dots, x_n\}$ es un sistema completo de representantes de coclases de H a derecha y $\{y_1, \dots, y_n\}$ es un sistema completo de representantes de coclases de H a izquierda. Para cada $i \in \{1, \dots, n\}$ sea

$$T_i = \{j : y_j H \cap Hx_i \neq \emptyset\}.$$

Si $I \subseteq \{1, \dots, n\}$ es un subconjunto no vacío, sea $J = \cup_{i \in I} T_i$. Si $i \in I$ y $g \in Hx_i$, entonces $y \in y_j H$ para algún $j \in \{1, \dots, n\}$. En particular, $j \in A_i$ y además

$$\bigcup_{i \in I} Hx_i \subseteq \bigcup_{j \in J} y_j H.$$

Como las uniones son disjuntas, al tomar cardinalidad en esta última inclusión y observar que $|H| = |Hx_i| = |y_j H|$ para todo i, j , se concluye que $|I| \leq |J|$.

Por el teorema de Hall, existen elementos distintos $t_1 \in T_1, \dots, t_n \in T_n$ tales que $Hx_i \cap y_{t_i} H \neq \emptyset$. Para cada $i \in \{1, \dots, n\}$ sea $g_i \in Hx_i \cap y_{t_i} H$. Entonces g_1, \dots, g_n es un sistema completo de representantes de coclases de H a derecha y a izquierda. \square

Para poder demostrar el teorema de Weiss necesitamos unos resultados auxiliares sobre coclases dobles.

Lema 18.3. Sean G un grupo finito, H y K subgrupos de G del mismo índice y $x \in G$. Si $\alpha_1, \dots, \alpha_m$ es un sistema completo de representantes de $H/(xKx^{-1} \cap H)$, entonces

$$HxK = \bigcup_{i=1}^m \alpha_i xK \quad (\text{unión disjunta}). \quad (18.1) \quad \boxed{\text{eq:Weiss}}$$

En particular,

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|}.$$

Demostración. Sea $L = xKx^{-1} \cap H$. Primero observemos que la unión es disjunta. Si $\alpha_i xK = \alpha_j xK$, entonces

$$x^{-1} \alpha_j^{-1} \alpha_i x = (\alpha_j x)^{-1} (\alpha_i x) \in K.$$

Luego $\alpha_j^{-1} \alpha_i \in xKx \cap H = L$, es decir $\alpha_i L = \alpha_j L$, lo que implica $i = j$.

Veamos ahora que $HxK \subseteq \cup_{i=1}^m \alpha_i xK$, ya que la otra inclusión es trivial. Como $H = \cup_{i=1}^m \alpha_i L$, entonces

$$HxK \subseteq \bigcup_{i=1}^m \alpha_i LxK = \bigcup_{i=1}^m \alpha_i xK,$$

pues $LxK = xK$.

El tomar cardinalidad en (18.1) obtenemos $|HxK| = m|K|$. \square

Lema 18.4. Sean G un grupo finito y $x \in G$. Si H y K son subgrupos de G , entonces

$$\#\{yK : yK \subseteq HxK\} = (H : xKx^{-1} \cap H).$$

Demostración. Sea $L = xKx^{-1} \cap H$. Consideremos la función

$$\varphi : H/L \rightarrow \{yK : yK \subseteq HxK\}, \quad hL \mapsto hxK.$$

Veamos primero que φ está bien definida. Si $hL = h_1L$ para $h, h_1 \in H$, entonces $h_1^{-1}h \in L = xKx^{-1} \cap H$, es decir $h_1^{-1}h = xkx^{-1}$ para algún $k \in K$. Como entonces $(h_1x)^{-1}(hx) = x^{-1}h_1^{-1}hx \in K$, se concluye que $(hx)K = (h_1x)K$.

Claramente, φ es sobreyectiva, pues $hxK = \varphi(hL)$ para todo $h \in H$ y $k \in K$. Veamos entonces que φ es inyectiva. Si $hxK = h_1xK$, entonces $x^{-1}h_1^{-1}hx \in K$. Luego $h_1^{-1}h \in xKx^{-1} \cap H = L$, es decir $h_1L = hL$. \square

Análogamente puede demostrarse que bajo las hipótesis del lema, también se tiene que $\#\{Hz : Hz \subseteq HxK\} = (K : x^{-1}Hx \cap K)$.

Teorema 18.5 (Weiss). *Sea G un grupo finito y sean H y K subgrupos de G del mismo índice. Entonces existe un sistema común de representantes de coclases a izquierda de H en G y de coclases a derecha de K en G .*

Demostración. Primero observamos que las coclases Hy y zK tienen un representante en común si y sólo si $Hy \cap zK \neq \emptyset$ pues

$$Hx = Hy \text{ y } zK = xK \iff xy^{-1} \in H \text{ y } z^{-1}x \in K \iff x \in Hy \cap zK.$$

Sabemos que G es unión disjunta de (H, K) -coclases dobles.

Afirmación. Si

$$HxK = \bigcup_{i=1}^k Hy_i = \bigcup_{j=1}^l z_jK,$$

donde las uniones son disjuntas, entonces $k = l$ (pues H y K tienen el mismo orden) y para cada $i \in \{1, \dots, k\}$ se tiene que $Hy_i \cap z_jK \neq \emptyset$ para todo $j \in \{1, \dots, l\}$.

Fijemos $i_0 \in \{1, \dots, k\}$. Sin perder generalidad (reordenando, si fuera necesario) podemos suponer que $Hy_{i_0} \cap z_jK \neq \emptyset$ para todo $j \in \{1, \dots, m\}$. Como

$$Hy_{i_0} \subseteq \bigcup_{i=1}^k Hy_i = HxK = \bigcup_{j=1}^l z_jK,$$

entonces, en particular, $k = \#\{Hy_i : Hy_i \subseteq HxK\} = (H : xHx^{-1} \cap K)$. Como además $Hy_{i_0}K \subseteq \bigcup_{j=1}^m z_jK$, entonces

$$\frac{|H||K|}{|H \cap xKx^{-1}|} = |Hy_{i_0}K| \leq m|K|.$$

Luego se concluye que $k = m$, pues $k = (H : L) \leq m \leq k$. \square

Capítulo 19

Los teoremas de Hall y Wielandt

Definición 19.1. Sea p un número primo. Un p -grupo P se dice **elemental abeliano** si $x^p = 1$ para todo $x \in P$.

Definición 19.2. Un subgrupo M de G se dice **minimal-normal** si $M \neq 1$, M es normal en G y el único subgrupo normal de G contenido propiamente en M es el trivial.

Ejemplo 19.3. Si un subgrupo normal M es minimal (con respecto a la inclusión), entonces es minimal-normal. Sin embargo, la recíproca no es cierta. El subgrupo de \mathbb{A}_4 generado por $(12)(34)$, $(13)(24)$ y $(14)(23)$ es normal-minimal en \mathbb{A}_4 pero no es minimal.

Ejercicio 19.4. Demuestre que todo grupo finito contiene un subgrupo minimal-normal.

Ejemplo 19.5. Sea $G = \mathbb{D}_6 = \langle r, s : r^6 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diedral de doce elementos. Los subgrupos $S = \langle r^2 \rangle$ y $T = \langle r^3 \rangle$ son minimal-normales en G .

Ejemplo 19.6. Sea $G = \mathbf{SL}_2(3)$. No es difícil demostrar que el único subgrupo minimal-normal de G es el centro $Z(\mathbf{SL}_2(3)) \simeq C_2$:

```
gap> List(MinimalNormalSubgroups(SL(2,3)), \
StructureDescription);
[ "C2" ]
```

Un subgrupo H de G se dice **característico** si $f(H) \subseteq H$ para todo $f \in \text{Aut}(G)$. El centro y el conmutador de un grupo son ejemplos de subgrupos característicos. Es fácil demostrar que un subgrupo característico es normal.

Ejercicio 19.7. Si H es característico en K y K es normal en G , entonces H es normal en G .

El resultado que sigue es muy útil.

lemma:minimal_normal

Lema 19.8. Sea M un subgrupo minimal-normal de G . Si M es resoluble y finito entonces M es un p -grupo elemental abeliano para algún primo p .

Demostración. Como M es resoluble, $[M, M] \subsetneq M$. Además $[M, M]$ es normal en G pues $[M, M]$ es característico en M y M es normal en G . La minimal-normalidad del subgrupo M implica que $[M, M] = \{1\}$ y luego M es abeliano.

Si M es finito, existe un primo p tal que $1 \neq P = \{x \in M : x^p = 1\} \subseteq M$. Como P es característico en M , P es normal en G . Por minimalidad $P = M$. \square

Teorema 19.9. Sea G un grupo finito no trivial resoluble.

- 1) Todo subgrupo maximal tiene índice p^α para algún primo p .
- 2) Existe un primo p tal que G contiene un p -subgrupo minimal-normal.

Demostración. Para demostrar la primera afirmación procederemos por inducción en $|G|$. Si $|G|$ es una potencia de un primo no hay nada para demostrar. Supongamos entonces que $|G| \geq 6$ y sea M un subgrupo maximal de G . Sea N un subgrupo minimal-normal de G y sea $\pi: G \rightarrow G/N$ el morfismo canónico. Si $N = G$, entonces $N = G$ es un p -grupo y el resultado ya está demostrado. Supongamos entonces que $N \neq G$. Como $M \subseteq NM \subseteq G$, se tiene que $M = NM$ o bien $NM = G$ (por maximalidad de M). Si $M = NM \supseteq N$, entonces $\pi(M)$ es un subgrupo maximal de $\pi(G) = G/N$ y luego

$$(G : M) = (\pi(G) : \pi(M))$$

es una potencia de un primo por hipótesis inductiva. Si en cambio $NM = G$ entonces

$$(G : M) = \frac{|G|}{|M|} = \frac{|NM|}{|N|} = \frac{|N|}{|N \cap M|}$$

es una potencia de un primo pues N es un p -grupo por el lema anterior.

La demostración de la segunda afirmación queda como ejercicio \square

Ejemplo 19.10. Sea $G = \mathbb{S}_4$. El 2-subgrupo

$$K = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$$

es minimal-normal. Sin embargo, G no posee 3-subgrupos minimal-normales.

Teorema 19.11. Sea G un grupo finito no trivial. Entonces G es resoluble si y sólo si todo cociente no trivial de G contiene un subgrupo normal abeliano no trivial.

Demostración. Todo cociente de G es resoluble y por lo tanto contiene un subgrupo minimal-normal, que resulta abeliano. Para demostrar la recíproca procederemos por inducción en $|G|$. Sea N un subgrupo normal abeliano de G . Si $N = G$ entonces G es resoluble por ser abeliano. Si $N \neq G$, entonces $|G/N| < |G|$. Como todo cociente de G/N es un cociente de G , el grupo G/N satisface las hipótesis del teorema. Luego G/N es resoluble por hipótesis inductiva y entonces, como N y G/N son resolubles, G es resoluble. \square

Como aplicación del teorema 26.4 de Schur–Zassenhaus, en el capítulo ??, teorema 26.6, demostraremos que si G es un grupo finito resoluble no trivial y p es un primo que divide al orden de G , existe un subgrupo maximal de índice una potencia de p . Otra aplicación del teorema de Schur–Zassenhaus: la teoría de Hall, una generalización de la teoría de Sylow para grupos resolubles.

exercise:resoluble

Ejercicio 19.12. Sea G un grupo. Demuestre que G es resoluble si y sólo si existe una sucesión de subgrupos normales

$$\{1\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = G$$

tales que cada cociente N_i/N_{i-1} es abeliano.

lemma:Frattini_argument

Lema 19.13 (Argumento de Frattini). Sea G un grupo finito y sea K un subgrupo normal de G . Si $P \in \text{Syl}_p(K)$ para algún primo p , entonces $G = KN_G(P)$.

Demostración. Sea $g \in G$. Como $gPg^{-1} \subseteq gKg^{-1} = K$ pues K es normal en G y además $gPg^{-1} \in \text{Syl}_p(K)$, existe $k \in K$ tal que $kPk^{-1} = gPg^{-1}$. Luego $k^{-1}g \in N_G(P)$ pues $P = (k^{-1}g)P(k^{-1}g)^{-1}$. Tenemos entonces que $g = k(k^{-1}g) \in KN_G(P)$. \square

theorem:Hall

Teorema 19.14 (Hall). Sea G un grupo finito tal que todo subgrupo maximal de G tiene índice primo o el cuadrado de un primo. Entonces G es resoluble.

Demostración. Procederemos por inducción en $|G|$. Sea N un subgrupo minimal-normal de G y sea p el mayor divisor primo de $|N|$. Sean $P \in \text{Syl}_p(N)$ y $L = N_G(P)$. Si $L = G$ entonces P es normal en G y luego, como P y G/P son resolubles por hipótesis inductiva, G es resoluble. Supongamos entonces que $L \neq G$ y sea M un subgrupo maximal que contiene a L . Por el argumento de Frattini (lemma 19.13), $G = NL = NM$. Como M es maximal, existe un primo q tal que

$$(N : N \cap M) = (G : M) \in \{q, q^2\}$$

pues $(G : M) = |G|/|M| = |NM|/|M| = |N|/|N \cap M|$. Luego q divide a $|N|$ y entonces $q \leq p$; en particular $q \not\equiv 1 \pmod{p}$ (pues si $q \equiv 1 \pmod{p}$, entonces $q \mid p-1$ y luego $p \leq q-1 < q \leq p$, una contradicción). Si $g \in G$ entonces

$$gPg^{-1} \subseteq gNg^{-1} = N$$

y luego $gPg^{-1} \in \text{Syl}_p(N)$. Al hacer actuar a G por conjugación en $\text{Syl}_p(P)$, vemos que la cantidad de p -subgrupos de N es entonces igual a

$$(G : N_G(P)) = (G : L) \equiv 1 \pmod{p}.$$

Como $L \subseteq M$ se tiene que $L = N_M(P)$.

Como $P \subseteq M$, podemos hacer actuar a P en el conjunto $X = \{mPm^{-1} : m \in M\}$. Veamos que $\{P\}$ es la única órbita que contiene un único elemento. Si $\{P_1\}$ es una órbita con un único elemento, digamos $P_1 = mPm^{-1}$ para algún $m \in M$, entonces $P = m^{-1}P_1m = P_1$.

Descomponemos ahora al conjunto X como unión disjunta de órbitas

$$X = \{P\} \cup O(P_1) \cup \cdots \cup O(P_k),$$

donde $\{P\}$ es la única órbita que contiene solamente un elemento y cada $O(P_j)$ tiene cardinal divisible por p . Luego

$$(M : N_M(P)) = (M : L) = |X| \equiv 1 \pmod{p}.$$

De la igualdad $(G : L) = (G : M)(M : L)$ se concluye que $(G : M) \equiv 1 \pmod{p}$. Luego $(G : M) = q^2 \equiv 1 \pmod{p}$. Como esto implica que $q \equiv -1 \pmod{p}$, se concluye que $q = 2$ y $p = q + 1 = 3$.

Como $(N : N \cap M) = 4$, al hacer actuar a N en $N/N \cap M$ por multiplicación a izquierda tenemos un morfismo no trivial $\rho : N \rightarrow \mathbb{S}_4$. Como $[N, N]$ es característico en N y N es normal en G , por la minimal-normalidad del subgrupo N hay dos posibilidades: $[N, N] = \{1\}$ o bien $[N, N] = N$. Si $[N, N] = N$ entonces

$$\rho(N) = \rho([N, N]) = [\rho(N), \rho(N)].$$

Como \mathbb{S}_4 es resoluble, $\rho(N)$ es resoluble y luego $\rho(N) = \{1\}$, una contradicción. Luego $[N, N] = \{1\}$. Como N es resoluble por ser abeliano y G/N es resoluble por hipótesis inductiva, G es resoluble. \square

Para terminar esta sección veremos dos resultados que permiten detectar resolubilidad. Primero necesitamos un lema.

lemma:4Wielandt

Lema 19.15. Sea G un grupo finito. Sean H y K subgrupos de G de índices coprimos. Entonces $G = HK$ y $(H : H \cap K) = (G : K)$.

Demostración. Sea $D = H \cap K$. Como

$$(G : D) = \frac{|G|}{|H \cap K|} = (G : H)(H : H \cap K),$$

$(G : H)$ divide a $(G : D)$. Similarmente obtenemos que $(G : K)$ divide a $(G : D)$. Como $(G : H)$ y $(G : K)$ son coprimos, se concluye que $(G : H)(G : K)$ divide a $(G : D)$. En particular,

$$\frac{|G|}{|H|} \frac{|G|}{|K|} = (G : H)(G : K) \leq (G : D) = \frac{|G|}{|H \cap K|},$$

que implica $|G| = |HK|$. Como entonces $|G| = |HK| = |H||K|/|H \cap K|$, se concluye que $(G : K) = (H : H \cap K)$. \square

Recordemos que si H es un subgrupo de G , la **clausura normal** H^G de H en G se define como el subgrupo

$$H^G = \langle xHx^{-1} : x \in G \rangle.$$

Ejercicio 19.16. Sea G un grupo y H un subgrupo. Demuestre que H^G es normal en G y que H^G es el (único) menor subgrupo normal de G que contiene a H .

Ejemplo 19.17. Sea $G = \mathbb{A}_4$ y sea $H = \{\text{id}, (12)(34)\}$. La clausura normal de H en G es el grupo $H^G = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$. El código:

```
gap> G := AlternatingGroup(4);;
gap> NormalClosure(G, Subgroup(G, [(1,2)(3,4)]));
Group([(1,2)(3,4), (1,3)(2,4)])
gap> StructureDescription(last);
"C2 x C2"
```

theorem:Wielandt:solvable

Teorema 19.18 (Wielandt). Sea G un grupo finito y sean H, K, L subgrupos de G con índices coprimos dos a dos. Si H, K, L son resolubles, entonces G es resoluble.

Demostración. Podemos suponer que $G \neq \{1\}$. Procederemos por inducción en $|G|$. Sea N un subgrupo de G minimal-normal y sea $\pi: G \rightarrow G/N$ el morfismo canónico. Los subgrupos $\pi(H) = \pi(HN)$, $\pi(K) = \pi(KN)$, $\pi(L) = \pi(LN)$ de $\pi(G) = G/N$ son resolubles. Los índices de $\pi(H)$, $\pi(K)$ y $\pi(L)$ en $\pi(G)$ son coprimos dos a dos gracias al teorema de la correspondencia. Por hipótesis inductiva, $\pi(G)$ es resoluble. Si $H = \{1\}$ entonces $|G| = (G:H)$ es coprimo con $(G:K)$ y luego $G = K$ es resoluble. Si $H \neq \{1\}$ sea M un subgrupo minimal-normal de H . Por el lema 19.8, M es un p -grupo para algún primo p . Sin pérdida de generalidad podemos suponer que el primo p no divide a $(G:K)$ [pues si p divide a $(G:K)$ entonces p no divide a $(G:L)$ y solamente hay que cambiar a K por L]. Existe entonces $P \in \text{Syl}_p(G)$ tal que $P \subseteq K$. Como los subgrupos de Sylow son conjugados, existe $g \in G$ tal que $M \subseteq gKg^{-1}$. Como $(G:gKg^{-1}) = (G:K)$ es coprimo con $(G:H)$, el lema 19.15 implica que $G = (gKg^{-1})H$.

Veamos que todos los conjugados de M están en gKg^{-1} . Si $x \in G$ escribimos $x = uv$ con $u \in gKg^{-1}$, $v \in H$ y luego, como M es normal en H ,

$$xMx^{-1} = (uv)M(uv)^{-1} = uMu^{-1} \subseteq gKg^{-1}.$$

En particular, $\{1\} \neq M^G \subseteq gKg^{-1}$ es resoluble pues gKg^{-1} es resoluble. Como por hipótesis inductiva el cociente G/M^G es resoluble, se concluye que G es resoluble al aplicar el teorema 15.4. \square

Definición 19.19. Sea G un grupo finito de orden $p^\alpha m$ con p coprimo con m . Un subgrupo H de G se dice un p -complemento si $|H| = m$.

Ejemplo 19.20. Sea $G = \mathbb{S}_3$. El subgrupo $H = \langle (123) \rangle$ es un 2-complemento y el subgrupo $K = \langle (12) \rangle$ es un 3-complemento.

Recordemos que un teorema de Burnside afirma que todo grupo finito G de orden divisible por exactamente dos números primos es resoluble. Este resultado es necesario para demostrar el siguiente teorema de Hall:

theorem:Hall:solvable

Teorema 19.21 (Hall). Sea G un grupo finito tal que admite un p -complemento para todo primo que divide al orden de G . Entonces G es resoluble.

Demostración. Sea $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ con los p_j primos distintos. Procederemos por inducción en k . Si $k = 1$ el resultado es cierto pues G es un p -grupo. Si $k = 2$ el resultado es válido gracias al teorema de Burnside. Supongamos entonces que $k \geq 3$. Para cada $j \in \{1, 2, 3\}$ sea H_j un p_j -complemento en G . Como $|H_j| = |G|/p_j^{\alpha_j}$, los H_j tienen índices coprimos.

Veamos que H_1 es soluble. Observemos que $|H_1| = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Sea p un primo que divide a $|H_1|$ y sea Q un p -complemento en G . Como $(G : H_1)$ y $(G : Q)$ son coprimos, el lema 19.15 implica que

$$(H_1 : H_1 \cap Q) = (G : Q)$$

y luego $H_1 \cap Q$ es un p -complemento en H_1 . Luego H_1 es soluble por hipótesis inductiva. De la misma forma se demuestra que H_2 y H_3 son solubles.

Como H_1, H_2 y H_3 son solubles y tiene índices coprimos, el resultado se obtiene al aplicar el teorema de Wielandt. \square

Capítulo 20

Nilpotencia

Primero comenzaremos repasando algunas nociones básicas sobre conmutadores y subgrupos generados por conmutadores.

Si G es un grupo y $x, y, z \in G$, denotaremos la conjugación (como acción a izquierda) de la siguiente forma: ${}^x y = xyx^{-1}$. El conmutador entre x y y se escribirá entonces como

$$[x, y] = xyx^{-1}y^{-1} = ({}^x y)y^{-1}.$$

Además escribiremos $[x, y, z] = [x, [y, z]]$. Si X, Y, Z son subgrupos de G escribimos $[X, Y, Z] = [X, [Y, Z]]$. Observemos que $[X, Y] = [Y, X]$.

exercise:HallWitt

Ejercicio 20.1 (La identidad de Hall–Witt). Sean G un grupo y $x, y, z \in G$. Demuestre que

$$({}^y [x, y^{-1}, z]) ({}^z [y, z^{-1}, x]) ({}^x [z, x^{-1}, y]) = 1. \quad (20.1)$$

eq:HallWitt

Es interesante observar que si G es un grupo tal que $[G, G]$ es central, entonces la identidad de Hall–Witt se transforma en la identidad de Jacobi.

lemma:3subgrupos

Lema 20.2 (de los tres subgrupos de Hall). Sean X, Y, Z subgrupos de un grupo G tales que $[X, Y, Z] = [Y, Z, X] = \{1\}$. Entonces $[Z, X, Y] = \{1\}$.

Demostración. Alcanza con ver que $[z, x^{-1}, y] = 1$ para todo $x \in X, y \in Y, z \in Z$ (pues si $[x, y] \in C_G(z)$ entonces $[X, Y] \subseteq C_G(z)$). Como $[y^{-1}, z] \in [Y, Z]$, entonces $[x, y^{-1}, z] \in [X, Y, Z] = \{1\}$; luego ${}^y [x, y^{-1}, z] = 1$. Similarmente, ${}^z [y, z^{-1}, x] = 1$. Entonces, al usar la identidad de Hall–Witt, se concluye que $[z, x^{-1}, y] = 1$. \square

lemma:3subgrupos_general

Lema 20.3. Sea N un subgrupo normal de un grupo G y sean X, Y, Z subgrupos de G . Si $[X, Y, Z] \subseteq N$ y $[Y, Z, X] \subseteq N$. Entonces $[Z, X, Y] \subseteq N$.

Demostración. Sea $\pi: G \rightarrow G/N$ el morfismo canónico. Como $[X, Y, Z] \subseteq N$,

$$\begin{aligned} \{1\} &= \pi([X, Y, Z]) = \pi([X, [Y, Z]]) \\ &= [\pi(X), \pi([Y, Z])] = [\pi(X), [\pi(Y), \pi(Z)]] = [\pi(X), \pi(Y), \pi(Z)]. \end{aligned}$$

Similarmente $[\pi(Y), \pi(Z), \pi(X)] = \{1\}$. Entonces, gracias al lema de los tres subgrupos, $[\pi(Z), \pi(X), \pi(Y)] = \{1\}$, es decir $[Z, X, Y] \subseteq N$. \square

Definición 20.4. Sea G un grupo. La **serie central descendente** es la sucesión de subgrupos $\gamma_k(G)$ definida inductivamente como

$$\gamma_1(G) = G, \quad \gamma_{i+1}(G) = [G, \gamma_i(G)] \quad i \geq 1.$$

Definición 20.5. Un grupo G se dice **nilpotente** si existe c tal que $\gamma_{c+1}(G) = \{1\}$. El menor de los c tales que $\gamma_{c+1}(G) = \{1\}$ será el **índice (o clase) de nilpotencia** de G .

ca:nilpotente=>resoluble

Ejercicio 20.6. Demuestre que todo grupo nilpotente es resoluble.

Ejemplo 20.7. Un grupo es nilpotente de clase uno si y sólo si es abeliano.

Ejemplo 20.8. \mathbb{S}_3 es resoluble pues $\mathbb{S}_3 \supseteq \mathbb{A}_3 \supseteq \{1\}$ es una serie de composición con factores abelianos pero \mathbb{S}_3 no es nilpotente pues

$$\gamma_1(\mathbb{S}_3) = \mathbb{A}_3, \quad \gamma_2(\mathbb{S}_3) = [\mathbb{A}_3, \mathbb{S}_3] = \mathbb{A}_3.$$

Luego $\gamma_i(\mathbb{S}_3) \neq 1$ para todo $i \geq 1$.

Ejemplo 20.9. El grupo $G = \mathbb{A}_4$ no es nilpotente pues

$$\gamma_1(G) = G, \quad \gamma_j(G) = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$$

para todo $j \geq 2$. Podemos usar la función `LowerCentralSeries` para calcular la sucesión $\gamma_j(G)$:

```
gap> List(LowerCentralSeries(AlternatingGroup(4)), \
StructureDescription);
[ "A4", "C2 x C2" ]
```

Alternativamente, podemos calcular a mano la sucesión $\gamma_j(G)$:

```
gap> G := AlternatingGroup(4);;
gap> gamma_1 := G;;
gap> gamma_2 := DerivedSubgroup(G);;
gap> gamma_3 := CommutatorSubgroup(gamma_2, G);;
gap> StructureDescription(gamma_1);
"A4"
gap> StructureDescription(gamma_2);
"C2 x C2"
gap> StructureDescription(gamma_3);
"C2 x C2"
```

Ejemplo 20.10. El grupo $G = \text{SL}_2(3)$ no es nilpotente:

```
gap> IsNilpotent(SL(2, 3));
false
```

xca:gamma

Ejercicio 20.11. Sea G un grupo. Demuestre las siguientes afirmaciones:

- 1) Cada $\gamma_i(G)$ es un subgrupo característico de G .
- 2) $\gamma_i(G) \supseteq \gamma_{i+1}(G)$ para todo $i \geq 1$.
- 3) Si $f: G \rightarrow H$ es un morfismo sobreyectivo, $f(\gamma_i(G)) = \gamma_i(H)$ para todo $i \geq 1$.

xca:HxK_nilpotente

Ejercicio 20.12. Demuestre que si H y K son nilpotentes entonces $H \times K$ es nilpotente.

theorem:nilpotente

Teorema 20.13. Sea G un grupo nilpotente.

- 1) Si H es un subgrupo de G entonces H es nilpotente.
- 2) Si $f: G \rightarrow H$ es un morfismo sobreyectivo, entonces H es nilpotente.

Demostración. La primera afirmación es cierta pues $\gamma_i(H) \subseteq \gamma_i(G)$ para todo $i \geq 1$. La segunda afirmación: si existe c tal que $\gamma_{c+1}(G) = \{1\}$ entonces

$$\gamma_{c+1}(H) = f(\gamma_{c+1}(G)) = f(\{1\}) = \{1\}. \quad \square$$

Ejemplo 20.14. A diferencia de lo que pasa con grupos resolubles, podríamos tener un grupo G no nilpotente con un subgrupo normal K tal que K y G/K son nilpotentes. Por ejemplo: Sea $G = \mathbb{S}_3$ y sea $K = \mathbb{A}_3$. Entonces G no es nilpotente a pesar de que K y $G/K \simeq C_2$ sean nilpotentes.

sition:pgrupo_nilpotente

Proposición 20.15. Todo p -grupo finito es nilpotente.

Demostración. Procederemos por inducción en $|G|$. El caso $G = \{1\}$ es trivial. Si suponemos que el resultado es válido para p -grupos de orden $< |G|$, entonces, como G es un p -grupo, $Z(G) \neq \{1\}$. Esto implica que $G/Z(G)$ es un p -grupo nilpotente (por hipótesis inductiva) y luego existe c tal que $\gamma_{c+1}(G/Z(G)) = \{1\}$.

Sea $\pi: G \rightarrow G/Z(G)$ el morfismo canónico. Por el ejercicio ??,

$$\pi(\gamma_{c+1}(G)) = \gamma_{c+1}(G/Z(G)) = \{1\}$$

y entonces $\gamma_{c+1}(G) \subseteq \ker \pi = Z(G)$. Luego G es nilpotente pues

$$\gamma_{c+2}(G) = [\gamma_{c+1}(G), G] = [Z(G), G] = \{1\}. \quad \square$$

theorem:gamma

Teorema 20.16. Si G es un grupo, $[\gamma_i(G), \gamma_j(G)] \subseteq \gamma_{i+j}(G)$ para todo $i, j \geq 1$.

Demostración. Procederemos por inducción en j . El caso $j = 1$ es trivial pues $[G, \gamma_1(G)] = \gamma_{j+1}(G)$ por definición. Supongamos entonces que el resultado vale para algún $j \geq 1$ y para todo $i \geq 1$.

Primero observemos que

$$[G, \gamma_i(G), \gamma_j(G)] = [\gamma_i(G), G, \gamma_j(G)] = [\gamma_{i+1}(G), \gamma_j(G)] \subseteq \gamma_{i+j+1}(G)$$

por hipótesis inductiva. Además, también por hipótesis inductiva,

$$[\gamma_i(G), \gamma_j(G), G] \subseteq [\gamma_{i+j}(G), G] = \gamma_{i+j+1}(G).$$

El lema 20.3 implica entonces que $[\gamma_j(G), G, \gamma_i(G)] \subseteq \gamma_{i+j+1}(G)$. Luego

$$[\gamma_i(G), \gamma_{j+1}(G)] = [\gamma_{j+1}(G), \gamma_i(G)] = [\gamma_j(G), G, \gamma_i(G)] \subseteq \gamma_{i+j+1}(G). \quad \square$$

Podríamos considerar conmutadores arbitrarios donde no necesariamente se asocia siempre hacia la izquierda. Por ejemplo $[G, G, G] = [[G, G], G]$ y $[G, [G, G]]$ son ambos conmutadores de peso tres.

Corolario 20.17. *Sea G un grupo. Entonces todo conmutador de peso n está contenido en $\gamma_n(G)$.*

Demostración. Procederemos por inducción en n . El caso $n = 1$ es trivial. Supongamos entonces que el resultado es válido para algún $n \geq 1$. Tenemos entonces un conmutador de la forma $[A, B]$, donde A es un conmutador de peso k , B es un conmutador de peso l y $n + 1 = k + l$. Como $k < n$ y $l < n$, la hipótesis inductiva implica que $A \subseteq \gamma_k(G)$ y $B \subseteq \gamma_l(G)$. Luego $[A, B] \subseteq [\gamma_k(G), \gamma_l(G)] \subseteq \gamma_{k+l}(G)$ por el teorema anterior. \square

En el siguiente lema veremos que los grupos nilpotentes satisfacen la **condición normalizadora**.

lemma:normalizadora

Lema 20.18 (condición normalizadora). *Sea G un grupo nilpotente. Si H es un subgrupo propio de G entonces $H \subsetneq N_G(H)$.*

Demostración. Sabemos que existe c tal que $G = \gamma_1(G) \supseteq \cdots \supseteq \gamma_{c+1}(G) = \{1\}$. Como $\{1\} = \gamma_{c+1}(G) \subseteq H$ y $\gamma_1(G) \not\subseteq H$, sea el mínimo k tal que $\gamma_k(G) \subseteq H$. Como

$$[\gamma_{k-1}(G), H] \subseteq [\gamma_{k-1}(G), G] = \gamma_k(G) \subseteq H,$$

se tiene que $xHx^{-1} \subseteq H$ para todo $x \in \gamma_{k-1}(G)$, es decir $\gamma_{k-1}(G) \subseteq N_G(H)$. Si $N_G(H) = H$ entonces $\gamma_{k-1}(G) \subseteq H$, que contradice la minimalidad de k . \square

Si G es un grupo se define sucesión $\zeta_0(G), \zeta_1(G), \dots$ inductivamente de la siguiente forma:

$$\zeta_0(G) = \{1\}, \quad \zeta_{i+1}(G) = \{g \in G : [g, x] \in \zeta_i(G) \text{ para todo } x \in G\}, \quad i \geq 0.$$

Por ejemplo: $\zeta_1(G) = Z(G)$.

lemma:central_ascendente

Lema 20.19. *Sea G un grupo. Para todo $i \geq 0$ el conjunto $\zeta_i(G)$ es un subgrupo normal de G .*

Demostración. Procederemos por inducción en i . El caso $i = 0$ es trivial pues $\zeta_0(G) = 1$. Supongamos entonces que el resultado es válido para i . Veamos primero que $\zeta_{i+1}(G)$ es un subgrupo de G . Sean $g, h \in \zeta_{i+1}(G)$ y sea $x \in G$. Por hipótesis inductiva,

$$\begin{aligned} [g^{-1}, x] &= (xg^{-1})[g, x^{-1}](xg^{-1})^{-1} \in (xg^{-1})\zeta_i(G)(xg^{-1})^{-1} = \zeta_i(G), \\ [gh, x] &= [g, h]x[h^{-1}, x] \in \zeta_i(G). \end{aligned}$$

Como $1 \in \zeta_{i+1}(G)$, se concluye que todos los $\zeta_i(G)$ son subgrupos de G . La normalidad también se demuestra por inducción en i : si $g \in \zeta_{i+1}(G)$, $x \in G$ entonces $xgx^{-1} \in \zeta_{i+1}(G)$ pues

$$[xgx^{-1}, y] = x[g, x^{-1}yx]x^{-1} \in \zeta_i(G)$$

para todo $y \in G$. □

Definición 20.20. Sea G un grupo. Se define la **serie central ascendente** de G como la sucesión

$$1 = \zeta_0(G) \subseteq \zeta_1(G) \subseteq \zeta_2(G) \subseteq \cdots$$

Recordemos que un grupo G se dice **perfecto** si $[G, G] = G$.

theorem:Grun

Teorema 20.21 (Grün). Si G es un grupo perfecto, entonces $Z(G/Z(G)) = \{1\}$.

Demostración. Si usamos el lema de los tres subgrupos con $X = Y = G$ y $Z = \zeta_2(G)$, $\{1\} = [\zeta_2(G), G, G] = [\zeta_2(G), [G, G]] = [\zeta_2(G), G]$. Luego $\zeta_2(G) \subseteq Z(G)$ y entonces $\zeta_2(G) = Z(G/Z(G)) = \{1\}$. □

Si H y K son subgrupos de G se define

$$[H, K] = \langle [h, k] : h \in H, k \in K \rangle.$$

Sea G un grupo. Se dice que un subgrupo K de G **normaliza** a H si $K \subseteq N_G(H)$. Se dice que un subgrupo K de G **centraliza** a H si $K \subseteq C_G(H)$, es decir si y sólo si $[H, K] = \{1\}$.

Ejercicio 20.22. Sean K y H subgrupos de G con $K \subseteq H$ y K normal en G . Demuestre que $[H, G] \subseteq K$ si y sólo si $H/K \subseteq Z(G/K)$.

lemma:gamma_zeta

Lema 20.23. Sea G un grupo. Existe c tal que $\zeta_c(G) = G$ si y sólo si $\gamma_{c+1}(G) = \{1\}$. Más aún, en ese caso

$$\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$$

para todo $i \in \{0, 1, \dots, c\}$.

Demostración. Supongamos primero que $\zeta_c(G) = G$. Por inducción vamos a demostrar que $\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$. Como el caso $i = 0$ es trivial, supongamos que el resultado es válido para un cierto $i \geq 0$. Si $g \in \gamma_{i+2}(G) = [\gamma_{i+1}(G), G]$, podemos escribir

$$g = \prod_{k=1}^N [g_k, x_k],$$

donde $g_1, \dots, g_N \in \gamma_{i+1}(G)$ y $x_1, \dots, x_N \in G$. Por hipótesis inductiva

$$g_j \in \gamma_j(G) \subseteq \zeta_{c-j}(G)$$

y entonces $[g_j, x_j] \in \zeta_{c-i-1}(G)$ para todo j . Luego $g \in \zeta_{c-(i+1)}(G)$. La implicación que queremos queda demostrada al tomar $i = c$.

Supongamos ahora que $\gamma_{c+1}(G) = 1$. Demostremos por inducción en $c - i$ que $\gamma_{c+1-i}(G) \subseteq \zeta_{c-i}(G)$. El caso $c - i = 0$ es trivial. Si el resultado es válido para algún $c - i \geq 0$, sea $g \in \gamma_{c+2-i}(G) = [\gamma_{c+1-i}(G), G]$. Escribimos

$$g = \prod_{k=1}^N [g_k, x_k]$$

con $g_1, \dots, g_N \in \gamma_{c+1-i}(G) \subseteq \zeta_i(G)$ por hipótesis inductiva. Luego $g \in \zeta_{c-(i+1)}(G)$ pues cada $[g_j, x_j] \in \zeta_{i-1}(G)$. Al tomar $i = 0$ se obtiene la implicación buscada. \square

Ejemplo 20.24. Sea $G = \mathbb{S}_3$. Entonces $\zeta_j(G) = \{1\}$ para todo $j \geq 0$:

```
gap> UpperCentralSeries(SymmetricGroup(3));
[ Group(()) ]
```

Definición 20.25. Sea G un grupo. Una **serie central** para G es una sucesión

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \{1\}$$

de subgrupos normales de G tal que para cada $i \in \{1, \dots, n\}$, $\pi_i(G_{i-1})$ es un subgrupo de $Z(G/G_i)$, donde $\pi_i: G \rightarrow G/G_i$ es el morfismo canónico.

lemma:serie_central

Lema 20.26. Sea G un grupo y sea $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \{1\}$ una serie central para G . Entonces $\gamma_{i+1}(G) \subseteq G_i$ para todo i .

Demostración. Procederemos por inducción en i . El caso $i = 0$ es trivial. Supongamos que el resultado es válido para algún $i \geq 0$. Entonces

$$\gamma_{i+1}(G) = [G, \gamma_i(G)] \subseteq [G, G_{i-1}] \subseteq G_i$$

pues, como $\pi_i(G_{i-1}) \subseteq Z(G/G_i)$, entonces $\pi([G, G_{i-1}]) = [\pi(G), \pi(G_{i-1})] = \{1\}$ y luego $[G, G_{i-1}] \subseteq G_i$. \square

Teorema 20.27. Un grupo es nilpotente si y sólo si admite una serie central.

Demostración. Si el grupo G es nilpotente, entonces los $\gamma_j(G)$ forman una serie central para G . Recíprocamente, si $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \{1\}$ es una serie central para G , entonces, por el lema anterior, G es nilpotente pues

$$\gamma_{n+1}(G) \subseteq G_n = \{1\}. \quad \square$$

xca:nilpotente_central

Ejercicio 20.28. Sea G un grupo. Demuestre que si K es un subgrupo de $Z(G)$ tal que G/K es nilpotente, entonces G es nilpotente.

Teorema 20.29 (Hirsch). Sea G un grupo nilpotente. Si H es un subgrupo normal no trivial de G entonces $H \cap Z(G) \neq \{1\}$. En particular, $Z(G) \neq \{1\}$.

theorem:Z(nilpotent)

Demostración. Como $\zeta_0(G) = \{1\}$ y existe c tal que $\zeta_c(G) = G$, existe

$$m = \min\{k : H \cap \zeta_k(G) \neq \{1\}\}.$$

Como H es normal,

$$[H \cap \zeta_m(G), G] \subseteq H \cap [\zeta_m(G), G] \subseteq H \cap \zeta_{m-1}(G) = \{1\}.$$

Luego $\{1\} \neq H \cap \zeta_m(G) \subseteq H \cap Z(G)$. Si $H = G$ entonces $Z(G) \neq \{1\}$. \square

nilpotente_minimalnormal

Ejercicio 20.30. Sea G un grupo nilpotente y sea M un subgrupo minimal-normal de G . Demuestre que $M \subseteq Z(G)$.

Corolario 20.31. Sea G un grupo nilpotente no abeliano y sea A un subgrupo maximal-normal y abeliano de G . Entonces $A = C_G(A)$.

Demostración. Como A es abeliano, $A \subseteq C_G(A)$. Supongamos que $A \neq C_G(A)$. El centralizador $C_G(A)$ es normal en G pues, como A es normal en G ,

$$gC_G(A)g^{-1} = C_G(gAg^{-1}) = C_G(A).$$

para todo $g \in G$. Sea $\pi: G \rightarrow G/A$ el morfismo canónico. Entonces $\pi(C_G(A))$ es un subgrupo normal no trivial de $\pi(G)$. Como G es nilpotente, $\pi(G)$ es nilpotente y, por el teorema de Hirsch, $\pi(C_G(A)) \cap Z(\pi(G)) \neq \{1\}$. Sea $x \in C_G(A) \setminus A$ tal que $\pi(x)$ es central en $\pi(G)$. El grupo $\langle A, x \rangle$ es abeliano pues $x \in C_G(A)$. Además $\langle A, x \rangle$ es normal en G pues A es normal en G y si $g \in G$ entonces $gxg^{-1}x^{-1} \in A$ porque $\pi(x)$ es central y luego $gxg^{-1} \in \langle A, x \rangle$. Luego $A \subsetneq \langle A, x \rangle \subsetneq G$, una contradicción. \square

Teorema 20.32. Sea G un grupo nilpotente. Valen las siguientes afirmaciones:

- 1) Todo subgrupo minimal-normal tiene orden primo y es central.
- 2) Todo subgrupo maximal es normal de índice primo y contiene a $[G, G]$.

Demostración. Demostremos la primera afirmación. Sea N un subgrupo minimal-normal. Como $N \cap Z(G) \neq \{1\}$ por el teorema de Hirsch, $N \cap Z(G)$ es un subgrupo normal de G contenido en N . Luego $N = N \cap Z(G) \subseteq Z(G)$ por la minimalidad de N . En particular, N es abeliano. Además, como todo subgrupo de N es normal en G , N es simple y luego $N \simeq C_p$ para algún primo p .

Demostremos ahora la segunda afirmación. Si M es un subgrupo maximal, M es normal en G gracias a la condición normalizadora. La maximalidad de M implica que G/M no contiene subgrupos propios no triviales. Luego $G/M \simeq C_p$ para algún primo p . Como en particular G/M es abeliano, $[G, G] \subseteq M$. \square

Es importante remarcar que el teorema anterior no garantiza, por ejemplo, la existencia de subgrupos maximales. Recordemos que \mathbb{Q} es un grupo abeliano (por lo tanto, nilpotente) que no tiene subgrupos maximales.

proposition:g^n

Proposición 20.33. Sea G un grupo nilpotente y sea H un subgrupo de G de índice n . Si $g \in G$ entonces $g^n \in H$.

Demostración. El resultado es obvio en el caso en que H sea un subgrupo normal. Sea $H_0 = H$ y $H_{i+1} = N_G(H_i)$ para $i \geq 0$. Por definición, H_i es normal en H_{i+1} y además, como G es nilpotente, si $H_i \neq G$ entonces $H_i \subsetneq H_{i+1}$ por la condición normalizadora. Como $(G : H)$ es finito, existe k tal que $H_k = G$. Veamos que

$$g^{(G:H)} = g^{(H_k:H_{k-1})(H_{k-1}:H_{k-2})\cdots(H_1:H_0)} \in H.$$

Observemos que $g^{(H_k:H_{k-1})} \in H_{k-1}$ pues H_{k-1} es normal en $H_k = G$, y que, como $g^{(H_k:H_{k-1})} \in H_k$, entonces

$$g^{(H_k:H_{k-2})} = g^{(H_k:H_{k-1})(H_{k-1}:H_{k-2})} = \left(g^{(H_k:H_{k-1})}\right)^{(H_{k-1}:H_{k-2})} \in H_{k-2}$$

pues H_{k-2} es normal en H_{k-1} . Al repetir este argumento, $g^{(G:H)} \in H$. \square

Ejemplo 20.34. La proposición anterior no vale si el grupo G no es nilpotente. Sea $G = \mathbb{S}_3$ y sea $H = \{\text{id}, (12)\}$ de índice tres. Si $g = (13)$ entonces $g^3 = (13) \notin H$.

El lema que daremos a continuación es una herramienta útil para hacer demostraciones por inducción en grupos nilpotentes.

lemma : a [GG]

Lema 20.35. Sea G un grupo nilpotente de clase $c \geq 2$. Si $x \in G$ entonces el subgrupo $\langle x, [G, G] \rangle$ es nilpotente de clase $< c$.

Demostración. Sea $H = \langle x, [G, G] \rangle$. Si $x \in [G, G]$, el resultado es cierto. Supongamos entonces que $x \notin [G, G]$. Observemos que

$$H = \{x^n c : n \in \mathbb{Z}, c \in [G, G]\},$$

pues $[G, G]$ es normal en G . Para demostrar el lema alcanza entonces con probar que $[H, H] \subseteq \gamma_3(G)$. Sean $h = x^n c, k = x^m d \in H$ con $c, d \in [G, G]$. Como

$$[h, x^m] = [x^n, [c, x^m]][c, x^m] \in \gamma_4(G)\gamma_3(G) \subseteq \gamma_3(G),$$

entonces

$$\begin{aligned} [h, k] &= [h, x^m][x^m, [h, d]][h, d] \\ &= [x^n, [c, x^m]][c, x^m][x^m, [h, d]][h, d] \in \gamma_3(G). \end{aligned} \quad \square$$

Veamos un ejemplo, está hecho con la computadora.

Ejemplo 20.36. Sea $G = \mathbb{D}_8 = \langle r, s : r^8 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diedral de orden 16. El grupo G es nilpotente de clase tres y $[G, G] = \{1, r^2, r^4, r^6\} \simeq C_4$. El subgrupo $\langle s, [G, G] \rangle \simeq \mathbb{D}_4$ es nilpotente de clase dos.

```
gap> G := DihedralGroup(IsPermGroup, 16); ;
gap> gens := GeneratorsOfGroup(G); ;
gap> r := gens[1]; ;
gap> s := gens[2]; ;
```



```

gap> D := DerivedSubgroup(G);;
gap> S := Subgroup(G, Concatenation(Elements(D), [s]));;
gap> StructureDescription(S);
"D8"
gap> NilpotencyClassOfGroup(G);
3
gap> NilpotencyClassOfGroup(S);
2

```

Ahora una aplicación del lema.

theorem:T(nilpotent)

Teorema 20.37. Si G es un grupo nilpotente, entonces

$$T(G) = \{g \in G : g^n = 1 \text{ para algún } n \in \mathbb{N}\}$$

es un subgrupo de G .

Demostración. Sean $a, b \in T(G)$ y sean

$$A = \langle a, [G, G] \rangle, \quad B = \langle b, [G, G] \rangle.$$

Como A y B son nilpotentes por el lema anterior, por hipótesis inductiva, $T(A)$ es un subgrupo de A y $T(B)$ es un subgrupo de B . Como $T(A)$ es característico en A y A es normal en G , $T(A)$ es normal en G . Similarmente se demuestra que $T(B)$ es normal en B . Veamos ahora que todo elemento de $T(A)T(B)$ tiene orden finito: si $x \in T(A)T(B)$, digamos $x = a_1 b_1$ con a_1 de orden m , entonces x tiene orden finito pues

$$x^m = (a_1 b_1)^m = (a_1 b_1 a_1^{-1})(a_1^2 b_1 a_1^{-2}) \cdots (a_1^{m-1} b_1 a_1^{-m+1}) b_1 \in T(B).$$

Para entender mejor el truco hagamos un caso concreto, digamos $m = 3$. La fórmula en este caso queda así:

$$\begin{aligned} (a_1 b_1)^3 &= (a_1 b_1)(a_1 b_1)(a_1 b_1) \\ &= (a_1 b_1 a_1^{-1})(a_1^2 b_1 a_1^{-2}) a_1^3 b_1 = (a_1 b_1 a_1^{-1})(a_1^2 b_1 a_1^{-2}) b_1, \end{aligned}$$

pues $a_1^3 = 1$.

El truco nos permite entonces demostrar que ab y a^{-1} tienen ambos orden finito. Luego $T(G)$ es un subgrupo de G . \square

Otra aplicación.

theorem:a=b

Teorema 20.38. Sea G un grupo nilpotente y sin torsión y sean $a, b \in G$. Si existe $n \neq 0$ tal que $a^n = b^n$ entonces $a = b$.

Demostración. Procederemos por inducción en el orden de nilpotencia c de G . El resultado es trivialmente cierto si G es abeliano. Supongamos entonces que G es nilpotente de índice $c \geq 1$. Como $\langle a, [G, G] \rangle$ es un subgrupo de G nilpotente de índice $< c$, y $bab^{-1} = [b, a]a \in \langle a, [G, G] \rangle$, por hipótesis inductiva, $ba = ab$ pues

$$a^n = (bab^{-1})^n = b^n.$$

Luego $(ab^{-1})^n = a^n b^{-n} = 1$ y por lo tanto, como G no tiene torsión, se concluye que $a = b$. \square

Corolario 20.39. *Sea G un grupo nilpotente sin torsión. Sean $x, y \in G$ tales que $x^n y^m = y^m x^n$ para algún $n, m \neq 0$, entonces $xy = yx$.*

Demostración. Sean $a = x$ y $b = y^n x y^{-n}$. Como $a^m = b^m$, el teorema anterior implica que $a = b$ y luego $xy^n = y^n x$. Al usar nuevamente ese teorema, esta vez con $a = y$ y $b = xyx^{-1}$, se concluye que $xy = yx$. \square

lemma:fg

Lema 20.40. *Sea G un grupo finitamente generado y sea H un subgrupo de índice finito. Entonces H es finitamente generado.*

Demostración. Supongamos que G está generado por $\{g_1, \dots, g_m\}$. Podemos suponer, sin pérdida de generalidad, que para cada i existe k tal que $g_i^{-1} = g_k$.

Sea $\{1 = t_1, \dots, t_n\}$ un transversal de H en G , es decir un conjunto de representantes de G/H . Para $i \in \{1, \dots, n\}$, $j \in \{1, \dots, m\}$, escribimos

$$t_i g_j = h(i, j) t_{k(i, j)}.$$

Vamos a demostrar que H está generado por los $h(i, j)$. Sea $x \in H$. Escribamos

$$\begin{aligned} x &= g_{i_1} \cdots g_{i_s} \\ &= (t_1 g_{i_1}) g_{i_2} \cdots g_{i_s} \\ &= h(1, i_1) t_{k_1} g_{i_2} \cdots g_{i_s} \\ &= h(1, i_1) h(k_1, i_2) t_{k_2} g_{i_3} \cdots g_{i_s} \\ &= h(1, i_1) h(k_1, i_2) \cdots h(k_{s-1}, i_s) t_{k_s}, \end{aligned}$$

donde $k_1, \dots, k_{s-1} \in \{1, \dots, n\}$. Como $t_{k_s} \in H$ pues $x \in H$, entonces $t_{k_s} = 1 \in H$ y luego x está generado por los $h(i, j)$. \square

theorem:T(G) finito

Teorema 20.41. *Sea G un grupo finitamente generado, de torsión y nilpotente. Entonces G es finito.*

Demostración. Procederemos por inducción en la clase de nilpotencia c . El caso $c = 1$ es verdadero pues G es abeliano. Supongamos entonces que el resultado es válido para $c \geq 1$. Como $[G, G]$ y $G/[G, G]$ son nilpotentes de clase $< c$, finitamente generados por el lema anterior y de torsión, por hipótesis inductiva se tiene que $[G, G]$ y $G/[G, G]$ son finitos. Luego G es también finito, de hecho puede probarse que G es de orden $|[G, G]|(G : [G, G])$. \square

El siguiente lema también resultará muy útil, especialmente en caso de trabajar con grupos finitos nilpotentes.

lemma:normalizador

Lema 20.42. *Sean G un grupo finito, p un primo que divide a $|G|$ y $P \in \text{Syl}_p(G)$. Entonces*

$$N_G(N_G(P)) = N_G(P).$$

Demostración. Sea $H = N_G(P)$. Como P es normal en H , P es el único p -subgrupo de Sylow de H . Para ver que $N_G(H) = H$ basta demostrar que $N_G(H) \subseteq H$. Sea $g \in N_G(H)$. Como

$$gPg^{-1} \subseteq gHg^{-1} = H,$$

$gPg^{-1} \in \text{Syl}_p(H)$ y H tiene un único p -subgrupo de Sylow, $P = gPg^{-1}$. Luego $g \in N_G(P) = H$. \square

theorem:nilpotente:eq

Teorema 20.43. Sea G un grupo finito. Son equivalentes:

- 1) G es nilpotente.
- 2) Todo subgrupo de Sylow de G es normal.
- 3) G es producto directo de sus subgrupos de Sylow.

Demostración. Veamos que (1) \implies (2). Sea $P \in \text{Syl}_p(G)$. Queremos ver que P es normal en G , es decir $N_G(P) = G$. Por el lema anterior, $N_G(N_G(P)) = N_G(P)$. La condición normalizadora implica entonces que $N_G(P) = G$.

Veamos ahora que (2) \implies (3). Sean p_1, \dots, p_k los factores primos de $|G|$ y para cada $i \in \{1, \dots, k\}$ sea $P_i \in \text{Syl}_{p_i}(G)$. Por hipótesis, cada P_j es normal en G .

Vamos a demostrar que $P_1 \cdots P_j \simeq P_1 \times \cdots \times P_j$ para todo j . El caso $j = 1$ es trivial. Supongamos entonces que el resultado vale para algún $j \geq 1$. Como

$$N = P_1 \cdots P_j \simeq P_1 \times \cdots \times P_j$$

es normal en G y tiene orden coprimo con $|P_{j+1}|$, $N \cap P_{j+1} = \{1\}$. Luego

$$NP_{j+1} \simeq N \times P_{j+1} \simeq P_1 \times \cdots \times P_j \times P_{j+1}$$

pues P_{j+1} es también normal en G .

Ahora que sabemos que $P_1 \cdots P_k \simeq P_1 \times \cdots \times P_k$ es un subgrupo de orden $|G|$, se concluye que $G = P_1 \times \cdots \times P_k$.

Para ver que (3) \implies (1) simplemente hace falta observar que todo p -grupo es nilpotente (proposición 20.15) y que el producto directo de finitos nilpotentes es nilpotente. \square

xca:truco

Ejercicio 20.44. Sea G un grupo finito. Demuestre que si $P \in \text{Syl}_p(G)$ y M es un subgrupo de G tal que $N_G(P) \subseteq M$ entonces $M = N_G(M)$.

xca:normalizadora

Ejercicio 20.45. Sea G un grupo finito. Son equivalentes:

- 1) G es nilpotente.
- 2) Si $H \subsetneq G$ es un subgrupo entonces $H \subsetneq N_G(H)$.
- 3) Todo subgrupo maximal de G es normal en G .

Teorema 20.46. Sea G un grupo finito nilpotente. Si p es un primo que divide al orden de G , existe un subgrupo minimal-normal de orden p y existe un subgrupo maximal de índice p .

Demostración. Supongamos que $|G| = p^\alpha m$, donde p es un primo coprimo con m . Escribamos $G = P \times H$, donde $P \in \text{Syl}_p(G)$. Como $Z(P)$ es un subgrupo normal no trivial de P , todo subgrupo de $Z(P)$ minimal-normal en G tiene orden p (y esos subgrupos existen porque G es un grupo finito). Por otro lado, como P contiene un subgrupo de índice p , que resulta maximal. Luego $P \times H$ también contiene un subgrupo maximal de índice p . \square

xca:pgrupos

Ejercicio 20.47. Sea p un primo y sea G un grupo no trivial de orden p^n . Demuestre las siguientes afirmaciones:

- 1) G tiene un subgrupo normal de orden p .
- 2) Para todo $j \in \{0, \dots, n\}$ existe un subgrupo normal de G de orden p^j .

:nilpotente_equivalencia

Ejercicio 20.48. Sea G un grupo finito. Demuestre que las siguientes afirmaciones son equivalentes:

- 1) G es nilpotente.
- 2) Cualesquiera dos elementos de órdenes coprimos conmutan.
- 3) Todo cociente no trivial de G tiene centro no trivial.
- 4) Si d divide al orden de G , existe un subgrupo normal de G de orden d .

El siguiente resultado, que puede demostrarse en forma completamente elemental, fue descubierto en 2014.

Teorema 20.49 (Baumslag–Wiegold). Sea G un grupo finito tal que $|xy| = |x||y|$ si x e y son elementos de órdenes coprimos. Entonces G es nilpotente.

Demostración. Sean p_1, \dots, p_n los distintos primos que dividen al orden de G . Para cada $i \in \{1, \dots, n\}$ sea $P_i \in \text{Syl}_{p_i}(G)$. Primero vamos a demostrar que $G = P_1 \cdots P_n$. La inclusión no trivial equivale a demostrar que la función

$$\psi: P_1 \times \cdots \times P_n \rightarrow G, \quad (x_1, \dots, x_n) \mapsto x_1 \cdots x_n$$

es sobreyectiva. Procederemos de la siguiente forma. Primero vemos que la función ψ es inyectiva. En efecto, si $\psi(x_1, \dots, x_n) = \psi(y_1, \dots, y_n)$, entonces

$$x_1 \cdots x_n = y_1 \cdots y_n.$$

Si $y_n \neq x_n$, entonces $x_1 \cdots x_{n-1} = (y_1 \cdots y_{n-1})y_n x_n^{-1}$. Pero $x_1 \cdots x_{n-1}$ es un elemento de orden coprimo con p_n y $y_1 \cdots y_{n-1}y_n x_n^{-1}$ es un elemento de orden múltiplo de p_n , una contradicción. Entonces $x_n = y_n$ y luego, el mismo argumento, prueba que ψ es inyectiva. Como $|P_1 \times \cdots \times P_n| = |G|$, se concluye que ψ es biyectiva. En particular, ψ es sobreyectiva y luego $G = P_1 \cdots P_n$.

Veamos ahora que cada P_j es normal en G . Sea $j \in \{1, \dots, n\}$ y sea $x_j \in P_j$. Sea $g \in G$ y sea $y_j = gx_jg^{-1}$. Como $y_j \in G$, podemos escribir $y_j = z_1 \cdots z_n$ con $z_k \in P_k$ para todo k . Como el orden de y_j es una potencia del primo p_j , el elemento $z_1 \cdots z_n$ tiene orden una potencia de p_j y luego $z_k = 1$ para todo $k \neq j$ y además $y_j = z_j \in P_j$. Como cada subgrupo de Sylow es normal en G , se concluye que G es nilpotente. \square

lemma:commutador

Lema 20.50. Si $x, y \in G$ son tales que $[x, y] \in C_G(x) \cap C_G(y)$, entonces

$$[x, y]^n = [x^n, y] = [x, y^n]$$

para todo $n \in \mathbb{Z}$.

Demostración. Procederemos por inducción en $n \geq 0$. El caso $n = 0$ es trivial. Supongamos entonces que el resultado vale para algún $n \geq 0$. Entonces, como $[x, y] \in C_G(x)$,

$$[x, y]^{n+1} = [x, y]^n [x, y] = [x^n, y] [x, y] = [x^n, y] x y x^{-1} y^{-1} = x [x^n, y] y x^{-1} y^{-1} = [x^{n+1}, y].$$

Para demostrar el lema en el caso $n < 0$ basta observar que, como $[x, y]^{-1} = [x^{-1}, y]$, $[x, y]^{-n} = [x^{-1}, y]^n = [x^{-n}, y]$. \square

lemma:Hall

Lema 20.51 (Hall). Sea G un grupo nilpotente de clase dos y $x, y \in G$. Entonces

$$(xy)^n = [y, x]^{n(n-1)/2} x^n y^n$$

para todo $n \in \mathbb{N}$.

Demostración. Procederemos por inducción en n . Como el caso $n = 1$ es trivial, supongamos que el resultado es válido para algún $n \geq 1$. Entonces, gracias al lema anterior,

$$\begin{aligned} (xy)^{n+1} &= (xy)^n (xy) = [y, x]^{n(n-1)/2} x^n y^{n-1} (yx) y \\ &= [y, x]^{n(n-1)/2} x^n [y^n, x] x y^{n+1} = [y, x]^{n(n-1)/2} [y, x]^n x^{n+1} y^{n+1}. \end{aligned} \quad \square$$

lemma:class2

Lema 20.52. Sea $p > 2$ un número primo y sea P un p -grupo de clase de nilpotencia ≤ 2 . Si $[y, x]^p = 1$ para todo $x, y \in P$ entonces $P \rightarrow [P, P]$, $x \mapsto x^p$, es un morfismo de grupos.

Demostración. Por lema de Hall, $(xy)^p = [y, x]^{p(p-1)/2} x^p y^p = x^p y^p$. \square

thm:class2

Teorema 20.53. Sea $p > 2$ un número primo y sea P un p -grupo de clase de nilpotencia ≤ 2 . Entonces $\{x \in P : x^p = 1\}$ es un subgrupo de P .

Demostración. Como P tiene clase de nilpotencia dos, los conmutadores son centrales. Para cada $x \in G$, la función $g \mapsto [g, x]$ es un morfismo de grupos pues

$$[gh, x] = ghxh^{-1}g^{-1}x^{-1} = g[h, x]xg^{-1}x^{-1} = [g, x][h, x].$$

En particular, si $x, y \in P$ con $x^p = y^p = 1$, entonces

$$[x, y]^p = [x^p, y] = [1, y] = 1.$$

Luego, al usar el lema de Hall, se concluye que $(xy)^p = [y, x]^{p(p-1)/2} x^p y^p = 1$. \square

Capítulo 21

La cantidad de grupos finitos

En este capítulo mencionaremos algunos problemas y algunos resultados relacionados con la cantidad de clases de isomorfismo de grupos finitos de un orden dado. Este problema de clasificación es obviamente casi tan antiguo como la teoría de grupos. Al dar los primeros pasos en teoría de grupos nos encontramos con algunos resultados fáciles de demostrar:

- Existe un único grupo finito de orden primo y es cíclico.
- Existen dos grupos de orden cuatro, ambos abelianos.
- Existen dos grupos de orden seis, uno de ellos es no abeliano.
- Los grupos de orden p^2 son abelianos.

Con los teoremas de Sylow se puede ir un poco más lejos. Es fácil demostrar, por ejemplo, que existe un único grupo de orden 15 y es cíclico. El mismo resultado puede demostrarse para otros órdenes, por ejemplo 455 y 615.

Una pregunta surge naturalmente. ¿Para qué valores de n existe un único grupo (que obviamente resultará isomorfo a C_n) de orden n ? La respuesta fue dada por Burnside.

Definición 21.1. Un número $n \in \mathbb{N}$ se dice **cíclico** si C_n es el único grupo (salvo isomorfismo) de orden n .

Algunos ejemplos de números cíclicos: 2, 3, 15 y $615 = 3 \cdot 5 \cdot 41$.

Teorema 21.2 (Burnside). Sea $n \in \mathbb{N}$. Entonces n es cíclico si y sólo si n y $\phi(n)$ son coprimos.

Demostración. Supongamos que n es cíclico. Sin perder generalidad podemos suponer que n es libre de cuadrados (pues de lo contrario, si $n = p^a m$ con $m \in \mathbb{N}$, p primo tal que $\text{mcd}(p, m) = 1$ y $a \geq 2$, el grupo $C_m \times C_p^a$ tiene orden n y no es cíclico). Escribimos entonces

$$n = p_1 \cdots p_k$$

con los p_j primos distintos y $\phi(n) = (p_1 - 1) \cdots (p_k - 1)$. Si $\text{mcd}(n, \phi(n)) \neq 1$, existen primos distintos p y q tales que p divide a $q - 1$. El grupo $G = C_m \times (C_p \rtimes C_q)$ tiene orden $n = pqm$ y no es cíclico.

Supongamos que $\text{mcd}(n, \phi(n)) = 1$ y que n no es cíclico. Sea G un grupo de mínimo orden n no cíclico.

Si perder generalidad podemos suponer que n es libre de cuadrados: si $n = p^\alpha m$, p primo, $m \in \mathbb{N}$ coprimo con p y $\alpha \geq 2$, entonces, como $\phi(n) = p^{\alpha-1}(p-1)\phi(m)$, tendríamos que p divide a $\text{mcd}(n, \phi(n))$. Luego

$$n = p_1 \cdots p_k,$$

con los p_j primos distintos.

Afirmación. Todo subgrupo de G y todo cociente de G es cíclico.

Si m divide a n entonces $\text{mcd}(m, \phi(m)) = 1$ pues n y $\phi(n) = (p_1 - 1) \cdots (p_k - 1)$ son coprimos. Luego todo subgrupo y todo cociente propio es cíclico por la minimalidad de n .

Afirmación. $Z(G) = \{1\}$.

Para cada $i \in \{1, \dots, k\}$ sea $x_i \in G$ un elemento de orden p_i . Si G fuera abeliano, G sería cíclico: $x_1 \cdots x_k$ sería un elemento de orden n . Luego $Z(G) \neq G$. Ahora bien, si $1 < |Z(G)| < n$, entonces $G/Z(G)$ sería cíclico (pues todo cociente de G lo es) y luego G sería abeliano.

Afirmación. Si M es un subgrupo maximal de G y $x \in M \setminus \{1\}$, entonces $M = C_G(x)$. En particular, si M y N son subgrupos maximales distintos, entonces $M \cap N = \{1\}$.

Como $Z(G) \neq \{1\}$, $C_G(x) \neq G$. Y como M es cíclico, $M \subseteq C_G(x)$. Luego, por maximalidad, $M = C_G(x)$. Si M y N son dos subgrupos maximales y $x \in M \cap N \setminus \{1\}$, entonces $M = N = C_G(x)$.

Afirmación. Si M es un subgrupo maximal, $M = N_G(M)$.

Sea $x \in N_G(M) \setminus \{1\}$ y sea $\alpha \in \text{Aut}(M)$ dado por $y \mapsto xyx^{-1}$. Como M es cíclico, si $m = |M|$ entonces $|\text{Aut}(M)|$ tiene orden $\phi(m)$. Por otro lado, como $|x|$ divide a n , $|\alpha|$ divide a n . Luego $|\alpha|$ divide a $\text{mcd}(n, \phi(m)) = 1$. Esto significa que $x \in C_G(M)$, es decir: $N_G(M) \subseteq C_G(M)$. Como

$$M \subseteq N_G(M) \subseteq C_G(M)$$

M es maximal y $Z(G) \neq \{1\}$, obtenemos que $M = N_G(M) = C_G(M)$.

Sean M_1, \dots, M_l los representantes de las clases de conjugación de subgrupos maximales de G . Para cada $j \in \{1, \dots, l\}$ sea $m_j = |M_j|$. Como $M_j = N_G(M_j)$ para cada j , la órbita de M_j tiene n/m_j elementos.

Como para cada $g \in G \setminus \{1\}$ existe un único subgrupo maximal M tal que $g \in M$,

$$n = 1 + \sum_{j=1}^l \frac{n}{m_j} (m_j - 1). \quad (21.1) \quad \boxed{\text{eq:particion}}$$

Si $l = 1$ entonces $n = m_1$, una contradicción. Si $l > 1$ entonces, como para cada j se tiene que $m_j \geq 2$, al reescribir (21.1), tenemos

$$\frac{1}{n} + l - 1 = \sum_{j=1}^l \frac{1}{m_j} \leq \frac{l}{2}.$$

De esta desigualdad obtenemos $nl \leq 2n - 2 < 2n$ y entonces $l < 2$, absurdo. \square

Análogamente pueden definirse números abelianos y nilpotentes. Estos números están clasificados y una demostración elemental puede consultarse en [28]. También existe la noción de número resoluble. Gracias al teorema de Feit–Thompson todo número impar es un número resoluble. Estos números también están clasificados, aunque la demostración es bastante más difícil ya que depende de un teorema muy profundo de Thompson y del famoso teorema de Feit–Thompson.

En [6] se define la función $\text{gnu}(n)$, que devuelve la cantidad de clases de isomorfismo de grupos de orden n . Por ejemplo, $\text{gnu}(1) = \text{gnu}(2) = \text{gnu}(3) = \text{gnu}(5) = 1$ y $\text{gnu}(4) = \text{gnu}(6) = 2$. El nombre viene de *groups number*.

El teorema de Burnside puede reformularse así:

$$\text{gnu}(n) = 1 \iff n \text{ es cíclico} \iff \text{mcd}(n, \phi(n)) = 1.$$

En [6] Conway, Dietrich y O’Brien caracterizaron los $n \in \mathbb{N}$ tales que $\text{gnu}(n) = 2$, $\text{gnu}(n) = 3$, $\text{gnu}(n) = 4$.

En la enciclopedia de sucesiones, la sucesión

$$\text{gnu}(1), \text{gnu}(2), \text{gnu}(3), \text{gnu}(4) \dots$$

es A000001, ver <http://oeis.org/A000001> para más información.

GAP contiene una base de datos con todos los grupos de orden ≤ 2000 , excepto los grupos de orden 1024. La base de datos contiene además otros grupos, por ejemplo aquellos de orden p^n para todo número primo p y todo $n \leq 6$. La base de datos fue escrita por Besche, Eick y O’Brien y hoy en día es una herramienta fundamental en teoría de grupos [4]. En particular, esta base de datos nos permite calcular fácilmente algunos valores de la función gnu .

La función `NrSmallGroups` devuelve la cantidad de clases de isomorfismo de grupos de un cierto orden. Definimos entonces la función gnu y calculamos algunos ejemplos:

```
gap> gnu := NrSmallGroups;;
gap> gnu(16);
14
gap> gnu(32);
51
gap> gnu(64);
267
gap> gnu(27);
5
gap> gnu(81);
```

```

15
gap> gnu(128);
2328
gap> gnu(512);
10494213

```

Se sabe que $\text{gnu}(1024) = 49487365422$, aunque este valor no puede obtenerse con **GAP** ya que, para ahorrar memoria, la base de datos no incluye la inmensa lista de grupos de orden 1024. Los grupos de orden 1024 fueron clasificados por Besche, Eick y O'Brien, el anuncio fue hecho en [3].

Más del 99 % de los grupos de orden < 2000 es de orden 1024. De hecho, como vimos, hay 49487365422 grupos de orden 1024 y la cantidad de clases de isomorfismo de grupos de orden $n \neq 1024$ con $n < 2016$ es 423164131.

```

gap> Sum([1..1023], gnu)+Sum(List([1025..2015], gnu));
423164131

```

Estos números nos dan aproximadamente 99,15 %.

Estas observaciones sugieren naturalmente la siguiente conjetura, que parece ser parte del folclore matemático:

Conjetura 21.3. Casi todo grupo finito es un 2-grupo.

La numerología que hicimos nos permite evitar tener que hacer precisiones sobre qué significa «casi todo grupo finito». Problemas similares aparecen en el capítulo 22 del libro [5].

Problema 21.1. Calcular $\text{gnu}(2048)$.

Se sabe que $\text{gnu}(2048) > 1774274116992170$, que es la cantidad de subgrupos de orden 2048 de una cierta clase.

Conjetura 21.4. Sea $n \in \mathbb{N}$. La sucesión

$$\text{gnu}(n), \text{gnu}^2(n) = \text{gnu}(\text{gnu}(n)), \text{gnu}^3(n) \dots$$

se estabiliza en 1.

No es difícil verificar que la conjetura es verdadera para $n < 2000$.

La siguiente conjetura apareció en forma independiente en varios lugares. Aparentemente la primera aparición más o menos explícita fue alrededor de 1930 y se debe Miller. Independientemente MacHale la formuló cuarenta años más tarde.

Conjetura 21.5. La función $\mathbb{N} \rightarrow \mathbb{N}$, $n \mapsto \text{gnu}(n)$ es sobreyectiva.

Para más información sobre esta conjetura referimos a [5, §21.6].

Si bien hay muchas conjeturas sobre el comportamiento de la función que cuenta la cantidad de clases de isomorfismos de grupos finitos, existen varios resultados. El siguiente es completamente elemental:

Teorema 21.6. Si $n \in \mathbb{N}$, entonces $\text{gnu}(n) \leq n^{n \log_2 n}$.

Demostración. Si G es un grupo, sea

$$d(G) = \min\{k : \text{existen } g_1, \dots, g_k \in G \text{ tales que } G = \langle g_1, \dots, g_k \rangle\}.$$

Vamos a demostrar que si $|G| = n$, entonces $d(G) \leq \log n$. Sea

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \dots \subsetneq G_r = G$$

una sucesión maximal de subgrupos. Para cada $i \in \{1, \dots, r\}$ sea $g_i \in G_i \setminus G_{i-1}$. Se demuestra fácilmente que

$$G_i = \langle g_1, \dots, g_i \rangle$$

para todo i . En efecto, si existe algún i tal que $G_i \neq \langle g_1, \dots, g_i \rangle$, entonces existe $g \in G_i \setminus \langle g_1, \dots, g_i \rangle$ y luego

$$\langle g_1, \dots, g_i \rangle \subsetneq \langle G_i, g \rangle \subsetneq G_{i+1}$$

lo que contradice la maximalidad de la sucesión de subgrupos. En particular, G está generado por r elementos.

Por el teorema de Lagrange,

$$n = |G| = \prod_{i=1}^r (G_i : G_{i-1}) \geq 2^r$$

y entonces $r \leq \lfloor \log_2 n \rfloor$. Como G es isomorfo a un subgrupo de \mathbb{S}_n por el teorema de Cayley, entonces

$$\begin{aligned} \text{gnu}(n) &\leq \text{cantidad de subgrupos de orden } n \text{ de } \mathbb{S}_n \\ &\leq \text{cantidad de subgrupos de } \mathbb{S}_n \text{ generados por } \lfloor \log_2 n \rfloor \text{ elementos} \\ &\leq \text{cantidad de subconjuntos de } \mathbb{S}_n \text{ de } \lfloor \log_2 n \rfloor \text{ elementos.} \end{aligned}$$

Como la cantidad de subconjuntos de \mathbb{S}_n de $\lfloor \log_2 n \rfloor$ elementos es

$$\binom{n!}{\lfloor \log_2 n \rfloor} \leq (n!)^{\log_2 n}$$

pues $\binom{n}{k} \leq n^k$, se concluye que $\text{gnu}(n) \leq n^{n \log_2 n}$. □

En el caso de p -grupos puede probarse elementalmente que

$$\text{gnu}(p^n) \leq p^{\frac{1}{6}(n^3 - n)},$$

ver [5, Theorem 5.1]. Se conocen cotas mucho más sofisticada:

Teorema 21.7 (Higman–Sims). Si p es un número primo y $n \in \mathbb{N}$, entonces

$$p^{\frac{2}{27}n^3 - O(n^2)} \leq \text{gnu}(p^n) \leq p^{\frac{2}{27}n^3 + O(n^{\frac{8}{3}})}.$$

La demostración del teorema anterior resulta de combinar los trabajos de Higman [16] y Sims [32]. Una presentación moderna puede encontrarse en el libro [5].

En [17] Higman conjeturó que $\text{gnu}(p^n)$ es una función polinomial de p y p módulo N para una cierta cantidad finita de enteros N . Se conoce como la conjetura PORC.

Conjetura 21.8 (Higman). Sea $n \in \mathbb{N}$. Existen entonces N polinomios

$$P_0(X), P_1(X), \dots, P_{N-1}(X)$$

tales que si $p \equiv i \pmod{N}$, entonces $\text{gnu}(p^n) = P_i(p)$.

PORC viene de *Polynomial On Residue Classes*.

Se sabe que la conjetura es cierta para $n \leq 7$, aunque el problema permanece abierto para $n \geq 8$. En [7], un trabajo de más de setenta páginas, du Sautoy y Vaughan–Lee construyeron una familia de grupos de orden p^{10} que sugiere que la conjetura PORC podría no ser verdadera. De todas formas, la conjetura PORC de Higman sigue abierta.

Teorema 21.9 (Pyber). Si $n \in \mathbb{N}$, entonces $\text{gnu}(n) \leq n^{\frac{2}{27}\mu(n)^2 + O(\mu(n)^{\frac{5}{3}})}$, donde $\mu(n)$ es el mayor exponente que aparece en la factorización en primos de n .

La demostración aparece en [29] y en el caso de grupos no resolubles utiliza la clasificación de grupos simples. Una presentación detallada puede consultarse en el libro [5] de Blackburn, Neumann y Venkataraman.

Capítulo 22

El subgrupo de Frattini

Definición 22.1. Sea G un grupo. Si G posee grupos maximales, se define el **subgrupo de Frattini** $\Phi(G)$ como la intersección de los subgrupos maximales de G . En caso contrario, se define $\Phi(G) = G$.

Ejercicio 22.2. Demuestre que $\Phi(G)$ es un subgrupo característico de G .

Ejemplo 22.3. Sea $G = \mathbb{S}_3$. Los subgrupos maximales de G son

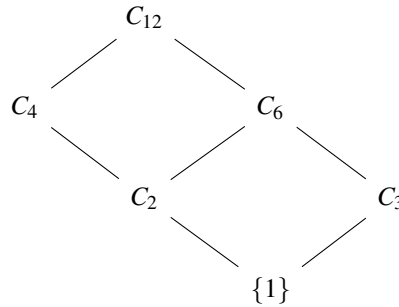
$$M_1 = \langle (123) \rangle, \quad M_2 = \langle (12) \rangle, \quad M_3 = \langle (23) \rangle, \quad M_4 = \langle (13) \rangle.$$

Luego $\Phi(G) = \{1\}$.

Ejemplo 22.4. Sea $G = \langle g \rangle \simeq C_{12}$. Como G es cíclico, los subgrupos de G son

$$\{1\}, \quad \langle g^6 \rangle \simeq C_2, \quad \langle g^4 \rangle \simeq C_3, \quad \langle g^3 \rangle \simeq C_4, \quad \langle g^2 \rangle \simeq C_6, \quad G.$$

Como los únicos subgrupos maximales son $\langle g^3 \rangle \simeq C_4$ y $\langle g^2 \rangle \simeq C_6$, obtenemos que $\Phi(G) = \langle g^3 \rangle \cap \langle g^2 \rangle = \langle g^6 \rangle \simeq C_2$. Veamos el diagrama:



Ejemplo 22.5. Sea $G = \mathbf{SL}_2(3)$. El siguiente código muestra que $\Phi(G) \simeq C_2$:

```
gap> StructureDescription(FrattiniSubgroup(SL(2,3)));
"C2"
```

lemma:Dedekind

Lema 22.6 (Dedekind). Sean H, K, L subgrupos de G tales que $H \subseteq L \subseteq G$. Entonces $HK \cap L = H(K \cap L)$.

Demostración. Demostraremos que $HK \cap L \subseteq H(K \cap L)$ pues la otra inclusión es trivial. Si $x = hk \in HK \cap L$, donde $x \in L$, $h \in H$, $k \in K$, entonces $k = h^{-1}x \in L \cap K$ pues $H \subseteq L$. Luego $x = hk \in H(K \cap L)$. \square

lemma:G=HPhi(G)

Lema 22.7. Sea G un grupo finito. Si H es un subgrupo de G tal que $G = H\Phi(G)$ entonces $H = G$.

Demostración. Supongamos que $H \neq G$ y sea M un subgrupo maximal de G tal que $H \subseteq M$. Como $\Phi(G) \subseteq M$, $G = H\Phi(G) \subseteq M$, una contradicción. \square

proposition:phi(N)phi(G)

Proposición 22.8. Sea N un subgrupo normal de un grupo finito G . Entonces $\Phi(N) \subseteq \Phi(G)$.

Demostración. Como $\Phi(N)$ es característico en N y N es normal en G , $\Phi(N)$ es normal en G . Supongamos entonces que existe un subgrupo maximal M de G tal que $\Phi(N) \not\subseteq M$. La maximalidad de M implica entonces que $\Phi(N)M = G$ pues de lo contrario $M = \Phi(N)M \supseteq \Phi(N)$. Por el lema de Dedekind (con $H = \Phi(N)$, $K = M$ y $L = N$),

$$N = G \cap N = (\Phi(N)M) \cap N = \Phi(N)(M \cap N).$$

Ahora el lema anterior con $G = N$ y $H = M \cap N$ implica que $\Phi(N) \subseteq N \subseteq M$, una contradicción. Luego todo subgrupo maximal de G contiene a $\Phi(N)$ y por lo tanto $\Phi(G) \supseteq \Phi(N)$. \square

El lema que sigue nos dice que los elementos del subgrupo de Frattini son esencialmente los "no-generadores" del grupo.

lemma:nongenerators

Lema 22.9 (de los no-generadores). Sea G un grupo finito. Entonces

$$\Phi(G) = \{x \in G : \text{si } G = \langle x, Y \rangle \text{ para algún } Y \subseteq G \text{ entonces } G = \langle Y \rangle\}.$$

Demostración. Veamos primero la inclusión \supseteq . Sea $x \in G$ y sea M un subgrupo maximal de G . Si $x \notin M$ entonces, como $G = \langle x, M \rangle$, se tiene $G = \langle M \rangle = M$, absurdo. Luego $x \in M$ para todo subgrupo maximal M y entonces $x \in \Phi(G)$.

Veamos ahora la inclusión \subseteq . Sea $x \in \Phi(G)$ tal que $G = \langle x, Y \rangle$ para algún subconjunto Y de G . Si $G \neq \langle Y \rangle$, existe un subgrupo maximal M tal que $\langle Y \rangle \subseteq M$. Como $x \in M$, $G = \langle x, Y \rangle \subseteq M$, una contradicción. \square

Ejemplo 22.10. Sea p un número primo. Sea G un p -grupo elemental abeliano, es decir $G \simeq C_p^m$ para algún $m \in \mathbb{N}$. Supongamos además que $G = \langle x_1 \rangle \times \cdots \times \langle x_m \rangle$ con $\langle x_j \rangle \simeq C_p$. Veamos que $\Phi(G)$ es trivial. Sea $j \in \{1, \dots, m\}$ y sea $n_j \in \{1, \dots, p-1\}$. Como el conjunto

$$\{x_1, \dots, x_{j-1}, x_j^{n_j}, x_{j+1}, \dots, x_m\}$$

genera al grupo G y $\{x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_m\}$ no lo hace, entonces $x_j^{n_j} \notin \Phi(G)$ por el lema de los no-generadores. Luego $\Phi(G) = \{1\}$.

theorem:Frattini

Teorema 22.11 (Frattini). *Sea G un grupo finito. Entonces $\Phi(G)$ es nilpotente.*

Demostración. Sea $P \in \text{Syl}_p(\Phi(G))$ para algún primo p . Como $\Phi(G)$ es normal en G , gracias al argumento de Frattini (que vimos en el lema 19.13) podemos escribir $G = \Phi(G)N_G(P)$. Por el lema 22.7, $G = N_G(P)$. Como todo subgrupo de Sylow de $\Phi(G)$ es normal en G , $\Phi(G)$ es nilpotente. \square

exercise:G/M

Ejercicio 22.12. Sea G un grupo y sea M un subgrupo normal de G maximal. Demuestre que G/M es cíclico de orden primo.

theorem:Gaschutz

Teorema 22.13 (Gaschütz). *Si G es un grupo finito entonces*

$$[G, G] \cap Z(G) \subseteq \Phi(G).$$

Demostración. Sea $D = [G, G] \cap Z(G)$. Supongamos que D no está contenido en $\Phi(G)$. Como $\Phi(G)$ está contenido en todo subgrupo maximal de G , existe un subgrupo maximal M de G tal que D no está contenido en M . Esto implica que $G = MD$. Como $D \subseteq Z(G)$, M es normal en G pues si $g = md \in G = MD$ entonces

$$gMg^{-1} = (md)Md^{-1}m^{-1} = mMm^{-1} = M.$$

Como G/M es cíclico de orden primo, en particular, G/M es abeliano y luego $[G, G] \subseteq M$. En consecuencia, $D \subseteq [G, G] \subseteq M$, una contradicción. \square

lemma:N_G(H)=H

Lema 22.14. *Sea G un grupo finito y sea $P \in \text{Syl}_p(G)$. Sea H un subgrupo de G tal que $N_G(P) \subseteq H$. Entonces $N_G(H) = H$.*

Demostración. Sea $x \in N_G(H)$. Como $P \in \text{Syl}_p(H)$ y $Q = xPx^{-1} \in \text{Syl}_p(H)$, gracias al segundo teorema de Sylow existe $h \in H$ tal que $hQh^{-1} = (hx)P(hx)^{-1} = P$. Entonces $hx \in N_G(P) \subseteq H$ y luego $x \in H$. \square

theorem:Wielandt

Teorema 22.15 (Wielandt). *Sea G un grupo finito. Entonces G es nilpotente si y sólo si $[G, G] \subseteq \Phi(G)$.*

Demostración. Supongamos que $[G, G] \subseteq \Phi(G)$. Sea $P \in \text{Syl}_p(G)$. Si $N_G(P) \neq G$ entonces $N_G(P) \subseteq M$ para algún subgrupo maximal M de G . Si $g \in G$ y $m \in M$ entonces, como

$$gmg^{-1}m^{-1} = [g, m] \in [G, G] \subseteq \Phi(G) \subseteq M,$$

M es normal en G . Como además $N_G(P) \subseteq M$, el lema 22.14 implica que

$$G = N_G(M) = M,$$

una contradicción. Luego $N_G(P) = G$. Todo subgrupo de Sylow de G es normal en G y entonces G es nilpotente.

Supongamos ahora que G es nilpotente. Sea M un subgrupo maximal de G . Como M es normal en G y maximal, G/M no tiene subgrupos propios no triviales. Luego $G/M \simeq C_p$ para algún primo p . En particular G/M es abeliano y luego $[G, G] \subseteq M$. Como $[G, G]$ está contenido en todo subgrupo maximal de G , $[G, G] \subseteq \Phi(G)$. \square

theorem:G/phi(G)

Teorema 22.16. Sea G un grupo finito. Entonces G es nilpotente si y sólo si $G/\Phi(G)$ es nilpotente.

Demostración. Si G es nilpotente, entonces $G/\Phi(G)$ es nilpotente. Supongamos que $G/\Phi(G)$ es nilpotente. Sea $P \in \text{Syl}_p(G)$. Como $\Phi(G)P/\Phi(G) \in \text{Syl}_p(G/\Phi(G))$ y $G/\Phi(G)$ es nilpotente, $\Phi(G)P/\Phi(G)$ es un subgrupo normal de $G/\Phi(G)$. Luego, por el teorema de la correspondencia, $\Phi(G)P$ es un subgrupo normal de G . Como $P \in \text{Syl}_p(\Phi(G)P)$, el argumento de Frattini (que vimos en el lema 19.13) implica que

$$G = \Phi(G)PN_G(P) = \Phi(G)N_G(P)$$

pues $P \subseteq N_G(P)$. Luego $G = N_G(P)$ por el lema 22.7) y entonces P es normal en G . Esto implica que G es nilpotente. \square

theorem:Hall_nilpotente

Teorema 22.17 (Hall). Sea G un grupo finito y sea N un subgrupo normal de G . Si N y $G/[N, N]$ son nilpotentes, entonces G es nilpotente.

Demostración. Como N es nilpotente, $[N, N] \subseteq \Phi(N)$ por el teorema de Wielandt (teorema 22.15). Por la proposición 22.8, $[N, N] \subseteq \Phi(N) \subseteq \Phi(G)$. Por propiedad universal, existe un morfismo $G/[N, N] \rightarrow G/\Phi(G)$ sobreyectivo que hace conmutar el diagrama

$$\begin{array}{ccc} G & \longrightarrow & G/\Phi(G) \\ \downarrow & \nearrow & \\ G/[N, N] & & \end{array}$$

Como por hipótesis $G/[N, N]$ es nilpotente, $G/\Phi(G)$ es nilpotente por el teorema 20.13. Luego G es nilpotente por el teorema anterior. \square

Definición 22.18. Un **conjunto minimal de generadores** de un grupo G es un conjunto X de generadores de G tal que ningún subconjunto propio de X genera a G .

Es importante observar que un conjunto minimal de generadores puede no tener cardinal mínimo.

Ejemplo 22.19. Sea $G = \langle g \rangle \simeq C_6$. Si $a = g^2$ y $b = g^3$ entonces $\{a, b\}$ es un conjunto minimal de generadores de G , aunque no tiene cardinal mínimo pues por ejemplo $G = \langle ab \rangle$.

Si p es un número primo, \mathbb{F}_p denota al cuerpo de p elementos.

lemma:Burnside:minimal

Lema 22.20. Sea p un número primo y sea G un p -grupo finito. Entonces $G/\Phi(G)$ es un espacio vectorial sobre \mathbb{F}_p .

Demostración. Sea K un subgrupo maximal de G . Como G es nilpotente por la proposición 20.15, K es normal en G (ejercicio 20.45). Luego $G/K \simeq C_p$ por ser un p -grupo simple.

Basta ver que $G/\Phi(G)$ es p -grupo elemental abeliano. En un p -grupo pues G es un p -grupo. Sean K_1, \dots, K_m son los subgrupos maximales de G . Si $x \in G$ entonces

$x^p \in K_j$ para todo $j \in \{1, \dots, m\}$ y luego $x^p \in \Phi(G) = \cap_{j=1}^m K_j$. Además $G/\Phi(G)$ es abeliano pues $[G, G] \subseteq \Phi(G)$ por ser G nilpotente por el teorema de Wielandt (teorema 22.15). \square

theorem:Burnside:basis

Teorema 22.21 (Burnside). *Sea p un número primo y sea G un p -grupo finito. Si X es un conjunto minimal de generadores entonces $|X| = \dim G/\Phi(G)$.*

Demostración. Vimos en el lema anterior que $G/\Phi(G)$ es un espacio vectorial sobre \mathbb{F}_p . Sea $\pi: G \rightarrow G/\Phi(G)$ el morfismo canónico y sea $\{x_1, \dots, x_n\}$ un conjunto minimal de generadores de G . Veamos que $\{\pi(x_1), \dots, \pi(x_n)\}$ es un conjunto linealmente independiente de $G/\Phi(G)$. Supongamos sin perder generalidad que $\pi(x_1) \in \langle \pi(x_2), \dots, \pi(x_n) \rangle$. Existe entonces $y \in \langle x_2, \dots, x_n \rangle$ tal que $x_1 y^{-1} \in \Phi(G)$. Como G está generado por $\{x_1 y^{-1}, x_2, \dots, x_n\}$ y $x_1 y^{-1} \in \Phi(G)$, el lema de los no-generadores (lema 22.9) implica que G también está generado por $\{x_2, \dots, x_n\}$, una contradicción a la minimalidad. Luego $n = \dim G/\Phi(G)$. \square

Capítulo 23

El subgrupo de Fitting

Definición 23.1. Sea G un grupo finito y sea p un número primo. Se define el p -**radical** de G como el subgrupo

$$O_p(G) = \bigcap_{P \in \text{Syl}_p(G)} P.$$

lemma:core:Op(G)

Lema 23.2. Sea G un grupo finito y sea p un número primo.

- 1) $O_p(G)$ es normal en G .
- 2) Si N es un subgrupo normal de G contenido en algún $P \in \text{Syl}_p(G)$, entonces $N \subseteq O_p(G)$.

Demostración. Sea $P \in \text{Syl}_p(G)$ y hagamos actuar a G en G/P por multiplicación a izquierda. Tenemos entonces un morfismo $\rho: G \rightarrow \mathbb{S}_{G/P}$ con núcleo

$$\begin{aligned} \ker \rho &= \{x \in G : \rho_x = \text{id}\} = \{x \in G : xgP = gP \forall g \in G\} \\ &= \{x \in G : x \in gPg^{-1} \forall g \in G\} = \bigcap_{g \in G} gPg^{-1} = O_p(G). \end{aligned}$$

Luego $O_p(G)$ es normal en G .

Sea ahora N un subgrupo normal de G tal que $N \subseteq P$. Como para todo $g \in G$ se tiene $N = gNg^{-1} \subseteq gPg^{-1}$, se concluye que $N \subseteq O_p(G)$. \square

Definición 23.3. Sea G un grupo finito y sean p_1, \dots, p_k los factores primos de $|G|$. Se define el **subgrupo de Fitting** como el subgrupo

$$F(G) = O_{p_1}(G) \cdots O_{p_k}(G)$$

Ejercicio 23.4. Demuestre que $F(G)$ es característico en G .

Ejemplo 23.5. Sea $G = \mathbb{S}_3$. Es fácil ver que $O_2(G) = \{1\}$ y que $O_3(G) = \langle (123) \rangle$. Entonces $F(G) = \langle (123) \rangle$.

theorem:Fitting

Teorema 23.6 (Fitting). *Sea G un grupo finito. El subgrupo de Fitting $F(G)$ es normal en G y nilpotente. Además $F(G)$ contiene a todo subgrupo normal nilpotente de G .*

Demostración. Por definición $|F(G)|$ es el producto de los órdenes de los $O_p(G)$. Como entonces $O_p(G) \in \text{Syl}_p(F(G))$, se concluye que $F(G)$ es nilpotente por tener un p -subgrupo de Sylow normal para cada primo p . Luego $F(G)$ es nilpotente por el teorema 20.43.

Sea N un subgrupo normal de G nilpotente y sea $P \in \text{Syl}_p(N)$. Como N es nilpotente, P es normal en N y entonces P es el único p -subgrupo de Sylow de N . Luego P es característico en N y entonces P es normal en G . Como N es nilpotente, N es producto directo de sus subgrupos de Sylow. Luego $N \subseteq O_p(G)$ por el lema 23.2. \square

corollary:Z(G) subset F(G)

Corolario 23.7. *Sea G un grupo finito. Entonces $Z(G) \subseteq F(G)$.*

Demostración. Como $Z(G)$ es nilpotente (por ser abeliano) y $Z(G)$ es normal en G , $Z(G) \subseteq F(G)$ por el teorema de Fitting. \square

corollary:Fitting

Corolario 23.8 (Fitting). *Sean K y L subgrupos normales nilpotentes de un grupo finito G . Entonces KL es nilpotente.*

Demostración. Por el teorema de Fitting sabemos que $K \subseteq F(G)$ y $L \subseteq F(G)$. Esto implica que $KL \subseteq F(G)$ y luego KL es nilpotente pues $F(G)$ es nilpotente. \square

corollary:McapF(G)

Corolario 23.9. *Sea G un grupo finito y sea N un subgrupo normal de G . Entonces $N \cap F(G) = F(N)$.*

Demostración. Como $F(N)$ es característico en N , $F(N)$ es normal en G . Luego $F(N) \subseteq N \cap F(G)$ pues $F(N)$ es nilpotente. Para la otra inclusión, como $F(G)$ es normal en G , el subgrupo $F(G) \cap N$ es normal en N . Como $F(G) \cap N$ es nilpotente, $F(G) \cap N \subseteq F(N)$. \square

Veamos una aplicación a grupos finitos resolubles.

Teorema 23.10. *Sea G un grupo finito no trivial y resoluble. Todo subgrupo normal N no trivial contiene un subgrupo normal abeliano no trivial y este subgrupo está en realidad contenido en $F(N)$.*

Demostración. Sabemos que $N \cap G^{(0)} = N \neq \{1\}$. Como G es un grupo resoluble resoluble, existe $m \in \mathbb{N}$ tal que $N \cap G^{(m)} = \{1\}$. Sea $n \in \mathbb{N}$ maximal tal que $N \cap G^{(n)}$ es no trivial. Como $[N, N] \subseteq N$ y $[G^{(n)}, G^{(n)}] = G^{(n+1)}$,

$$[N \cap G^{(n)}, N \cap G^{(n)}] \subseteq N \cap G^{(n+1)} = \{1\}.$$

Luego $N \cap G^{(n)}$ es un subgrupo abeliano de G . Como además es normal y nilpotente, $N \cap G^{(n)} \subseteq N \cap F(G) = F(N)$. \square

theorem:F(G) centraliza

Teorema 23.11. *Si G es un grupo finito y N es un subgrupo minimal-normal entonces entonces $F(G) \subseteq C_G(N)$.*

Demostración. Por el teorema de Fitting, $F(G)$ es un subgrupo normal y nilpotente. Sea N un subgrupo minimal-normal de G . El subgrupo $N \cap F(G)$ es normal en G . Además $[F(G), N] \subseteq N \cap F(G)$. Si $N \cap F(G) = \{1\}$ entonces $[F(G), N] = \{1\}$. Si no, $N = N \cap F(G) \subseteq F(G)$ por la minimalidad de N . Como $F(G)$ es nilpotente, $N \cap Z(F(G)) \neq \{1\}$ por el teorema de Hirsch. Como $Z(F(G))$ es característico en $F(G)$ y $F(G)$ es normal en G , $Z(F(G))$ es normal en G . Como $\{1\} \neq N \cap Z(F(G))$ es normal en G , la minimalidad de N implica que $N = N \cap Z(F(G)) \subseteq Z(F(G))$ y luego $[F(G), N] = \{1\}$. \square

Corolario 23.12. *Sea G un grupo finito y resoluble.*

- 1) *Si N es un subgrupo minimal-normal entonces $N \subseteq Z(F(G))$.*
- 2) *Si H es un subgrupo normal entonces $H \cap F(G) \neq \{1\}$.*

Demostración. Demostremos la primera afirmación. Como N es un p -grupo por el lema 19.8, N es nilpotente y luego $N \subseteq F(G)$. Además $F(G) \subseteq C_G(N)$ por el teorema anterior. Luego $N \subseteq Z(F(G))$.

Demostremos ahora la segunda afirmación. El subgrupo H contiene un subgrupo minimal-normal N y $N \subseteq F(G)$. Luego $H \cap F(G) \neq \{1\}$. \square

Teorema 23.13. *Sea G un grupo finito.*

- 1) $\Phi(G) \subseteq F(G)$ y $Z(G) \subseteq F(G)$.
- 2) $F(G)/\Phi(G) \simeq F(G/\Phi(G))$.

Demostración. Demostremos la primera afirmación. Como $\Phi(G)$ es normal en G y nilpotente por el teorema 22.11 y $F(G)$ contiene a todo subgrupo normal nilpotente de G (teorema 23.6), $\Phi(G) \subseteq F(G)$. Además $Z(G)$ es normal y nilpotente (por ser abeliano) y luego $Z(G) \subseteq F(G)$.

Demostremos la segunda afirmación. Sea $\pi: G \rightarrow G/\Phi(G)$ el morfismo canónico. Como $F(G)$ es nilpotente, $\pi(F(G))$ es nilpotente y luego

$$\pi(F(G)) \subseteq F(G/\Phi(G))$$

por el teorema 23.6. Por otro lado, sea $H = \pi^{-1}(F(G/\Phi(G)))$. Por la correspondencia, H es un subgrupo normal de G que contiene a $\Phi(G)$. Si $P \in \text{Syl}_p(H)$ entonces $\pi(P) \in \text{Syl}_p(\pi(H))$ pues $\pi(P) \simeq P/P \cap \Phi(G)$ es un p -grupo y además $(\pi(H) : \pi(P))$ es coprimo con p pues

$$(\pi(H) : \pi(P)) = \frac{|\pi(H)|}{|\pi(P)|} = \frac{|H/\Phi(G)|}{|P/P \cap \Phi(G)|} = \frac{(H : P)}{(\Phi(G) : P \cap \Phi(G))}$$

es un divisor de $(H : P)$, que es coprimo con p . Como $\pi(H)$ es nilpotente, $\pi(P)$ es característico en $\pi(H)$ y luego $\pi(P)$ es normal en $\pi(G) = G/\Phi(G)$. Entonces $P\Phi(G) = \pi^{-1}(\pi(P))$ es normal en G . Como $P \in \text{Syl}_p(P\Phi(G))$, el argumento de

Fratini del lema 19.13 implica que $G = \Phi(G)N_G(P)$. Luego P es normal en G por el lema 22.7. Como P es nilpotente y normal en G , entonces $P \subseteq F(G)$ por el teorema 23.6. Luego $H \subseteq F(G)$ y entonces $F(G/\Phi(G)) = \pi(H) \subseteq \pi(F(G))$. \square

Capítulo 24

Super resolubilidad

super

Definición 24.1. Un grupo G se dice **súper-resoluble** si existe una sucesión de subgrupos normales

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

tal que cada cociente G_{i-1}/G_i es cíclico.

Observemos que en la definición anterior no se pide que G sea un grupo finito. Los cocientes pueden ser entonces grupos cíclicos de orden n o grupos cíclicos infinitos, es decir grupos isomorfos a \mathbb{Z} .

Ejemplo 24.2. El grupo diedral \mathbb{D}_n de orden $2n$ es súper-resoluble pues

$$\mathbb{D}_n \supseteq \langle r \rangle \supseteq \{1\}$$

es una sucesión de subgrupos normales con factores cíclicos.

Todo grupo súper-resoluble es resoluble, ver ejercicio 19.12.

Ejemplo 24.3. El grupo \mathbb{A}_4 es resoluble pero no es súper-resoluble. El único subgrupo propio no trivial normal de \mathbb{A}_4 es

$$\{\text{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2.$$

Luego \mathbb{A}_4 no posee una sucesión de subgrupos normales con factores cíclicos.

Ejercicio 24.4. Demuestre que el grupo $\text{Aff}(\mathbb{Z})$ es super resoluble.

Ejemplo 24.5. El grupo $\text{SL}_2(3)$ es resoluble pero no es súper-resoluble:

```
gap> IsSolvable(SL(2,3));
true
gap> IsSupersolvable(SL(2,3));
false
```

xca:super

Ejercicio 24.6. Demuestre las siguientes afirmaciones:

- 1) Todo subgrupo de un grupo súper-resoluble es súper-resoluble.
- 2) Todo cociente de un grupo súper-resoluble es súper-resoluble.

exercise:directosuper

Ejercicio 24.7. Demuestre que el producto directo de grupos súper-resolubles es súper-resoluble.

Ejercicio 24.8. Sean H y K subgrupos normales de un grupo G tales que G/K y G/H son súper-resolubles. Demuestre que $G/H \cap K$ es súper-resoluble.

proposition:Nciclico

Proposición 24.9. Sea N un subgrupo normal cíclico de un grupo G . Si G/N es súper-resoluble entonces G es súper-resoluble.

Demostración. Sea $\pi: G \rightarrow G/N$ el morfismo canónico y sea $Q = G/N$. Como Q es súper-resoluble, tenemos una sucesión

$$Q = Q_0 \supseteq Q_1 \supseteq \cdots \supseteq Q_n = \{1\}$$

de subgrupos normales de Q tales que cada cociente Q_{i-1}/Q_i es cíclico. Cada elemento de la sucesión

$$G = \pi^{-1}(Q) \supseteq \pi^{-1}(Q_1) \supseteq \cdots \supseteq \pi^{-1}(Q_n) = N \supseteq \{1\}$$

es normal en G (por la correspondencia) y dejamos como ejercicio demostrar que cada cociente es cíclico. \square

theorem:ZorCp

Teorema 24.10. Sea G un grupo súper-resoluble no trivial. Entonces G posee una sucesión de subgrupos $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ de subgrupos normales tales que cada cociente G_{i-1}/G_i es cíclico de orden primo o isomorfo a \mathbb{Z} .

Demostración. Sea $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ una sucesión de subgrupos normales tal que cada cociente G_{i-1}/G_i es cíclico. Sea $i \in \{1, \dots, n\}$ tal que el cociente $G_{i-1}/G_i \simeq C_n$ para algún n que no es primo y sea $\pi: G_{i-1} \rightarrow G_{i-1}/G_i$ el morfismo canónico. Sea p un primo que divide a n y sea H un subgrupo de G tal que $\pi(H)$ es un subgrupo de G_{i-1}/G_i de orden p . Por el teorema de la correspondencia, $G_i \subseteq H \subseteq G_{i-1}$.

Veamos que H es normal en G . Sea $g \in G$. Como $\pi(gHg^{-1})$ es un subgrupo de orden p del cíclico G_{i-1}/G_i , $\pi(gHg^{-1}) = \pi(H)$. Luego $gHg^{-1} = G_iH \subseteq H$ y en conclusión $gHg^{-1} = H$.

Observemos que H/G_i es cíclico de orden primo pues

$$H/G_i = H/H \cap G_i \simeq \pi(H) \simeq C_p$$

y que G_{i-1}/H también es cíclico pues

$$G_{i-1}/H \simeq \frac{G_{i-1}/G_i}{H/G_i}$$

es cociente de un grupo cíclico.

Demostramos que al insertar H en la sucesión obtenemos una nueva sucesión con factores cíclicos y donde H/G_i es cíclico de orden primo. Al repetir este proceso se obtiene el resultado deseado. \square

Una aplicación inmediata:

Corolario 24.11. *Un grupo finito súper-resoluble admite una sucesión de subgrupos $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ normales donde cada cociente G_{i-1}/G_i es cíclico de orden primo.*

Veamos otras propiedades importantes de grupos súper-resolubles.

Teorema 24.12. *Sea G un grupo súper-resoluble.*

- 1) Si N es minimal-normal en G entonces $N \simeq C_p$ para algún primo p .
- 2) Si M es maximal en G entonces $(G : M) = p$ para algún primo p .
- 3) El conmutador $[G, G]$ es nilpotente.
- 4) Si G es no abeliano existe un subgrupo normal $N \neq G$ tal que $Z(G) \subsetneq N$.

Demostración. Demostremos la primera afirmación. Como G es súper-resoluble, existe una sucesión $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{1\}$ de subgrupos normales con factores G_{i-1}/G_i cíclicos. Como cada $G_i \cap N$ es un subgrupo normal de G contenido en N , la minimalidad de N implica que cada $G_i \cap N$ es trivial o igual a N . Además $N \cap G_0 = N$ y $N \cap G_n = \{1\}$. Sea j el mínimo entero tal que $N \cap G_j = \{1\}$. Como $N \subseteq G_{j-1}$ (pues $N \cap G_{j-1} = N$), la composición

$$N \hookrightarrow G_{j-1} \rightarrow G_{j-1}/G_j$$

es un morfismo inyectivo, pues tiene núcleo igual a $N \cap G_j = \{1\}$. Luego N es cíclico por ser isomorfo a un subgrupo del cíclico G_{i-1}/G_i . Si $G_{i-1}/G_i \simeq \mathbb{Z}$ entonces $N \simeq \mathbb{Z}$ pero no sería minimal-normal ya que por ejemplo $2\mathbb{Z}$ es un subgrupo característico de \mathbb{Z} y por lo tanto es normal en G . Luego N es cíclico y finito y entonces $N \simeq C_p$.

Demostremos la segunda afirmación. Sea M un subgrupo maximal de G . Si M es normal en G entonces G/M no contiene subgrupos propios no triviales. Luego $G/M \simeq C_p$ para algún primo p . Supongamos entonces que M no es normal en G . Sea $H = \bigcap_{g \in G} M g^{-1}$ y sea $\pi: G \rightarrow G/H$. Como $\pi(M)$ es maximal en $\pi(G) = G/H$ y además

$$(G : M) = (G/H : M/H) = (G/H : M/H \cap M) = (\pi(G) : \pi(M)),$$

podemos suponer que M no contiene subgrupos normales no triviales de G , ya que en vez de trabajar con G lo hacemos con el cociente G/H . Como G es súper-resoluble existe una sucesión $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ de subgrupos normales de G con factores isomorfos a \mathbb{Z} o cíclicos de orden primo. Sea $N = G_{n-1}$. Como N es cíclico, todo subgrupo de N es característico en N y por lo tanto es normal en G . En particular, $M \cap N$ es normal en G y luego $M \cap N = \{1\}$. Como $M \subseteq NM \subseteq G$, entonces, por la maximalidad de M , $M = NM$ o bien $G = NM$. Pero como $N \subseteq NM = M$ es una contradicción, se concluye que $G = NM$. Si $N \simeq C_p$ para

algún primo p , entonces $(G : M) = p$ y la afirmación queda demostrada. Si $N \simeq \mathbb{Z}$ sea H un subgrupo propio de N . Como H es característico en N , H es normal en G y luego, como $M \subseteq HM \subseteq NM = G$, la maximalidad de M implica que $HM = M$ o bien $HM = G$. Como el caso $HM = M$ implica que $H \subseteq M \cap N = \{1\}$, podemos suponer que $HM = G$. Si $n \in N \setminus H$ entonces $n = hm$ para algún $h \in H$, $m \in M$. Luego $h = n$ pues $h^{-1}n \in N \cap M = \{1\}$, una contradicción.

Demostremos ahora la tercera afirmación. Como G es súper-resoluble, existe una sucesión

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

de subgrupos normales tal que cada G_i/G_{i+1} es cíclico. Para cada $i \in \{0, \dots, n\}$ sea $H_i = [G, G] \cap G_i$. Como $[G, G]$ y los G_i son normales en G , se tiene una sucesión

$$[G, G] = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = 1$$

de subgrupos normales de G . Como H_i y H_{i+1} es normal en G , el grupo G actúa por conjugación en H_i/H_{i+1} . Esto induce un morfismo $\gamma: G \rightarrow \text{Aut}(H_i/H_{i+1})$. Como H_i/H_{i+1} es cíclico, $\text{Aut}(H_i/H_{i+1})$ es abeliano y luego $[G, G] \subseteq \ker \gamma$. Luego $[G, G]$ actúa trivialmente por conjugación en H_i/H_{i+1} y entonces

$$H_i/H_{i+1} \subseteq Z([G, G]/H_{i+1}).$$

Por último demostremos la cuarta afirmación. Como G es no abeliano, $Z(G) \neq G$. Sea $\pi: G \rightarrow G/Z(G)$ el morfismo canónico. El cociente $G/Z(G)$ es súper-resoluble y la sucesión

$$G/Z(G) = \pi(G) \supseteq \pi(G_1) \supseteq \cdots \supseteq \pi(1) = 1$$

es una sucesión de subgrupos normales de $G/Z(G)$ con cocientes cíclicos. En particular, $1 \neq \pi(G_1)$ es propio y normal en $G/Z(G)$. Por el teorema de la correspondencia, $\pi^{-1}(\pi(G_1)) \neq G$ es un subgrupo normal de G que contiene propiamente a $Z(G)$. \square

Ejemplo 24.13. Si G es un grupo resoluble, no necesariamente $[G, G]$ es un grupo nilpotente. El grupo \mathbb{S}_4 es resoluble pero $[\mathbb{S}_4, \mathbb{S}_4] = \mathbb{A}_4$ no es nilpotente.

proposition:psuper

Proposición 24.14. Sea p un número primo. Todo p -grupo finito es súper-resoluble.

Demostración. Sea G un contraejemplo de orden minimal. Podemos suponer que $|G| = p^n$ con $n > 1$ (pues si $n = 1$ el grupo G es trivialmente súper-resoluble). Como G es un p -grupo, es nilpotente y existe un subgrupo normal N de orden p . El cociente G/N tiene orden p^{n-1} entonces es súper-resoluble pues $|G/N| < |G|$. Como N es cíclico y G/N es súper-resoluble, G es súper-resoluble por la proposición 24.9. \square

Corolario 24.15. Todo grupo finito nilpotente es súper-resoluble.

Demostración. Todo grupo finito nilpotente es producto directo (finito) de subgrupos de Sylow. Como cada p -grupo es súper-resoluble por la proposición 24.14, el resultado se obtiene inmediatamente del ejercicio 24.7. \square

Teorema 24.16. *Todo grupo súper-resoluble tiene subgrupos maximales.*

Demostración. Procederemos por inducción en la longitud de la sucesión de super-resolubilidad. Si la longitud es uno, el teorema es cierto pues en este caso el grupo es cíclico. Supongamos entonces que G admite una sucesión

$$G = G_0 \supseteq \cdots \supseteq G_k = 1$$

y que la afirmación es cierta para grupos súper-resolubles con sucesiones de longitud $< k$. Como G_{k-1} es normal en G , sea $\pi: G \rightarrow G/G_{k-1}$ el morfismo canónico. Entonces la sucesión

$$G/G_{k-1} = \pi(G) \supseteq \pi(G_1) \supseteq \cdots \supseteq \pi(G_{k-1}) = 1$$

prueba la resolubilidad de $\pi(G)$ y tiene longitud $< k$. Por hipótesis inductiva, G/G_{k-1} admite subgrupos maximales y luego, por el teorema de la correspondencia, G también admite subgrupos maximales. \square

Los grupos resolubles o nilpotentes no siempre admiten subgrupos maximales, ver por ejemplo \mathbb{Q} .

Definición 24.17. Se dice que un grupo G satisface la **condición maximal para subgrupos** si todo subconjunto \mathcal{S} no vacío de subgrupos tiene un subgrupo maximal (es decir, no contenido en ningún otro subgrupo de \mathcal{S}).

lemma:MAX=fg

Lema 24.18. *Sea G un grupo. Entonces G satisface la condición maximal para subgrupos si y sólo si todo subgrupo de G es finitamente generado.*

Demostración. Supongamos que G satisface la condición maximal para subgrupos y sea H un subgrupo de G . Sea \mathcal{S} el conjunto de subgrupos de H finitamente generados. Como \mathcal{S} es no vacío (pues $1 \in \mathcal{S}$), existe un elemento maximal $M \in \mathcal{S}$. Sea $x \in H$. Como $\langle M, x \rangle \in \mathcal{S}$, $M = \langle M, x \rangle$ y luego $x \in M$. Como entonces $H = M$, H es finitamente generado.

Supongamos ahora que todo subgrupo de G es finitamente generado. Si \mathcal{S} es un subconjunto no vacío de subgrupos de G sin elemento maximal, podemos construir una sucesión de subgrupos $S_1 \subseteq S_2 \subseteq \cdots$ que no se estabiliza (acá necesitamos utilizar el axioma de elección). Como la unión

$$S = \bigcup_{j \geq 1} S_j$$

es un subgrupo de G , es finitamente generado y luego $S \subseteq S_k$ para algún k suficientemente grande, una contradicción. \square

proposition:max:N

Proposición 24.19. *Sea G un grupo y sea H un subgrupo de G . Si G satisface la condición maximal para subgrupos entonces H también.*

Demostración. Es consecuencia inmediata del lema 24.18. \square

proposition:max:G/N

Proposición 24.20. Sea G un grupo y sea N un subgrupo normal de G . Si G/N y N satisfacen la condición maximal para subgrupos entonces G también.

Demostración. Sea $\pi: G \rightarrow G/N$ el morfismo canónico. Sea \mathcal{S} un subconjunto no vacío de subgrupos de G . El conjunto $\{S \cap N : S \in \mathcal{S}\}$ tiene un elemento maximal A y el conjunto $\{\pi(S) : S \in \mathcal{S}, S \cap N = A\}$ tiene un elemento maximal B . Sea $S \in \mathcal{S}$ tal que $\pi(S) = B$ y $S \cap N = A$. Si S no es maximal en \mathcal{S} , existe $T \in \mathcal{S}$ tal que $S \subsetneq T$, $N \cap T = A$ y $\pi(T) = B$. Sea $x \in T \setminus S$. Como $\pi(xN) = \pi(x) \in \pi(T) = B$, existe $y \in S$ tal que $xN = yN$. Luego $y^{-1}x \in N \cap T = A = N \cap S$, una contradicción pues $x \notin S$. \square

proposition:superfg

Proposición 24.21. Todo grupo súper-resoluble satisface la condición maximal para subgrupos. En particular, todo grupo súper-resoluble es finitamente generado.

Demostración. Procederemos por inducción en la longitud n de la sucesión de superresolubilidad. El caso $n = 1$ es trivial pues entonces G es cíclico. Supongamos entonces que el resultado vale para grupos súper-resolubles con serie de longitud $\leq n - 1$. Sea G un grupo súper-resoluble no trivial y sea

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

una sucesión de subgrupos normales de G con factores cíclicos. Como G_{n-1} es súper-resoluble por el ejercicio ??, G_{n-1} satisface la condición maximal para subgrupos por hipótesis inductiva. Luego, por la proposición 24.20, G satisface la condición maximal para subgrupos porque G/G_{n-1} es un grupo cíclico. \square

Ejemplo 24.22. El grupo abeliano \mathbb{Q} es nilpotente pero no es súper-resoluble porque no es finitamente generado.

Si G es un grupo y $x_1, \dots, x_{n+1} \in G$ se define

$$[x_1, \dots, x_{n+1}] = [[x_1, \dots, x_n], x_{n+1}], \quad n \geq 1.$$

lemma:G_n

Lema 24.23. Sea G un grupo finitamente generado, digamos $G = \langle X \rangle$ con X finito. Para cada $n \geq 2$ se define

$$G_n = \langle g[x_1, \dots, x_n]g^{-1} : x_1, \dots, x_n \in X, g \in G \rangle.$$

Entonces $G_n = \gamma_n(G)$ para todo $n \geq 2$.

Demostración. Observemos que cada G_n es normal en G . Procederemos por inducción en n . El caso $n = 2$ es trivial. Supongamos entonces que $\gamma_{n-1}(G) = G_{n-1}$. Sean $x_1, \dots, x_n \in X$. Como $[x_1, \dots, x_n] \in \gamma_n(G)$, $G_{n-1} \subseteq \gamma_n(G)$. Sea $N = G_n$ y sea $\pi: G \rightarrow G/N$ el morfismo canónico. El grupo G/N es finitamente generado. Como

$$[\pi([x_1, \dots, x_{n-1}]), \pi(x_n)] = \pi([x_1, \dots, x_n]) = 1,$$

se tiene que $\pi([x_1, \dots, x_{n-1}]) \in Z(G/N)$. Luego $\pi(g[x_1, \dots, x_n]g^{-1}) = 1$ para todo $g \in G$ y, por hipótesis inductiva, se concluye que

$$\pi(\gamma_{n-1}(G)) = \pi(G_{n-1}) \subseteq Z(G/N).$$

Como entonces

$$\pi(\gamma_n(G)) = \pi([\gamma_{n-1}(G), G]) = [\pi(\gamma_{n-1}(G)), \pi(G)] = 1,$$

se concluye que $\gamma_n(G) \subseteq N = G_n$. \square

lemma:gamma_n/gamma_n+1

Lema 24.24. *Sea G un grupo finitamente generado. Entonces $\gamma_n(G)/\gamma_{n+1}(G)$ es finitamente generado.*

Demostración. Supongamos que $G = \langle X \rangle$ con X finito. Al escribir

$$g[x_1, \dots, x_n]g^{-1} = [g, [x_1, \dots, x_n]][x_1, \dots, x_n]$$

y usar el lema 24.23 para obtener que $[g, [x_1, \dots, x_n]] \in \gamma_{n+1}(G) = G_{n+1}$,

$$g[x_1, \dots, x_n]g^{-1} \equiv [x_1, \dots, x_n] \text{ mód } \gamma_{n+1}(G).$$

Luego $\gamma_n(G)/\gamma_{n+1}(G)$ está generado por el conjunto finito

$$\{[x_1, \dots, x_n]\gamma_{n+1}(G) : x_1, \dots, x_n \in X\}.$$

\square

theorem:super=fg

Teorema 24.25. *Sea G un grupo nilpotente. Entonces G es súper-resoluble si y sólo si G es finitamente generado.*

Demostración. Si G es súper-resoluble, es finitamente generado por la proposición 24.21. Supongamos que G es finitamente generado y nilpotente. Como por el lema 24.24 cada $\gamma_n(G)/\gamma_{n+1}(G)$ es finitamente generado, digamos por y_1, \dots, y_m . Sea $\pi: G \rightarrow G/\gamma_{n+1}(G)$ el morfismo canónico. Para cada $j \in \{1, \dots, m\}$ sea

$$K_j = \langle \gamma_{n+1}(G), y_1, \dots, y_j \rangle.$$

Como $[K_j, G] \subseteq [\gamma_n(G), G] = \gamma_{n+1}(G)$, se tiene que $\pi(K_j)$ es central en $\pi(G)$. Luego $\pi(K_j)$ es normal en $\pi(G)$ y por lo tanto K_j es normal en G . Como cada K_j/K_{j-1} es cíclico generado por $y_j K_{j-1}$, entre $\gamma_n(G)$ y $\gamma_{n+1}(G)$ pudimos construir una sucesión de subgrupos normales de G con factores cíclicos. Como G es nilpotente, existe c tal que $\gamma_{c+1}(G) = 1$ y luego G es súper-resoluble. \square

corollary:nilpotente=>max

Corolario 24.26. *Todo grupo nilpotente finitamente generado satisface la condición maximal en subgrupos.*

Demostración. Es consecuencia del teorema 24.25 y la proposición 24.21. \square

Teorema 24.27. *Sea G un grupo nilpotente y finitamente generado. Entonces $T(G)$ es finito.*

Demostración. Como G es nilpotente, G satisface la condición maximal para subgrupos por el corolario 24.26 y entonces todo subgrupo de G es finitamente generado. Como $T(G)$ es un subgrupo por el teorema 20.37, es finitamente generado y de torsión. Luego $T(G)$ es finito por el teorema 20.41. \square

Capítulo 25

Derivaciones

derivaciones

En este capítulo veremos el caso más sencillo de extensiones de grupos. Es fundamental recordar la noción de producto semidirecto.

Definición 25.1. Sean K y Q grupos. Una **extensión** de K por Q es un grupo G que tiene un subgrupo normal N isomorfo a K tal que $G/N \simeq Q$. Equivalentemente, una **extensión** de K por Q es una sucesión exacta corta¹

$$1 \longrightarrow K \xrightarrow{\iota} G \xrightarrow{p} Q \longrightarrow 1$$

Ejemplo 25.2. C_6 y S_3 son extensiones de C_3 por C_2 .

Ejemplo 25.3. C_6 es extensión de C_2 por C_3 .

Ejemplo 25.4. Sean K y Q grupos. El producto directo $K \times Q$ es extensión de K por Q . También es extensión de Q por K .

Sea G una extensión de K por Q . Si L es un subgrupo de G que contiene a K entonces L es una extensión de K por L/K .

Definición 25.5. Sea $E: 1 \rightarrow K \xrightarrow{\iota} G \xrightarrow{p} Q \rightarrow 1$ una extensión. Un **levantamiento** para E es una función $\ell: Q \rightarrow G$ tal que $p(\ell(x)) = x$ para todo $x \in Q$.

xca:lifting

Ejercicio 25.6. Sea $E: 1 \rightarrow K \xrightarrow{\iota} G \xrightarrow{p} Q \rightarrow 1$ una extensión. Demuestre las siguientes afirmaciones:

- 1) Si $\ell: Q \rightarrow G$ es un levantamiento, $\ell(Q)$ es un transversal para $\ker p$ en G .
- 2) Todo transversal a $\ker p$ en G induce un levantamiento $\ell: Q \rightarrow G$.
- 3) Si $\ell: Q \rightarrow G$ es un levantamiento entonces $\ell(xy) \ker p = \ell(x)\ell(y) \ker p$.

Definición 25.7. Se dice que una extensión se **parte** si existe un levantamiento que es morfismo de grupos.

¹ ι es inyectiva, p es sobreyectiva y $\ker p = \iota(N)$.

El primer paso que daremos en este contexto es para entender las extensiones que se parten mediante "derivaciones".

Definición 25.8. Sean Q y K grupos. Supongamos que Q actúa por automorfismos en K . Una función $\varphi: Q \rightarrow K$ se dice un **1-cociclo** (o una **derivación**) si

$$\varphi(xy) = \varphi(x)(x \cdot \varphi(y))$$

para todo $x, y \in Q$. El conjunto de **derivaciones** de Q en K se define como

$$\text{Der}(Q, K) = Z^1(Q, K) = \{\delta: Q \rightarrow K : \delta \text{ es 1-cociclo}\}.$$

Ejemplo 25.9. Sea Q un grupo que actúa por automorfismos en K . Para cada $k \in K$, la función $Q \rightarrow K, x \mapsto [k, x] = kxk^{-1}x^{-1}$, es una derivación.

xca:1cocycle

Ejercicio 25.10. Sea $\varphi: Q \rightarrow K$ un 1-cociclo. Demuestre las siguientes afirmaciones:

- 1) $\varphi(1) = 1$.
- 2) $\varphi(y^{-1}) = (y^{-1} \cdot \varphi(y))^{-1} = y^{-1} \cdot \varphi(y)^{-1}$.
- 3) El conjunto $\ker \varphi = \{x \in Q : \varphi(x) = 1\}$ es un subgrupo de Q .

Recordemos que un subgrupo K de un grupo G admite un complemento Q si G se factoriza como $G = KQ$ y $K \cap Q = \{1\}$. El ejemplo típico es el siguiente, el producto semidirecto $G = K \rtimes Q$, donde K es un subgrupo normal de G y Q es un subgrupo de G tales que $K \cap Q = \{1\}$.

theorem:complementos

Teorema 25.11. Sea Q un grupo que actúa por automorfismos en el grupo K . Existe una biyección entre el conjunto de complementos de K en $K \rtimes Q$ y el conjunto $\text{Der}(Q, K)$.

Demostración. El grupo Q actúa en K por conjugación, entonces $\delta \in \text{Der}(Q, K)$ si y sólo si $\delta(xy) = \delta(x)x\delta(y)x^{-1}$, $x, y \in Q$. En este caso, las fórmulas del ejercicio anterior quedan así: $\delta(1) = 1$, $\delta(x^{-1}) = x^{-1}\delta(x)^{-1}x$.

Sea \mathcal{C} el conjunto de complementos de K en $K \rtimes Q$. Sea $C \in \mathcal{C}$. Si $x \in Q$, sabemos que existen únicos $k \in K$ y $c \in C$ tales que $x = k^{-1}c$. Queda bien definida entonces la función $\delta_C: Q \rightarrow K, x \mapsto k$. Vale que $\delta(x)x = c \in C$.

Veamos que $\delta_C \in \text{Der}(Q, K)$. Si $x, x_1 \in Q$, escribimos $x = k^{-1}c$ y $x_1 = k_1^{-1}c_1$, donde $k, k_1 \in K$ y $c, c_1 \in C$. Como K es normal en $K \rtimes Q$, podemos escribir a xx_1 como $xx_1 = k_2c_2$, donde $k_2 = k^{-1}(ck_1^{-1}c^{-1}) \in K$, $c_2 = cc_1 \in C$. Luego

$$\delta(xx_1)xx_1 = cc_1 = \delta(x)x\delta(x_1)x_1$$

implica que $\delta(xx_1) = \delta(x)x\delta(x_1)x^{-1}$. Tenemos así una función $F: \mathcal{C} \rightarrow \text{Der}(Q, K)$, $F(C) = \delta_C$.

Vamos a construir ahora $G: \text{Der}(Q, K) \rightarrow \mathcal{C}$. Para cada $\delta \in \text{Der}(Q, K)$ vamos a definir un complemento Δ de K en $K \rtimes Q$:

$$\Delta = \{\delta(x)x : x \in Q\}.$$

Veamos que Δ es un subgrupo de $K \rtimes Q$. Como $\delta(1) = 1$, $1 \in X$. Si $x, y \in Q$ entonces $\delta(x)x\delta(y)y = \delta(x)x\delta(y)x^{-1}xy = \delta(xy)xy \in \Delta$. Por último si $x \in Q$ entonces $(\delta(x)x)^{-1} = x^{-1}\delta(x)^{-1}xx^{-1} = \delta(x^{-1})x^{-1}$.

Veamos que $\Delta \cap K = \{1\}$. Si $x \in Q$ es tal que $\delta(x)x \in K$ entonces, como $\delta(x) \in K$, $x \in K \cap Q = 1$. Si $g \in G$ entonces existen únicos $k \in K$, $x \in Q$ tales que $g = kx$. Escribimos $g = k\delta(x)^{-1}\delta(x)x$. Como $k\delta(x)^{-1} \in K$ y $\delta(x)x \in \Delta$, se concluye que $G = K\Delta$. Queda bien definida entonces la función $G: \text{Der}(Q, K) \rightarrow \mathcal{C}$, $G(\delta) = \Delta$.

Veamos ahora que $G \circ F = \text{id}_{\mathcal{C}}$. Sea $C \in \mathcal{C}$. Entonces

$$G(F(C)) = G(\delta_C) = \{\delta_C(x)x : x \in Q\} = C,$$

por construcción. (Vimos que $\delta_C(x)x \in C$. Recíprocamente, si $c \in C$, escribimos $c = kx$ para únicos $k \in K$, $x \in Q$ y luego $x = k^{-1}c$ que implica $c = \delta_c(x)x$.)

Por último veamos que $F \circ G = \text{id}_{\text{Der}(Q, K)}$. Sea $\delta \in \text{Der}(Q, K)$. Entonces

$$F(G(\delta)) = F(\Delta) = \delta_\Delta.$$

Queremos demostrar que $\delta_\Delta = \delta$. Sea $x \in Q$. Existe $\delta(y)y \in \Delta$ para algún $y \in Q$ tal que $x = k^{-1}\delta(y)y$. Luego $\delta_\Delta(x)x = \delta(y)y$ y luego $\delta(x) = \delta(y)$ por la unicidad de la escritura. \square

Definición 25.12. Sean Q y K grupos. Supongamos que Q actúa por automorfismos en K . Un $\delta \in \text{Der}(Q, K)$ se dice **interior** si existe $k \in K$ tal que $\delta(x) = [k, x]$ para todo $x \in Q$. El conjunto de **derivaciones interiores** será denotado por

$$\text{Inn}(Q, K) = B^1(Q, K) = \{\delta \in \text{Der}(Q, K) : \delta \text{ es interior}\}.$$

Una derivación interior también se llama **1-coborde**.

theorem:Sysak

Teorema 25.13 (Sysak). Sean Q y K grupos tales que Q actúa por automorfismos en K . Sea $\delta \in \text{Der}(Q, K)$.

- 1) $\Delta = \{\delta(x)x : x \in Q\}$ es un complemento para K en $K \rtimes Q$.
- 2) $\delta \in \text{Inn}(Q, K)$ si y sólo si Q y Δ son conjugados en K .
- 3) $\ker \delta = Q \cap \Delta$.
- 4) δ es sobreyectiva si y sólo si $K \rtimes Q = \Delta Q$.

Demostración. Vimos en la demostración del teorema 25.11 que el conjunto Δ es un complemento para K en $K \rtimes Q$.

Demostremos la segunda afirmación. Si suponemos que δ es interior, existe $k \in K$ tal que $\delta(x) = [k, x] = kxk^{-1}x^{-1}$ para todo $x \in Q$. Como $\delta(x)x = kxk^{-1}$ para todo $x \in Q$, $\Delta = kQk^{-1}$. Recíprocamente, si existe $k \in K$ tal que $\Delta = kQk^{-1}$, para cada $x \in Q$ existe $y \in Q$ tal que $\delta(x)x = kyk^{-1}$. Como $[k, y] = kyk^{-1}y^{-1} \in K$, $\delta(x) \in K$ y $\delta(x)x = [k, y]y \in KQ$, se concluye que $x = y$ y luego $\delta(x) = [k, x]$.

Demostremos la tercera afirmación. Si $x \in Q$ es tal que $\delta(x)x = y \in Q$ entonces $\delta(x) = yx^{-1} \in K \cap Q = \{1\}$. Recíprocamente, si $x \in Q$ es tal que $\delta(x) = 1$ entonces $x = \delta(x)x \in Q \cap \Delta$.

Demostremos la cuarta afirmación. Si δ es sobreyectiva, para cada $k \in K$ existe $y \in Q$ tal que $\delta(y) = k$. Luego $K \rtimes Q \subseteq \Delta Q$ pues $kx = \delta(y)x = (\delta(y)y)y^{-1}x \in \Delta Q$. Además $\Delta Q \subseteq K \rtimes Q$ pues si $\delta(x) \in K$ para todo $x \in Q$. Recíprocamente, si $k \in K$ y $x \in Q$ existen $y, z \in Q$ tales que $kx = \delta(y)yz$; en particular, por la unicidad de la escritura de $K \rtimes Q$, $k = \delta(y)$. \square

Un caso importante de grupos que admiten factorización es el siguiente:

Definición 25.14. Un grupo G admite una **factorización triple** si tiene subgrupos A, B y M tales que $G = MA = MB = AB$ y $A \cap M = B \cap M = \{1\}$.

Una consecuencia inmediata del teorema de Sysak:

Corolario 25.15. Supongamos que el grupo Q actúa por automorfismos en K . Sea $\delta \in \text{Der}(Q, K)$ sobreyectivo. Entonces $G = K \rtimes Q$ admite una factorización triple.

Otra consecuencia:

xca:kerlcocycle

Ejercicio 25.16. Sea $\delta \in \text{Der}(Q, K)$.

- 1) Demuestre que δ es inyectiva si y sólo si $\ker \delta = \{1\}$.
- 2) Si δ es biyectivo, demuestre que K admite un complemento Δ en $K \rtimes Q$ tal que $K \rtimes Q = K \rtimes \Delta = \Delta Q$ y $Q \cap \Delta = \{1\}$.

Capítulo 26

El teorema de Schur–Zassenhaus

lemma:1cocycle

Lema 26.1. Si $\varphi: G \rightarrow N$ es un 1-cociclo con núcleo K entonces $\varphi(x) = \varphi(y)$ si y sólo si $xK = yK$. En particular, $(G : K) = |\varphi(G)|$.

Demostración. Si $\varphi(x) = \varphi(y)$ entonces, como

$$\varphi(x^{-1}y) = \varphi(x^{-1})(x^{-1} \cdot \varphi(y)) = \varphi(x^{-1})(x^{-1} \cdot \varphi(x)) = \varphi(x^{-1}x) = \varphi(1) = 1,$$

tenemos $xK = yK$. Recíprocamente, si $x^{-1}y \in K$, entonces, como

$$1 = \varphi(x^{-1}y) = \varphi(x^{-1})(x^{-1} \cdot \varphi(y)),$$

tenemos que $\varphi(y) = x \cdot \varphi(x^{-1})^{-1}$. De acá obtenemos $\varphi(x) = \varphi(y)$.

La segunda afirmación resulta ahora evidente pues φ es constante en cada coclase de K y toma $(G : K)$ valores distintos. \square

lemma:d

Lema 26.2. Sea G un grupo finito, N un subgrupo normal abeliano de G y S, T, U transversales de N en G . Sea

$$d(S, T) = \prod st^{-1} \in N,$$

donde el producto se hace sobre todos los $s \in S$ y $t \in T$ tales que $sN = tN$. Valen las siguientes afirmaciones:

- 1) $d(S, T)d(T, U) = d(S, U)$.
- 2) $d(gS, gT) = gd(S, T)g^{-1}$ para todo $g \in G$.
- 3) $d(nS, S) = n^{(G:N)}$ para todo $n \in N$.

Demostración. Si $s \in S$, $t \in T$, $u \in U$ con $sN = tN = uN$ entonces, como N es abeliano y $(st^{-1})(tu^{-1}) = su^{-1}$,

$$d(S, T)d(T, U) = \prod (st^{-1})(tu^{-1}) = \prod su^{-1} = d(S, U).$$

Como $sN = tN$ si y sólo si $gsN = gtN$ para todo $g \in G$,

$$g \left(\prod st^{-1} \right) g^{-1} = \prod g st^{-1} g^{-1} = \prod (gs)(gt)^{-1} = d(gS, gT).$$

Por último, como N es normal, $nsN = sN$ para todo $n \in N$. Luego

$$d(nS, S) = \prod (ns)s^{-1} = n^{(G:N)}. \quad \square$$

SchurZassenhaus:abeliano

Teorema 26.3 (Schur–Zassenhaus). *Sea G un grupo finito y sea N un subgrupo normal abeliano de G . Si $|N|$ y $(G : N)$ son coprimos, N se complementa en G . Si N se complementa en G , todos los complementos son conjugados.*

Demostración. Sea T un transversal de N en G . Sea $\theta : G \rightarrow N$, $\theta(g) = d(gT, T)$. Como N es abeliano, el lema 26.2 implica que θ es un 1-cociclo, donde G actúa en N por conjugación:

$$\begin{aligned} \theta(xy) &= d(xyT, T) = d(xyT, xT)d(xT, T) \\ &= (xd(yT, T)x^{-1})d(xT, T) = (x \cdot \theta(y))\theta(x). \end{aligned}$$

Afirmación. $\theta|_N : N \rightarrow N$ es sobreyectiva.

Si $n \in N$, el lema 26.2 implica que $\theta(n) = d(nT, T) = n^{(G:N)}$. Pero como los números $|N|$ y $(G : N)$ son coprimos, existen $r, s \in \mathbb{Z}$ tales que $r|N| + s(G : N) = 1$. Luego

$$n = n^{r|N| + s(G:N)} = (n^s)^{(G:N)} = \theta(n^s).$$

Sea $H = \ker \theta$. Vamos a demostrar que H es un complemento para N . Por el ejercicio ??, H es un subgrupo de G . Como

$$|N| = |\theta(G)| = (G : H)$$

por el lema 26.1, se concluye que $|H|$ divide a $(G : N)$. Como $N \cap H$ es un subgrupo de N y de H , entonces $N \cap H = 1$ pues $|N|$ y $(G : N) = |H|$ son coprimos. Como $|NH| = |N||H| = |G|$, se concluye que $G = NH$ y entonces H es un complemento para N .

Veamos ahora que dos complementos para N son conjugados. Sea K un complemento de N en G . Como $NK = G$ y $N \cap K = 1$, K es un transversal para N . Sea $m = d(T, K) \in N$. Como $\theta|_N$ es sobreyectiva, existe $n \in N$ tal que $\theta(n) = m$. Por el lema 26.2, para todo $k \in K$ se tiene

$$kmk^{-1} = kd(T, K)k^{-1} = d(kT, kK) = d(kT, K) = d(kT, T)d(T, K) = \theta(k)m,$$

y luego $\theta(k) \in N$. Entonces, como N es abeliano, $\theta(n^{-1}) = m^{-1}$ y luego

$$\begin{aligned} \theta(nkn^{-1}) &= \theta(n)n\theta(kn^{-1})n^{-1} = m\theta(kn^{-1}) \\ &= m\theta(k)k\theta(n^{-1})k^{-1} = m\theta(k)km^{-1}k^{-1} = 1. \end{aligned}$$

Queda demostrado entonces que $nKn^{-1} \subseteq H = \ker \theta$. Como $|K| = (G : N) = |H|$, se concluye que $nKn^{-1} = H$. \square

En el siguiente teorema vemos que no es necesario suponer que el subgrupo normal N es abeliano.

theorem:SchurZassenhaus

Teorema 26.4 (Schur–Zassenhaus). *Sea G un grupo finito y sea N un subgrupo normal de G . Si $|N|$ y $(G : N)$ son coprimos entonces N se complementa en G .*

Demostración. Procederemos por inducción en $|G|$. Si existe un subgrupo propio K de G tal que $NK = G$ entonces, como $(K : K \cap N) = (G : N)$ es coprimo con $|N|$, es también coprimo con $|K \cap N|$. Como además $K \cap N$ es normal en K , por hipótesis inductiva, $K \cap N$ se complementa en K , y luego existe un subgrupo H de K tal que $|H| = (K : K \cap N) = (G : N)$.

Supongamos entonces que no existe un subgrupo propio K de G tal que $NK = G$. Podemos suponer que $N \neq 1$ (de lo contrario, basta tomar G como complemento de N en G). Como N está contenido en todo subgrupo maximal de G (pues si existe un maximal $M \subsetneq G$ tal que $N \not\subseteq M$ entonces $NM = G$), se tiene que $N \subseteq \Phi(G)$. Por el teorema de Frattini 22.11, $\Phi(G)$ es nilpotente y luego N es nilpotente; en particular, $Z(N) \neq 1$. Sea $\pi : G \rightarrow G/Z(N)$ el morfismo canónico. Como N es normal en G y $Z(N)$ es característico en N , $Z(N)$ es normal en G . Además

$$(\pi(G) : \pi(N)) = \frac{|\pi(G)|}{|\pi(N)|} = \frac{|G/Z(N)|}{|N/N \cap Z(N)|} = (G : N)$$

es coprimo con $|N|$, y entonces es también coprimo con $|\pi(N)|$. Por hipótesis inductiva, $\pi(N)$ admite un complemento en $G/Z(N)$, digamos $\pi(K)$ para algún subgrupo K de G . Luego $G = NK$ pues $\pi(G) = \pi(N)\pi(K) = \pi(NK)$. Como entonces $K = G$ (pues sabíamos que no existe K tal que $G = NK$), $\pi(N)$ es abeliano pues

$$\pi(Z(N)) = \pi(N) \cap \pi(K) = \pi(N) \cap \pi(G) = \pi(N).$$

Luego $N \subseteq Z(N)$ es abeliano y entonces, por el teorema 26.3, el subgrupo N admite un complemento. \square

urZassenhaus:conjugacion

Teorema 26.5. *Sea G un grupo finito y sea N un subgrupo normal de G tal que $|N|$ y $(G : N)$ son coprimos. Si N es resoluble o G/N es resoluble, todos los complementos de N en G son conjugados.*

Demostración. Sea G un contraejemplo minimal, es decir: existen complementos K_1 y K_2 a N en G tales que K_1 y K_2 no son conjugados, y $|G|$ toma el menor valor posible.

Afirmación. Todo subgrupo U de G satisface las hipótesis del teorema con respecto al subgrupo normal $U \cap N$.

Como N es normal en G , $U \cap N$ es normal en U . Además $|U \cap N|$ y $(U : U \cap N)$ son coprimos pues $|U \cap N|$ divide a $|N|$ y $(U : U \cap N) = (UN : N)$ divide a $(G : N)$. Si G/N es resoluble, entonces $U/U \cap N$ es resoluble pues $U/U \cap N$ es isomorfo a un subgrupo de G/N . Si N es resoluble, $U \cap N$ es resoluble.

Afirmación. Si existe un subgrupo normal L de G tal que $\pi(N)$ es normal en $\pi(G)$, donde $\pi: G \rightarrow G/L$ es el morfismo canónico, entonces $\pi(G)$ satisface las hipótesis del teorema con respecto a $\pi(N)$. En este caso, si H es un complemento para N en G , $\pi(H)$ es un complemento para $\pi(N)$ en $\pi(G)$.

Si N es resoluble, $\pi(N)$ es resoluble. Si G/N es resoluble, $\pi(G)/\pi(N) \simeq G/NL$ es resoluble. Además $(\pi(G) : \pi(N)) = \frac{|G/L|}{|N/N \cap L|}$ divide a $(G : N)$.

Si H es un complemento para N en G , $|\pi(H)|$ y $|\pi(N)|$ son coprimos. Luego $\pi(H)$ es un complemento para $\pi(N)$ pues $\pi(G) = \pi(N)\pi(H) = \pi(NH)$ y la intersección $\pi(N) \cap \pi(H)$ es trivial.

Afirmación. N es minimal-normal en G .

Sea $M \neq 1$ normal tal que $M \subseteq N$. Sea $\pi: G \rightarrow G/M$ el morfismo canónico. Vimos que $\pi(G)$ satisface las hipótesis del teorema con respecto al subgrupo normal $\pi(N)$. Por la minimalidad de G , existe $x \in G$ tal que $\pi(xK_1x^{-1}) = \pi(K_2)$. Sabemos que el subgrupo $U = MK_2$ también satisface las hipótesis del teorema con respecto al subgrupo normal $U \cap N$. Como además $xK_1x^{-1} \cup K_2 \subseteq U$, podemos concluir que xK_1x^{-1} y K_2 complementan a $U \cap N$ en U . Luego $MK_2 = G$ pues xK_1x^{-1} y K_2 no son conjugados y G es minimal. Esto implica que $M = N$ pues

$$\frac{|K_2|}{|M \cap K_2|} = |MK_2| = |G| = |NK_2| = |N||K_2|.$$

Afirmación. N no es resoluble y G/N es resoluble.

En caso contrario, por el lema 19.8 tendríamos que N es abeliano ya que N es minimal-normal, y luego tendríamos una contradicción al utilizar el teorema 26.3 que implicaría que K_1 y K_2 son conjugados.

Sea $p: G \rightarrow G/N$ el morfismo canónico y sea S tal que $p(S)$ minimal-normal en $p(G) = G/N$. Por el lema 19.8, $p(S)$ un p -grupo para algún primo p . Como $G = NK_1 = NK_2$ y $N \subseteq S$, el lema de Dedekind 22.6 implica que

$$S = N(S \cap K_1) = N(S \cap K_2).$$

Luego $S \cap K_1$ y $S \cap K_2$ complementan a N en S . En particular $S \cap K_1$ y $S \cap K_2$ son p -subgrupos de Sylow de S pues

$$|S \cap K_1| = |S : N| = |S \cap K_2|,$$

y p no divide a $|N|$. Por el teorema de Sylow, existe $s \in S$ tal que

$$S \cap sK_1s^{-1} = S \cap K_2.$$

En particular $S \neq G$ gracias a la minimalidad de G . Sea

$$L = S \cap K_2 = S \cap sK_1s^{-1} \neq 1.$$

Como S es normal en G , $sK_1s^{-1} \cup K_2 \subseteq N_G(L)$ (pues L es normal en sK_1s^{-1} y en K_2). Los subgrupos $sK_1s^{-1} \subseteq N_G(L)$ y $K_2 \subseteq N_G(L)$ complementan a $N \cap N_G(L)$ en $N_G(L)$, y luego $N_G(L) = G$ por la minimalidad de G (si $N_G(L) \neq G$ entonces sK_1s^{-1} y K_2 serían conjugados en G por serlo en $N_G(L)$). Luego L es normal en G .

Sea $\pi_L: G \rightarrow G/L$ el morfismo canónico. Como $\pi_L(K_1)$ y $\pi_L(K_2)$ complementan a $\pi_L(N)$ en $\pi_L(G)$, la minimalidad de $|G|$ implica que existe $g \in G$ tal que $\pi_L(gK_1g^{-1}) = \pi_L(K_2)$, es decir: existe $g \in G$ tal que $(gK_1g^{-1})L = K_2L$. Luego $gK_1g^{-1} \cup K_2 \subseteq \langle K_2, L \rangle = K_2$ pues $L \subseteq K_2$. Tenemos entonces que $gK_1g^{-1} = K_2$, una contradicción por la minimalidad de G . \square

Por el teorema de Feit–Thompson, no es necesario suponer que N o G/N es resoluble en el teorema anterior. Como todo grupo de orden impar es resoluble y $|N|$ es coprimo con $(G : N)$, alguno de estos grupos tiene orden impar.

Veamos una aplicación a grupos resolubles finitos.

theorem:solvable_maximal

Teorema 26.6. *Sea G un grupo finito resoluble y sea p un primo que divide al orden de G . Entonces existe un maximal M de índice una potencia de p .*

Demostración. Procederemos por inducción en $|G|$. Si G es un p -grupo, el resultado es verdadero. Veamos el caso general. Sea p un primo que divide al orden de G , sea N un subgrupo minimal-normal y sea $\pi: G \rightarrow G/N$ el morfismo canónico. Como G es resoluble, Por el lema 19.8, N es un q -grupo para algún primo q . Como G/N es resoluble, si p divide a $(G : N)$ entonces, por hipótesis inductiva, G/N tiene un subgrupo maximal M_1 de índice una potencia de p . Por el teorema de la correspondencia, $M = \pi^{-1}(M_1)$ es un subgrupo maximal de G de índice una potencia de p . Si p no divide a $(G : N)$, p divide a $|N|$ y luego $N \in \text{Syl}_p(G)$. Como N es normal en G y $|N|$ es coprimo con $|G/N|$, el teorema de Schur–Zassenhaus 26.4 implica que existe un complemento K a N en G , es decir $G = NK$ y $N \cap K = 1$. Sea M un subgrupo maximal que contiene a K . Entonces $(G : M)$ es una potencia de p . \square

Veamos ahora una aplicación a grupos super-resolubles finitos.

Definición 26.7. Un grupo finito G se dice **lagrangiano** si para cada d que divide a $|G|$ existe un subgrupo de G de orden d .

El grupo \mathbb{A}_4 no es lagrangiano pues no tiene subgrupos de orden seis.

Teorema 26.8. *Todo grupo finito super-resoluble es lagrangiano.*

Demostración. Sea p un primo que divide al orden de G . Como los subgrupos de un grupo súper-resoluble son súper-resolubles, basta ver que existe un subgrupo índice p . Como G es resoluble, existe un subgrupo maximal M de índice p^α por el teorema 26.6. Como los maximales de súper-resolubles tienen índice primo (teorema 24.12), se concluye que $\alpha = 1$. \square

Capítulo 27

Extensiones y cohomología

Definición 27.1. Sea G un grupo. Un G -módulo es un grupo abeliano A con una acción por automorfismos de G .

En esta sección G es un grupo y A es un G -módulo. El grupo A será escrito aditivamente.

Definición 27.2. Sea $n \geq 0$. Una **cocadena** de grado n (o n -cocadena) de G con valores en A es una función $f: G \times \cdots \times G \rightarrow A$, $(s_1, \dots, s_n) \mapsto f(s_1, \dots, s_n)$.

El conjunto $C^n(G, A)$ de n -cocadenas de G con valores en A es un grupo abeliano.

Definición 27.3. Sea $f \in C^n(G, A)$. Se define el **coborde** de f como el elemento $df \in C^{n+1}(G, A)$ dado por

$$df(s_1, \dots, s_{n+1}) = s_1 \cdot f(s_2, \dots, s_{n+1}) + \sum_{i=1}^n (-1)^i f(s_1, \dots, s_{i-1}, s_i s_{i+1}, s_{i+2}, \dots, s_{n+1}) + (-1)^{n+1} f(s_1, \dots, s_n).$$

Ejemplo 27.4. Veamos la función $d: C^0(G, A) \rightarrow C^1(G, A)$. Si $a \in C^0(G, A) = A$ entonces

$$da(s) = s \cdot a - a.$$

Luego $da = 0$ si y sólo si $s \cdot a = 0$ para todo $s \in G$.

Ejemplo 27.5. Veamos ahora la función $d: C^1(G, A) \rightarrow C^2(G, A)$. Si $f \in C^1(G, A)$ entonces

$$df(s, t) = s \cdot f(t) - f(st) + f(s).$$

Ejemplo 27.6. Veamos ahora la función $d: C^2(G, A) \rightarrow C^3(G, A)$. Si $f \in C^2(G, A)$ entonces

$$df(u, v, w) = u \cdot f(v, w) - f(uv, w) + f(u, vw) - f(u, v).$$

lemma:dd=0

Lema 27.7. La composición $C^n(G, A) \xrightarrow{d} C^{n+1}(G, A) \xrightarrow{d} C^{n+2}(G, A)$ es cero.

La demostración del lema anterior es fácil pero tediosa, por eso queda como ejercicio.

Definición 27.8. Sea f una cocadena f de grado n . Se dice que f es un **cociclo** de grado n si $df = 0$. Denotaremos por $Z^n(G, A)$ al conjunto de n -cociclos de G en A . Se dice que f es un **coborde** de grado n si existe una cocadena g de grado $(n-1)$ tal que $f = dg$. Denotaremos por $B^n(G, A)$ al conjunto de n -cobordes de G en A .

Obviamente $Z^n(G, A)$ es un grupo abeliano y $B^n(G, A) \subseteq Z^n(G, A)$.

Definición 27.9. El n -ésimo **grupo de cohomología** de G con valores en A es el grupo abeliano

$$H^n(G, A) = Z^n(G, A) / B^n(G, A).$$

xca:H0

Ejercicio 27.10. Demuestre que $H^0(G, A) = A^G$, donde

$$A^G = \{a \in A : s \cdot a = a \text{ para todo } s \in G\}.$$

Ejemplo 27.11. $f \in Z^1(G, A)$ si y sólo si $f(st) = s \cdot f(t) + f(s)$ para todo $s, t \in G$. En particular, si G actúa trivialmente en A , $Z^1(G, A) = \text{hom}(G, A)$. Como en este caso $B^1(G, A) = 0$, se concluye que $H^1(G, A) \simeq \text{hom}(G, A)$.

Ejemplo 27.12. $f \in Z^2(G, A)$ si y sólo si f es un **factor**, es decir:

$$u \cdot f(v, w) - f(uv, w) + f(u, vw) - f(u, v) = 0 \quad (27.1)$$

eq:2cociclo

para todo $u, v, w \in G$.

Ejercicio 27.13. Sea $f \in Z^2(G, A)$ tal que $f(1, 1) = 0$. Demuestre que

$$f(1, x) = f(x, 1) = 0$$

para todo $x \in G$.

Definición 27.14. Sean $f, g \in Z^2(G, A)$. Se dice que f y g son **cohomólogos** si existe algún coborde h tal que $f - g = dh$.

Un factor $f \in Z^2(G, A)$ se dice **normalizado** si $f(1, 1) = 0$.

lemma:normalizado

Lema 27.15. Todo $f \in Z^2(G, A)$ es cohomólogo a un factor normalizado.

Demostración. Sea $\gamma: G \rightarrow A$ tal que $\gamma(1) = -f(1, 1)$. Sea $g = f + d\gamma$. Entonces $g \in Z^2(G, A)$, $g(1, 1) = 0$ y $dg = d(f + d\gamma) = df$ pues $d^2 = 0$. \square

theorem:|G|H^2=0

Teorema 27.16. Sea G un grupo finito y sea A un G -módulo. Entonces

$$|G|H^n(G, A) = 0.$$

Demostración. Sea $m = |G|$. Sea $f \in Z^n(G, A)$. Vamos a demostrar que mf es un coborde. Sea

$$F(s_1, \dots, s_{n-1}) = \sum_{s \in G} f(s_1, \dots, s_{n-1}, s).$$

Como $f \in Z^n(G, A)$,

$$0 = s_1 \cdot f(s_2, \dots, s_{n+1}) - f(s_1 s_2, s_3, \dots, s_{n+1}) + \dots + (-1)^n f(s_1, \dots, s_n s_{n+1}) + (-1)^{n+1} f(s_1, \dots, s_n).$$

Al sumar estas igualdades sobre todo $s_{n+1} \in G$ obtenemos

$$0 = s_1 \cdot F(s_2, \dots, s_n) - F(s_1 s_2, \dots, s_n) + \dots + (-1)^n F(s_1, \dots, s_{n-1}) + (-1)^{n+1} mf(s_1, \dots, s_n).$$

Luego $0 = dF(s_1, \dots, s_n) - (-1)^n mf(s_1, \dots, s_n)$, es decir $mf = d((-1)^n F)$. \square

corollary:a->|G|a

Corolario 27.17. Sea G un grupo finito y A un G -módulo. Si $a \mapsto |G|a$ es un automorfismo de A entonces $H^n(G, A) = 0$ para todo $n \geq 1$.

Demostración. Como la función $x \mapsto |G|x$ es un automorfismo de $C^n(G, A)$ que conmuta con d , induce un automorfismo $H^n(G, A) \rightarrow H^n(G, A)$, $x \mapsto |G|x$. Como $|G|H^n(G, A) = 0$ por el teorema 27.16, se concluye que $H^n(G, A) = 0$. \square

corollary:H^n=0

Corolario 27.18. Sea G un grupo finito y A un G -módulo. Si A es finito y de orden coprimo con $|G|$ entonces $H^n(G, A) = 0$ para todo $n \geq 1$.

Demostración. Como $|G|H^n(G, A) = 0$ por el teorema 27.16 y $a \mapsto |G|a$ es un automorfismo de A , $H^n(G, A)$ por el corolario 27.17. \square

Corolario 27.19. Sea G un grupo finito y A un G -módulo finitamente generado. Entonces $H^n(G, A)$ es finito para todo $n \geq 1$.

Demostración. Como $C^n(G, A)$ es finitamente generado, $H^n(G, A)$ es finitamente generado. Luego $H^n(G, A)$ es finito por ser un grupo abeliano finitamente generado y de torsión. \square

Extensiones abelianas

Definición 27.20. Un **morfismo** entre las extensiones

$$1 \rightarrow K \xrightarrow{l} G \xrightarrow{p} Q \rightarrow 1, \quad 1 \rightarrow K_1 \xrightarrow{l_1} G_1 \xrightarrow{p_1} Q_1 \rightarrow 1,$$

es una terna (α, β, γ) de morfismos tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccccc}
1 & \longrightarrow & K & \xrightarrow{\iota} & G & \xrightarrow{p} & Q \longrightarrow 1 \\
& & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\
1 & \longrightarrow & K_1 & \xrightarrow{\iota_1} & G_1 & \xrightarrow{p_1} & Q_1 \longrightarrow 1
\end{array}$$

Definición 27.21. Diremos que las extensiones

$$E: 1 \rightarrow K \xrightarrow{\iota} G \xrightarrow{p} Q \rightarrow 1, \quad E_1: 1 \rightarrow K_1 \xrightarrow{\iota_1} G_1 \xrightarrow{p_1} Q \rightarrow 1,$$

son **isomorfas** si existe un morfismo $(\alpha, \beta, \text{id})$ entre E y E_1 con α isomorfismo. Las extensiones E y E_1 se dirán **equivalentes** si $K = K_1$ y $(\text{id}, \beta, \text{id})$ es un isomorfismo entre E y E_1 .

xca:extensiones

Ejercicio 27.22. Demuestre que si $(\alpha, \beta, \text{id})$ es un isomorfismo de extensiones entonces β es un isomorfismo de grupos.

Definición 27.23. Diremos que las extensiones

$$1 \rightarrow K \xrightarrow{\iota} G \xrightarrow{p} Q \rightarrow 1, \quad 1 \rightarrow K_1 \xrightarrow{\iota_1} G_1 \xrightarrow{p_1} Q \rightarrow 1,$$

son **equivalentes** si existe un morfismo $(\text{id}, \beta, \text{id})$ entre esas extensiones.

Definición 27.24. Un **dato** es un par (Q, K) , donde Q es un grupo y K es Q -módulo. Se dice que un grupo G **realiza** el dato (Q, K) si G es una extensión de K por Q y para todo levantamiento $\ell: Q \rightarrow G$ se tiene

$$x \cdot a = \ell(x)a\ell(x)^{-1}, \quad a \in K, x \in Q.$$

Definición 27.25. Sea Q un grupo y sea K un Q -módulo. Sea $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$ una extensión de K por Q que realiza el dato (K, Q) y sea $\ell: Q \rightarrow G$ un levantamiento tal que $\ell(1) = 1$. Un **factor** para ℓ es una función $f: Q \times Q \rightarrow K$ tal que

$$\ell(x)\ell(y) = f(x, y)\ell(xy) \tag{27.2}$$

eq:ell

para todo $x, y \in Q$.

Lema 27.26. Sea Q un grupo y sea K un Q -módulo. Sea $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$ una extensión de K por Q que realiza el dato (K, Q) . Si f es un factor para ℓ entonces

$$f(1, x) = f(x, 1) = 1, \tag{27.3}$$

eq:f(1x)

$$f(x, y)f(xy, z) = (x \cdot f(y, z))f(x, yz) \tag{27.4}$$

eq:fcocycle

para todo $x, y, z \in Q$.

Demostración. Si hacemos $x = 1$ en (27.3) obtenemos $1 = f(1, y)$. De la misma forma se obtiene la otra igualdad. Para demostrar la igualdad (27.4) calculamos

$$(\ell(x)\ell(y))\ell(z) = (f(x, y)\ell(xy))\ell(z) = f(x, y)(\ell(xy)\ell(z)) = f(x, y)f(xy, z)\ell(xyz).$$

Por otro lado, como la extensión realiza el dato (K, Q) ,

$$\begin{aligned}\ell(x)(\ell(y)\ell(z)) &= \ell(x)(f(y, z)\ell(yz)) \\ &= (x \cdot f(y, z))\ell(x)\ell(yz) = (x \cdot f(y, z))f(x, yz)\ell(xyz).\end{aligned}$$

La igualdad (27.4) se obtiene al observar que el producto de G es asociativo. \square

lemma : $G(K, Q, f)$

Lema 27.27. Sea Q un grupo y sea K un Q -módulo. Sea $f: Q \times Q \rightarrow K$ una función que satisface (27.3) y (27.4). Entonces existe una extensión $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$ de K por Q que realiza el dato (K, Q) y existe un levantamiento $\ell: Q \rightarrow G$ cuyo factor es f .

Demostración. Sea $G = K \times Q$ con el producto

$$(a, x)(b, y) = (a(x \cdot b)f(x, y), xy).$$

Veamos que el producto es asociativo:

$$\begin{aligned}((a, x)(b, y))(c, z) &= (a(x \cdot b)f(x, y), xy)(c, z) \\ &= (a(x \cdot b)f(x, y)((xy) \cdot c))f(xy, z), xyz)\end{aligned}$$

Por otro lado

$$\begin{aligned}(a, x)((b, y)(c, z)) &= (a, x)(b(y \cdot c)f(y, z), yz) \\ &= (a(x \cdot (b(y \cdot c)f(y, z))f(x, yz), xyz) \\ &= (a(x \cdot b)(xy) \cdot c)(x \cdot f(y, z))f(x, yz), xyz).\end{aligned}$$

Es fácil verificar que el neutro es $(1, 1)$ y el inverso de (a, x) es

$$(a, x)^{-1} = (x^{-1} \cdot (f(x, x^{-1})a)^{-1}, x^{-1}).$$

Sea $\ell: Q \rightarrow G$ un levantamiento. Si $x \in Q$ existe $b \in K$ tal que $\ell(x) = (b, x)$. Veamos que la extensión realiza el dato (K, Q) . Como $f(x, 1) = 1$ y K es abeliano,

$$\begin{aligned}\ell(x)(a, 1)\ell(x)^{-1} &= (b, x)(a, 1)(b, x)^{-1} \\ &= (b(x \cdot a)f(x, 1), x)(x^{-1} \cdot (f(x, x^{-1})b)^{-1}, x^{-1}) \\ &= (b(x \cdot a)b^{-1}f(x, x^{-1})^{-1}f(x, x^{-1}), 1) \\ &= (x \cdot a, 1).\end{aligned}$$

Por último, para ver que existe un levantamiento con factor f basta considerar $\ell: Q \rightarrow G$, $\ell(x) = (1, x)$ pues

$$\ell(x)\ell(y)(\ell(xy)^{-1} = (1, x)(1, y)(1, xy)^{-1} = (f(x, y), 1). \quad \square$$

Si Q es un grupo, K es un Q -módulo y $f: Q \times Q \rightarrow K$ es una función que satisface (27.3) y (27.4). El grupo G del lema 27.27 será denotado por $G(K, Q, f)$.

lemma:existe_f

Lema 27.28. Sea Q un grupo y sea K un Q -módulo. Sea $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$ una extensión de K por Q que realiza el dato (K, Q) . Entonces existe un factor $f: Q \times Q \rightarrow K$ tal que $G \simeq G(K, Q, f)$.

Demostración. Sea $\ell: Q \rightarrow G$ un levantamiento y sea f su factor. Como G es unión disjunta de coclases

$$G = \bigcup_{x \in Q} K\ell(x),$$

para cada $g \in G$ existen únicos $a \in K$ y $x \in Q$ tales que $g = a\ell(x)$. Queda entonces bien definida una función biyectiva $\phi: G \rightarrow G(K, Q, f)$, $a\ell(x) \mapsto (a, x)$. Veamos que ϕ es un morfismo de grupos:

$$\begin{aligned} \phi(a\ell(x)b\ell(y)) &= \phi(a\ell(x)b\ell(x)^{-1}\ell(x)\ell(y)) \\ &= \phi(a\ell(x)b\ell(x)^{-1}f(x, y)\ell(xy)) \\ &= \phi(a(x \cdot b)f(x, y)\ell(xy)) \\ &= (a(x \cdot b)f(x, y), xy) \\ &= \phi(a\ell(x))\phi(b\ell(y)). \end{aligned} \quad \square$$

lemma:coborde

Lema 27.29. Sean Q un grupo, K un Q -módulo y $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$ una extensión de K por Q que realiza el dato (K, Q) . Para $j \in \{1, 2\}$ sea $\ell_j: Q \rightarrow G$ un levantamiento con factor f_j tal que $\ell_j(1) = 1$. Entonces existe $\gamma: Q \rightarrow K$ tal que $\gamma(1) = 1$ y

$$f_2(x, y) = \gamma(x)(x \cdot \gamma(y))f_1(x, y)\gamma(xy)^{-1}$$

para todo $x, y \in Q$.

Demostración. Como $\ell_1(x)$ y $\ell_2(x)$ están en la misma coclase de K , existe $\gamma(x) \in K$ tal que $\ell_2(x) = \gamma(x)\ell_1(x)$. Como $\ell_1(1) = \ell_2(1) = 1$, $\gamma(1) = 1$. Además

$$\begin{aligned} f_2(x, y)\ell_2(xy) &= \ell_2(x)\ell_2(y) = \gamma(x)\ell_1(x)\gamma(y)\ell_1(y) \\ &= \gamma(x)\ell_1(x)\gamma(y)\ell_1(x)^{-1}\ell_1(x)\ell_1(y) \\ &= \gamma(x)(x \cdot \gamma(y))f_1(x, y)\ell_1(xy) = \gamma(x)(x \cdot \gamma(y))f_1(x, y)\gamma(xy)^{-1}\ell_2(xy), \end{aligned}$$

que implica lo que se quería demostrar. \square

Definición 27.30. Sean Q un grupo y K un Q -módulo. Una función $g: Q \times Q \rightarrow K$ se dice un **coborde** si existe una función $\gamma: Q \rightarrow K$ con $\gamma(1) = 1$ tal que

$$g(x, y) = (x \cdot \gamma(y))\gamma(xy)^{-1}\gamma(x)$$

para todo $x, y \in Q$.

lemma:equivalencia

Lema 27.31. Sean Q un grupo y K un Q -módulo. Dos extensiones G_1 y G_2 de K por Q que realizan el dato (K, Q) son equivalentes si y sólo existe un factor f_1 de G_1 y un factor f_2 de G_2 tales que $f_1f_2^{-1}$ es un coborde.

Demostración. Para cada $j \in \{1, 2\}$ sea $\ell_j: Q \rightarrow G$ un levantamiento con factor f_j y tal que $\ell_j(1) = 1$. Como G es unión disjunta de coclases

$$G = \bigcup_{x \in Q} K\ell_1(x)$$

todo $g_1 \in G_1$ se escribe unívocamente como $g_1 = a\ell_1(x)$ para $a \in K$ y $x \in Q$. Sea $\phi: G_1 \rightarrow G_2$, $a\ell_1(x) \mapsto a\gamma(x)\ell_2(x)$. Es evidente que ϕ hace conmutar al diagrama

$$\begin{array}{ccccccc} 1 & \longrightarrow & K & \longrightarrow & G_1 & \xrightarrow{p_1} & Q \longrightarrow 1 \\ & & \parallel & & \downarrow \phi & & \parallel \\ 1 & \longrightarrow & K & \longrightarrow & G_1 & \xrightarrow{p_2} & Q_1 \longrightarrow 1 \end{array} \quad (27.5) \quad \boxed{\text{eq:diagrama}}$$

Veamos que ϕ es morfismo. Por un lado tenemos

$$\phi(a\ell_1(x)b\ell_1(y)) = \phi(a(x \cdot b)f_1(x, y)\ell_1(xy)) = a(x \cdot b)f_1(x, y)\gamma(xy)\ell_2(xy).$$

Por otro lado, se tiene

$$\begin{aligned} \phi(a\ell_1(x))\phi(b\ell_1(y)) &= a\gamma(x)\ell_2(x)b\gamma(y)\ell_2(y) \\ &= a\gamma(x)(x \cdot b)\ell_2(x)\gamma(y)\ell_2(y) \\ &= a\gamma(x)(x \cdot b)(x \cdot \gamma(y))\ell_2(x)\ell_2(y) \\ &= a\gamma(x)(x \cdot b)(x \cdot \gamma(y))f_2(x, y)\ell_2(xy) \\ &= a(x \cdot b)\gamma(x)(x \cdot \gamma(y))f_2(x, y)\ell_2(xy) \end{aligned}$$

pues K es abeliano. Por el lema 27.29, existe una función $\gamma: Q \rightarrow K$ con $\gamma(1) = 1$ y tal que $f_1(x, y) = \gamma(x)(x \cdot \gamma(y))f_2(x, y)\gamma(xy)^{-1}$ para todo $x, y \in Q$. Luego ϕ es morfismo de grupos.

Recíprocamente, supongamos que existe γ tal que el diagrama (27.5) conmuta. En particular, $\gamma(a) = a$ para todo $a \in K$ y la función $\phi\ell_1: Q \rightarrow G_2$ es un levantamiento pues $x = p_1\ell_1(x) = p_2\phi\ell_1(x)$ para todo $x \in Q$. Como

$$\phi\ell_1(x)\phi\ell_1(y) = \phi f_1(x, y)\phi\ell_1(xy) = f_1(x, y)\phi\ell_1(xy)$$

para todo $x, y \in Q$, f_1 es también un factor para la extensión G_2 . Si f_2 es un factor para G_2 , entonces $f_1f_2^{-1}$ es un coborde por el lema 27.29. \square

Ejemplo 27.32. Sea p un número primo impar. Sean $K = \langle a \rangle \simeq C_p$, $G = \langle g \rangle \simeq C_{p^2}$ y $Q = \langle gK \rangle = G/K \simeq C_p$. Veamos que las extensiones

$$\begin{array}{ccccccc} 1 & \longrightarrow & K & \xrightarrow{i_1} & G_1 & \xrightarrow{p_1} & Q \longrightarrow 1 \\ & & \parallel & & \downarrow \phi & & \parallel \\ 1 & \longrightarrow & K & \xrightarrow{i_2} & G_1 & \xrightarrow{p_2} & Q_1 \longrightarrow 1 \end{array}$$

donde $\iota_1(a) = g^p$, $\iota_2(a) = g^{2p}$ y $p_1(g) = p_2(g) = gK$, no son equivalentes. Si existe ϕ entonces $\phi(g^p) = \phi\iota_1(a) = \iota_2(a) = g^{2p}$. Esto implica que $\phi(g) = g^2$ y luego $g \in K$ pues $gK = p_1(g) = p_2\phi(g) = g^2K$, una contradicción.

Sea Q un grupo y sea K un Q -módulo. Sea $E(Q, K)$ el conjunto de clases de equivalencia de extensiones $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$ que realizan el dato (Q, K) .

er:extensiones_abelianas

Teorema 27.33 (Schreier). *Sean Q un grupo y K un Q -módulo. Existe una correspondencia biyectiva entre $H^2(Q, K)$ y el conjunto $E(Q, K)$ de clases de equivalencia de extensiones que realizan el dato (Q, K) . Bajo esta correspondencia, el factor nulo se corresponde con la clase de equivalencia de extensiones que se parten.*

Demostración. Sea $[G]$ la clase de equivalencia de $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$. Sea $\phi: H^2(Q, K) \rightarrow E(Q, K)$ dado por $f + B^2(Q, K) \mapsto [G(K, Q, f)]$, donde $[G(K, Q, f)]$ es la clase de una extensión que realiza el dato (Q, K) (existe gracias al lema 27.27). El lema 27.31 implica que ϕ está bien definida y es una función inyectiva. La función ϕ es sobreyectiva pues el lema 27.28 implica que si $[G] \in E(Q, K)$ entonces $[G] = [G(K, Q, f)] = \phi(f + B^2(Q, K))$ para algún f . \square

Como aplicación del teorema de Schreier podemos dar una demostración breve de la existencia del complemento en el teorema de Schur–Zassenhaus 26.3. Para $Q = G/N$ consideramos la extensión $1 \rightarrow N \rightarrow G \rightarrow Q \rightarrow 1$. Como $|N|$ y $|Q|$ son coprimos, $H^2(Q, N) = 0$ por el corolario 27.18. Por el teorema de Schreier 27.33, $E(Q, N)$ contiene un único elemento y luego la extensión $1 \rightarrow N \rightarrow G \rightarrow Q \rightarrow 1$ se parte.

Capítulo 28

Teoría de Hall para grupos resolubles

Hall

Sea G un grupo finito y sea π un conjunto de números primos. Diremos que G es un π -grupo si todo primo que divide a $|G|$ pertenece a π . Obviamente un π -subgrupo de G es un subgrupo de G que además es un π -grupo. Un π -número es un entero tal que sus divisores primos están en π . El complemento de π en el conjunto de los números primos será denotado por π' . Luego un π' -número será un entero no divisible por los primos de π .

Definición 28.1. Sea π un conjunto de números primos. Un subgrupo H de G se dice un **π -subgrupo de Hall** si H es π -subgrupo de G y el índice $(G : H)$ es un π' -número.

theorem:HallE

Teorema 28.2 (Hall). *Sea π un conjunto de primos y sea G un grupo finito resoluble. Entonces G tiene un π -subgrupo de Hall.*

Demostración. Supongamos que G tiene orden $nm > 1$ con $(n : m) = 1$. Demostraremos por inducción en $|G|$ que existe un subgrupo de orden m . Sea K un subgrupo de G minimal-normal. Sea $\pi : G \rightarrow G/K$ el morfismo canónico. Como G es resoluble, K es un p -grupo por el lema 19.8.

Hay dos casos a considerar. Supongamos primero que p divide a m . Como $|G/K| < |G|$, por hipótesis inductiva y por la correspondencia, existe un subgrupo J de G que contiene a K tal que $\pi(J)$ es un subgrupo de $\pi(G) = G/K$ de orden $m/|K|$. Entonces J tiene orden m pues

$$m/|K| = |\pi(J)| = \frac{|J|}{|K \cap J|} = (J : K).$$

Supongamos ahora que p no divide a m . Por hipótesis inductiva y por la correspondencia, existe un subgrupo H de G que contiene a K tal que $\pi(H)$ es un subgrupo de G/K de orden m . Como $|H| = m|K|$, K es normal en H y $|K|$ es coprimo con $|H : K|$, el teorema de Schur–Zassenhaus 26.4 implica que existe un complemento J de K en H . Luego J es un subgrupo de G de orden $|J| = m$. \square

Ejemplo 28.3. El grupo \mathbb{A}_5 contiene un $\{2, 3\}$ -subgrupo de Hall isomorfo a \mathbb{A}_4 .

Ejemplo 28.4. El grupo simple $\text{PSL}_3(2)$ de orden 168 no contiene $\{2, 7\}$ -subgrupos de Hall.

El teorema 28.2 dice que para todo conjunto de primos π todo grupo finito contiene π -subgrupos de Hall.

theorem:HallC

Teorema 28.5 (Hall). *Sea G un grupo finito resoluble y sea π un conjunto de primos. Todos los π -subgrupos de Hall de G son conjugados.*

Demostración. Podemos suponer que $G \neq 1$. Procederemos por inducción en $|G|$. Sean H y K dos π -subgrupos de Hall de G . Sea M un subgrupo de G minimal-normal y sea $\pi: G \rightarrow G/M$ el morfismo canónico. Como G es resoluble, el lema 19.8 implica que M es un p -grupo para algún primo p . Como $\pi(H)$ y $\pi(K)$ son π -subgrupos de Hall de G/M , los subgrupos $\pi(H)$ y $\pi(K)$ son conjugados en G/M . Luego existe $g \in G$ tal que $gHMc^{-1} = KM$.

Hay dos casos a considerar. Supongamos primero que $p \in \pi$. Como $|HM|$ y $|KM|$ son π -números y $|H| = |K|$ es el mayor π -número que divide al orden de G , se concluye que $H = HM$ y $K = KM$. En particular, $gHg^{-1} = K$.

Supongamos ahora que $p \notin \pi$. Es evidente que K complementa a M en KM pues $K \cap M = 1$. Veamos que gHg^{-1} complementa a M en KM : como M es normal en G ,

$$(gHg^{-1})M = gHMc^{-1} = KM,$$

y $gHg^{-1} \cap M = 1$ ya que $p \notin \pi$. Estos complementos tienen que ser conjugados por el teorema de Schur–Zassenhaus 26.5. \square

Corolario 28.6. *Sea G un grupo finito y sea N un subgrupo normal de G de orden n . Supongamos que N o G/N es resoluble. Si $|G : N| = m$ es coprimo con n y m_1 divide a m , todo subgrupo de G de orden m_1 está contenido en algún subgrupo de orden m .*

Demostración. Sea H un complemento para N en G . Entonces $|H| = m$. Sea H_1 subgrupo de G tal que $|H_1| = m_1$. Como n y m son coprimos, $m_1 = |H_1| = |H \cap NH_1|$ pues

$$\frac{|H||N||H_1|}{|H \cap NH_1|} = \frac{|H||NH_1|}{|H \cap NH_1|} = |H(NH_1)| = |G| = |NH| = |N||H|.$$

Como H_1 y $H \cap NH_1$ son complementos para N en NH_1 , ambos de orden coprimo con n , existe $g \in G$ tal que $H_1 = g(H \cap NH_1)g^{-1}$. Luego $H_1 \subseteq gHg^{-1}$ y entonces $|gHg^{-1}| = m$. \square

Capítulo 29

Sistemas de Sylow

Dado un grupo finito G escribimos $\pi(G) = \{p_1, \dots, p_k\}$ para denotar el conjunto de divisores primos de $|G|$.

Definición 29.1. Sea G un grupo finito y sea $\pi(G) = \{p_1, \dots, p_k\}$. Para cada $j \in \{1, \dots, k\}$ sea Q_j un p'_j -subgrupo de Hall de G . El conjunto $\{Q_1, \dots, Q_k\}$ se denomina un **sistema de Sylow** de G .

La teoría de Hall demuestra el siguiente teorema:

Teorema 29.2. Sea G un grupo finito. Entonces G es resoluble si y sólo si G admite un sistema de Sylow.

Demostración. Sea $\pi(G) = \{p_1, \dots, p_k\}$. Si G es resoluble, entonces por el teorema de Hall 28.2 aplicado al conjunto $\pi(G) \setminus \{p_j\}$, para cada $j \in \{1, \dots, k\}$ existe un p'_j -subgrupo de Hall H_j . Luego $\{H_1, \dots, H_k\}$ es un sistema de Sylow de G . La recíproca es consecuencia directa del teorema de Hall 19.14. \square

Recordemos que dos subgrupos A y B se dicen **permutables** si $AB = BA$.

Ejemplo 29.3. Si $A \subseteq N_G(B)$ entonces A y B son permutables.

Ejemplo 29.4. Sean $G = \mathbb{S}_4$, $A = \mathbb{S}_3$ y $B = \langle (1234) \rangle$. Entonces $AB = BA = G$ pero $A \not\subseteq N_G(B)$ y $B \not\subseteq N_G(A)$.

Ejercicio 29.5. Sean A_1, \dots, A_n subgrupos permutables dos a dos. Demuestre que $A_1 \cdots A_n$ es un subgrupo de G .

lemma:indices_coprimos

Lema 29.6. Sean H y K dos subgrupos de G de índices finitos y coprimos. Entonces $(G : H \cap K) = (G : H)(G : K)$.

Demostración. La función $G/H \cap K \rightarrow G/H \times G/K$, $x(H \cap K) \mapsto (xH, xK)$, está bien definida y es inyectiva; en particular $(G : H \cap K) \leq (G : H)(G : K)$. Como $(G : H \cap K) = (G : H)(H : H \cap K) = (G : K)(K : H \cap K)$ y los índices $(G : H)$ y $(G : K)$ son coprimos, $(G : H)(G : K)$ divide a $(G : H \cap K)$. Luego

$$(G : H \cap K) = (G : H)(G : K).$$

□

lemma:system=>basis

Lema 29.7. Sea $\{Q_1, \dots, Q_k\}$ un sistema de Sylow de un grupo finito resoluble G . Entonces $P_i = \cap_{j \neq i} Q_j$ es un p_i -subgrupo de Sylow y los P_j son permutables dos a dos.

Demostración. Sea π un conjunto de primos. Supongamos que $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Para cada j , $(G : Q_j) = p_j^{\alpha_j}$. Sea $Q = \cap_{p_i \notin \pi} Q_i$. Entonces Q es un π -subgrupo de Hall pues, por el lema 29.6, $(G : Q) = \prod_{p_i \notin \pi} p_i^{\alpha_i}$. En particular, si $\pi = \{p_i, p_j\}$ con $i \neq j$, el subgrupo $K = \cap_{k \notin \{i, j\}} Q_k$ es un π -subgrupo de Hall de orden $p_i^{\alpha_i} p_j^{\alpha_j}$. Como K contiene a $P_i \cup P_j$ y $|P_i P_j| = p_i^{\alpha_i} p_j^{\alpha_j}$, se concluye que $P_i P_j = P_j P_i = K$. □

Definición 29.8. Sea G un grupo finito. Una **base de Sylow** para G es un conjunto $\{P_1, \dots, P_k\}$ de subgrupos de Sylow de G , uno por cada primo p_j que divide a $|G|$, donde $P_i P_j = P_j P_i$ para todo $i \neq j$.

proposition:sistemas=bases

Proposición 29.9. Sea G un grupo finito resoluble. Existe una biyección entre el conjunto de sistemas de Sylow para G y el conjunto de bases de Sylow para G .

Demostración. Vimos en el lema 29.7 que todo sistema de Sylow $\{Q_1, \dots, Q_k\}$ nos da una base de Sylow $\{P_1, \dots, P_k\}$ para G , donde $P_i = \cap_{j \neq i} Q_j$. Recíprocamente, si $\{P_1, \dots, P_k\}$ es una base de Sylow, sea $Q_i = \prod_{j \neq i} P_j$. Como los P_j son permutables dos a dos, Q_i es un subgrupo de orden $p_i^{\alpha_i}$. Luego $\{Q_1, \dots, Q_k\}$ es un sistema de Sylow para G . Para completar la demostración queda como ejercicio verificar que

$$\bigcap_{i \neq k} \prod_{j \neq i} P_j = P_k, \quad \prod_{k \neq i} \bigcap_{j \neq k} Q_j = Q_i.$$

□

Dos sistemas de Sylow $\{Q_1, \dots, Q_k\}$ y $\{Q'_1, \dots, Q'_k\}$ se dicen **conjugados** si existen $x \in G$ y $\sigma \in \mathbb{S}_k$ tales que $x Q_j x^{-1} = Q'_{\sigma(j)}$ para todo $j \in \{1, \dots, k\}$.

theorem:sistemas_conj

Teorema 29.10. En un grupo finito y resoluble G todos los sistemas de Sylow son conjugados.

Demostración. Sea \mathcal{S}_i el conjunto de p_i' -subgrupos de Hall. Como para todo conjunto de primos π , los π -subgrupos de Hall son conjugados, el grupo G actúa transitivamente en \mathcal{S}_i . En particular, $|\mathcal{S}_i| = (G : N_G(Q_i))$ para todo $Q_i \in \mathcal{S}_i$. Como

$$(G : N_G(Q_i))(N_G(Q) : Q_i) = (G : Q_i)$$

es una potencia de p_i , se concluye que $|\mathcal{S}_i|$ es una potencia del primo p_i .

El grupo G actúa por conjugación en $\mathcal{S} = \mathcal{S}_1 \times \dots \times \mathcal{S}_k$. Como el estabilizador de (Q_1, \dots, Q_k) es $N = \cap_{i=1}^k N_G(Q_i)$, y además $(G : N) = \prod_{i=1}^k |\mathcal{S}_i| = |\mathcal{S}|$, la acción de G en \mathcal{S} es transitiva y luego todos los sistemas de Sylow son conjugados. □

Dos bases de Sylow $\{P_1, \dots, P_k\}$ y $\{P'_1, \dots, P'_k\}$ se dicen **conjugadas** si existen $x \in G$ y $\sigma \in \mathbb{S}_k$ tales que $xP_jx^{-1} = P'_{\sigma(j)}$ para todo $j \in \{1, \dots, k\}$.

Corolario 29.11. *En un grupo finito y resoluble G todos las bases de Sylow son conjugadas.*

Demostración. Es consecuencia del teorema 29.10 y de la biyección de la proposición 29.9. \square

Si $\{P_1, \dots, P_k\}$ es una base de Sylow de G , el grupo

$$N = \bigcap_{i=1}^k N_G(P_i)$$

se conoce como **el normalizador de la base de Sylow**.

Teorema 29.12. *Sea G finito y resoluble. Si $\{P_1, \dots, P_k\}$ es una base de Sylow de G , su normalizador es un grupo nilpotente.*

Demostración. Por definición $N = \bigcap_{i=1}^k N_G(P_i) \subseteq N_G(P_i)$. Entonces P_i es un subgrupo normal del subgrupo NP_i . Como $(N : N \cap P_i) = (NP_i : P_i)$ divide a $(G : P_i)$, se concluye que $P_i \cap N \in \text{Syl}_p(N)$. Luego N es nilpotente pues cada subgrupo de Sylow $P_i \cap N$ de N es normal en N . \square

Ejemplo 29.13. Para calcular bases de Sylow se utiliza la función `SylowSystem`. Una base de Sylow para el grupo $\mathbf{SL}_2(3)$ es el conjunto $\{A, B\}$, donde

$$A = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq C_3, \quad B = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle \simeq Q_8.$$

El normalizador N del sistema es el subgrupo N generado por la matriz $\begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$.

Veamos el código:

```
gap> SL23 := SL(2,3);;
gap> basis := SylowSystem(SL23);
[ Group([ [ [ Z(3)^0, Z(3)^0 ], [ Z(3)^0, Z(3) ] ],
[ [ Z(3), Z(3)^0 ], [ Z(3)^0, Z(3)^0 ] ],
[ [ Z(3), 0*Z(3) ], [ 0*Z(3), Z(3) ] ] ]),
Group([ [ [ Z(3)^0, Z(3)^0 ], [ 0*Z(3), Z(3)^0 ] ] ] ) ]
gap> N := Intersection(Normalizer(SL23, basis[1]), \
> Normalizer(SL23, basis[2]));;
gap> GeneratorsOfGroup(N);
[ [ [ Z(3)^0, Z(3)^0 ], [ 0*Z(3), Z(3)^0 ] ],
[ [ Z(3), 0*Z(3) ], [ 0*Z(3), Z(3) ] ] ]
gap> Order(N);
6
```


Capítulo 30

Subnormalidad

Definición 30.1. Sea G un grupo. Un subgrupo H de G es **subnormal** si existe una sucesión de subgrupos

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = G$$

con H_i normal en H_{i+1} para todo $i \in \{0, \dots, k-1\}$.

Ejemplo 30.2. Sea $G = \mathbb{S}_4$. El subgrupo $K = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$ es normal en G . El subgrupo $L = \{\text{id}, (12)(34)\}$ no es normal en G pero es subnormal.

Ejercicio 30.3. Demuestre que el teorema de la correspondencia también preserva la subnormalidad.

theorem:subnormal

Teorema 30.4. Sea G un grupo finito. Entonces G es nilpotente si y sólo si todo subgrupo es subnormal.

Demostración. Supongamos que todo subgrupo de G es subnormal. Sea H un subgrupo subnormal de G , donde

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = G$$

con H_i normal en H_{i+1} . Sin pérdida de generalidad podemos suponer que $H \subsetneq H_1$. Como entonces $H \subsetneq H_1 \subseteq N_G(H)$, G es nilpotente por el ejercicio ??.

Supongamos ahora que G es nilpotente. Sea H un subgrupo de G . Procederemos por inducción en $(G : H)$. Si $(G : H) = 1$ entonces $H = G$ y no hay nada para demostrar. Si $H \neq G$, como $H \subsetneq N_G(H)$ por el lema 20.18,

$$(G : N_G(H)) < (G : H).$$

Por hipótesis inductiva, $N_G(H)$ es subnormal en G y luego, como H es normal en $N_G(H)$, se concluye que H subnormal en G . \square

Corolario 30.5. Sea G un grupo y sea K un subgrupo de G tal que $K \subseteq Z(G)$. Entonces G es nilpotente si y sólo si G/K es nilpotente.

Demostración. Si G es nilpotente, entonces G/K es nilpotente por el teorema 20.13. Demostremos la afirmación recíproca. Sea $\pi: G \rightarrow G/K$ el morfismo canónico. Sea U un subgrupo de G . Como G/K es nilpotente, el teorema 30.4 implica que $\pi(U)$ es un subgrupo subnormal de G/K . La correspondencia implica que UK es un subgrupo subnormal de G , y luego, como K es central, U es normal en UZ . Luego U es subnormal en G y entonces G es nilpotente por el teorema 30.4. \square

theorem:F(G) subnormalidad

Teorema 30.6. *Sea G un grupo finito y sea H un subgrupo de G . Entonces H es nilpotente y subnormal en G si y sólo si $H \subseteq F(G)$.*

Demostración. Supongamos que $H \subseteq F(G)$. Como $F(G)$ es nilpotente por el teorema 23.6, H es nilpotente por el teorema 20.13. Además, como H es subnormal en $F(G)$ por la teorema 30.4 y $F(G)$ es normal en G , H es subnormal en G .

Supongamos ahora que H es nilpotente y subnormal en G . Procederemos por inducción en $|G|$. Si $H = G$ el resultado es trivialmente cierto. Supongamos entonces que $H \neq G$. Como H es subnormal en G ,

$$H = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G.$$

Sea $M = H_{k-1}$. Como $M \neq G$ y M es normal en G , $H \subseteq F(M)$ por hipótesis inductiva. Luego $H \subseteq F(M) = M \cap F(G) \subseteq F(G)$ por el corolario 23.9. \square

lemma:McapN=1

Lema 30.7. *Sean M y N subgrupos normales de un grupo G tales que $M \cap N = 1$. Entonces $M \subseteq C_G(N)$.*

Demostración. Sean $m \in M$ y $n \in N$. Entonces $[n, m] = (nmn^{-1})m \in M$ pues M es normal en G y también $[n, m] = n(mn^{-1}m^{-1}) \in N$ pues N es normal en G . Luego $[n, m] \in M \cap N = 1$. \square

theorem:MsubsetNG(S)

Teorema 30.8 (Wielandt). *Sea G un grupo finito. Si S es un subgrupo subnormal de G y M es un subgrupo minimal-normal de G entonces $M \subseteq N_G(S)$.*

Demostración. Procederemos por inducción en $|G|$. Si $S = G$ no hay nada para demostrar. Supongamos que $S \neq G$. Como S es subnormal en G , existe una sucesión

$$S = S_0 \triangleleft S_1 \triangleleft \cdots \triangleleft S_{k-1} \triangleleft S_k = G.$$

Sea $N = S_{k-1}$.

Si $M \cap N \neq 1$ entonces $M \subseteq N$ (pues como M y N son normales en G , $M \cap N = M$ por la minimalidad de M). Vamos a demostrar que $M \subseteq \text{Soc}(N)$. Como $M \neq 1$ y M es normal en N , $M \cap \text{Soc}(N) \neq 1$. Además $\text{Soc}(N)$ es característico en N y N es normal en G , entonces $\text{Soc}(N)$ es normal en G . Luego $M \cap \text{Soc}(N)$ es un subgrupo normal de G . Como además $1 \neq M \cap \text{Soc}(N) \subseteq M$, se concluye que $M \cap \text{Soc}(N) = M$ por la minimalidad de M . Por hipótesis inductiva, todo subgrupo minimal-normal de N normaliza a S ; entonces $\text{Soc}(N) \subseteq N_N(S) \subseteq N_G(S)$ y luego

$$M \subseteq \text{Soc}(N) \subseteq N_G(S).$$

Si $M \cap N = 1$, el lema 30.7 implica que

$$M \subseteq C_G(N) \subseteq C_G(S) \subseteq N_G(S).$$

□

Corolario 30.9. *Sea G finito y sea S un subgrupo subnormal de G . Entonces $\text{Soc}(G) \subseteq N_G(S)$.*

Demostración. Como todo subgrupo minimal-normal de G está contenido en $N_G(S)$ por el teorema 30.8, $\text{Soc}(G) = \langle M : M \text{ subgrupo minimal-normal de } G \rangle \subseteq N_G(S)$.

□

En el siguiente teorema demostraremos que los subgrupos normales forman un reticulado.

theorem:STsubnormal

Teorema 30.10 (Wielandt). *Sea G un grupo finito y sean S, T subgrupos subnormales. Entonces $S \cap T$ y $\langle S, T \rangle$ son subnormales en G .*

Demostración. Demostremos primero que $S \cap T$ es subnormal en G . Como la subnormalidad es transitiva, basta ver que $S \cap T$ es subnormal en T . Como S es subnormal en G , existe una sucesión

$$S = S_0 \triangleleft S_1 \triangleleft \cdots \triangleleft S_k = G.$$

Cada $S_{j-1} \cap T$ es normal en $S_j \cap T$ y luego $S \cap T$ es subnormal en T .

Para demostrar que $\langle S, T \rangle$ es subnormal en G procederemos por inducción en $|G|$. Supongamos que $G \neq 1$ y sea M un subgrupo minimal-normal de G . Sea $\pi: G \rightarrow G/M$ el morfismo canónico. Como $\pi(S)$ y $\pi(T)$ son subnormales en G/M y $|G/M| < |G|$, la hipótesis inductiva implica que

$$\pi(\langle S, T \rangle M) = \pi(\langle S, T \rangle) = \langle \pi(S), \pi(T) \rangle$$

es subnormal en G/M . Por la correspondencia, $\langle S, T \rangle M$ es subnormal en G . Por otro lado, el teorema 30.8 implica que $M \subseteq N_G(S)$ y $M \subseteq N_G(T)$. Luego $M \subseteq N_G(\langle S, T \rangle)$. Como entonces $\langle S, T \rangle$ es normal en $\langle S, T \rangle M$ y $\langle S, T \rangle M$ es subnormal en G , se concluye que $\langle S, T \rangle$ es subnormal en G .

□

Capítulo 31

El teorema de la cremallera

El siguiente resultado de Wielandt es muy útil y se conoce como el **teorema de la cremallera**.

theorem:zipper

Teorema 31.1 (Wielandt). *Sea G un grupo finito y sea S un subgrupo de G tal que S es subnormal en todo subgrupo propio de G que contiene a S . Si S no es subnormal en G entonces existe un único maximal de G que contiene a S .*

Demostración. Procederemos por inducción en $(G : S)$. Si S no es subnormal en G entonces $S \neq G$ y entonces el caso $(G : S) = 1$ es trivialmente cierto.

Como S no es subnormal en G , $N_G(S) \neq G$. Entonces $S \subseteq N_G(S) \subseteq M$ para algún subgrupo maximal M de G . Supongamos que $S \subseteq K$ para algún subgrupo maximal K de G . Vamos a demostrar que $K = M$. Como $S \subseteq K \neq G$, S es subnormal en K . Si S es normal en K entonces $K \subseteq N_G(S) \subseteq M$ y luego $K = M$ por maximalidad de K . Si S no es normal en K , existen $m \geq 2$ subgrupos S_0, \dots, S_m de K tales que

$$S = S_0 \triangleleft S_1 \triangleleft \dots \triangleleft S_m = K,$$

donde S no es normal en S_2 . Sea $x \in S_2$ tal que $xSx^{-1} \neq S$ y sea $T = \langle S, xSx^{-1} \rangle \subseteq K$.

Como $xSx^{-1} \subseteq xS_1x^{-1} = S_1 \subseteq N_G(S)$, se tiene que $T \subseteq N_G(S) \subseteq M$. Además S es normal en T y luego $T \neq G$.

Veamos que el grupo T satisface las hipótesis del teorema. Si T fuera subnormal en G entonces, como S es normal en T , S sería subnormal en G . Si H es un subgrupo propio de G que contiene a T entonces, como $S \subseteq H$, S es subnormal en H . Además xSx^{-1} es también subnormal en H . Luego T es subnormal en H por el teorema 30.10.

Como $S \subsetneq T$, $(G : T) < (G : S)$. Por hipótesis inductiva, T está contenido en un único maximal de G . Luego $K = M$ pues $T \subseteq M$ y $T \subseteq K$. \square

Aplicaciones del teorema de la cremallera

La primera aplicación es el siguiente criterio para detectar subnormalidad. Antes de enunciar y demostrar el teorema, necesitamos un lema.

lemma:H=G

Lema 31.2. Sea G un grupo y H un subgrupo de G . Si $(xHx^{-1})H = G$ para algún $x \in G$ entonces $H = G$.

Demostración. Escribimos $x = uv$ con $u \in xHx^{-1}$, $v \in H$. Como $u \in xHx^{-1}$ y $u^{-1}x = v \in H$, se tiene que $H = vHv^{-1} = u^{-1}(xHx^{-1})u = xHx^{-1}$. Luego $G = H$. \square

Dos subgrupos S y T de un grupo G se dicen **permutables** si $ST = TS$.

Teorema 31.3. Sea G un grupo finito y sea S un subgrupo de G permutable con todos sus conjugados. Entonces S es subnormal en G .

Demostración. Procederemos por inducción en $|G|$. Supongamos que S es subnormal en todo subgrupo H tal que $S \subseteq H \subsetneq G$. Si S no es subnormal en G entonces, por el teorema 31.1, existe un único subgrupo maximal M de G tal que $S \subseteq M$. Sea $x \in G$ y sea $T = xSx^{-1}$. Por el lema 31.2 $ST \neq G$ (pues $S \neq G$) y entonces ST está contenido en algún subgrupo maximal de G . Como $S \subseteq ST$ y S está contenido en un único maximal, se concluye que $T \subseteq ST \subseteq M$. Como $S^G = \langle xSx^{-1} : x \in G \rangle \subseteq M \neq G$, por hipótesis inductiva S es subnormal en S^G . Luego S es subnormal en G pues S^G es normal en G , una contradicción. \square

theorem:Baer

Teorema 31.4 (Baer). Sean G un grupo finito y H un subgrupo de G . Entonces $H \subseteq F(G)$ si y sólo si $\langle H, xHx^{-1} \rangle$ es nilpotente para todo $x \in G$.

Demostración. Si $H \subseteq F(G)$ entonces $xHx^{-1} \subseteq F(G)$ para todo $x \in G$ pues $F(G)$ es normal en G . Luego $\langle H, xHx^{-1} \rangle$ es nilpotente por ser un subgrupo de $F(G)$.

Demostraremos la recíproca. Supongamos que $\langle H, xHx^{-1} \rangle$ es nilpotente para todo $x \in G$. Como $H \subseteq \langle H, xHx^{-1} \rangle$, H es nilpotente. Por el teorema 30.6 basta ver que H es subnormal en G . Procederemos por inducción en $|G|$. Supongamos que H no es subnormal en G . Si H está contenido propiamente en algún subgrupo K entonces, como $\langle H, kHk^{-1} \rangle$ es nilpotente para todo $k \in K$, H es subnormal en K por hipótesis inductiva. Por el teorema 31.1, existe un único maximal M de G que contiene a H . Vamos a considerar dos casos posibles: a) $G = \langle H, xHx^{-1} \rangle$ para algún $x \in G$. Como G entonces es nilpotente, H es subnormal en G por el teorema 30.4, una contradicción. b) $\langle H, xHx^{-1} \rangle \neq G$ para todo $x \in G$. En este caso, para cada $x \in G$ existe un subgrupo maximal que contiene a $\langle H, xHx^{-1} \rangle$. Como $H \subseteq \langle H, xHx^{-1} \rangle$ y H está contenido en un único maximal, se concluye que $\langle H, xHx^{-1} \rangle \subseteq M$ para todo $x \in G$. En particular, la clausura normal H^G de H está propiamente contenida en G . Como por hipótesis inductiva H es subnormal en H^G y H^G es normal en G , se concluye que H es subnormal en G , una contradicción. \square

theorem:Zenkov

Teorema 31.5 (Zenkov). Sean G un grupo finito y A, B subgrupos abelianos de G . Sea $M \in \{A \cap gBg^{-1} : g \in G\}$ tal que ningún $A \cap gBg^{-1}$ está propiamente contenido en M . Entonces $M \subseteq F(G)$.

Demostración. Sin pérdida de generalidad podemos suponer que $M = A \cap B$. Demostraremos por inducción en $|G|$ que $M \subseteq F(G)$.

Supongamos que $G = \langle A, gBg^{-1} \rangle$ para algún $g \in G$. Como A y B son abelianos, $A \cap gBg^{-1} \subseteq Z(G)$. Luego

$$A \cap gBg^{-1} = g^{-1}(A \cap gBg^{-1})g \subseteq A \cap B = M.$$

Por la minimalidad de M , $M = A \cap gBg^{-1} \subseteq Z(G) \subseteq F(G)$ por el corolario 23.7.

Supongamos ahora que $G \neq \langle A, gBg^{-1} \rangle$ para todo $g \in G$. Fijemos $g \in G$. Sean $H = \langle A, gBg^{-1} \rangle \neq G$ y $C = B \cap H$. Al usar que $A \subseteq H$ se obtiene fácilmente que $M = A \cap B = A \cap C$ y que $A \cap hCh^{-1} = A \cap hBh^{-1}$ para todo $h \in H$. Esto implica que ningún $A \cap hCh^{-1}$ está propiamente contenido en $A \cap C$. Al aplicar la hipótesis inductiva al subgrupo H obtenemos entonces

$$M = A \cap B = A \cap C \subseteq F(H).$$

Vamos a demostrar ahora que todo p -subgrupo de Sylow P de M está contenido en $F(G)$. Como M está generado por sus subgrupos de Sylow, esto implica que $M \subseteq F(G)$. Si $P \in \text{Syl}_p(M)$ entonces $P \subseteq M \subseteq F(H)$. Como $O_p(H)$ es el único p -subgrupo de Sylow de $F(H)$, $P \subseteq O_p(H)$. Como $P \subseteq M \subseteq B$,

$$gPg^{-1} \subseteq gBg^{-1} \subseteq H$$

para todo $g \in G$. Entonces $O_p(H)(gPg^{-1})$ es un p -subgrupo de H que contiene a $\langle P, gPg^{-1} \rangle$. Luego $\langle P, gPg^{-1} \rangle$ es nilpotente para todo $g \in G$ por ser un p -grupo. Por el teorema de Baer 31.4, $P \subseteq F(G)$ para todo p -subgrupo de Sylow P de M . \square

corollary:Zenkov

Corolario 31.6. Sea G un grupo finito no trivial y sea A un subgrupo abeliano tal que $|A| \geq (G : A)$. Entonces $A \cap F(G) \neq 1$.

Demostración. Sea $g \in G$. Podemos suponer que $G \neq A$ y luego $(gAg^{-1})A \neq G$ por el lema 31.2. Como $|gAg^{-1}||A| = |A|^2 \geq |A|(G : A) = |G|$,

$$|G| > |gAg^{-1}A| = \frac{|A||gAg^{-1}|}{|A \cap gAg^{-1}|} \geq \frac{|G|}{|A \cap gAg^{-1}|}.$$

Luego $A \cap gAg^{-1} \neq 1$ para todo $g \in G$. En particular, ningún $A \cap gAg^{-1}$ está propiamente contenido en A y luego, por el teorema de Zenkov 31.5, $A \subseteq F(G)$. \square

Corolario 31.7. Sea $G = NA$ un grupo finito, donde N es normal en G , A es un subgrupo abeliano y $C_A(N) = 1$. Si $F(N) = 1$, entonces $|A| < |N|$.

Demostración. Como N es normal en G , $N \cap F(G) = F(N) = 1$ por el corolario 23.9. Luego $[N, F(G)] = 1$ porque N y $F(G)$ son ambos normales en G . Como

$$|A| \geq |N| \geq \frac{|N|}{|N \cap A|} = (NA : A) = (G : A),$$

$A \cap F(G) \neq 1$ por el corolario 31.6. Si $1 \neq a \in A \cap F(G)$, entonces $a \in C_A(N) = 1$, una contradicción. \square

theorem:Brodkey

Teorema 31.8 (Brodkey). Sea G un grupo finito tal que existe $P \in \text{Syl}_p(G)$ abeliano. Entonces existen $S, T \in \text{Syl}_p(G)$ tales que $S \cap T = O_p(G)$.

Demostración. Al aplicar el teorema de Zenkov 31.5 con $A = B = P$ se tiene que $P \cap gPg^{-1} \subseteq F(G)$ para algún $g \in G$. Como $O_p(G)$ es el único p -subgrupo de Sylow de $F(G)$, $P \cap gPg^{-1} \subseteq O_p(G)$. Luego $P \cap gPg^{-1} = P_p(G)$ pues $O_p(G)$ está contenido en todo p -subgrupo de Sylow de G . \square

corollary:GP2

Corolario 31.9. Sea G un grupo finito. Si existe $P \in \text{Syl}_p(G)$ abeliano,

$$(G : O_p(G)) \leq (G : P)^2.$$

Demostración. Por el teorema de Brodkey 31.8, existen $S, T \in \text{Syl}_p(G)$ tales que $S \cap T = O_p(G)$. Entonces

$$|G| \geq |ST| = \frac{|S||T|}{|S \cap T|} = \frac{|P|^2}{|O_p(G)|},$$

que implica el corolario. \square

Corolario 31.10. Sea G un grupo finito. Si existe un subgrupo $P \in \text{Syl}_p(G)$ abeliano tal que $|P| < \sqrt{|G|}$ entonces $O_p(G) \neq 1$.

Demostración. Como $(G : P)^2 < |G|$, el corolario 31.9 implica que $O_p(G) \neq 1$. \square

exercise:G/Z(G)

Ejercicio 31.11. Sea G un grupo y sea $K \subseteq Z(G)$. Demuestre que si G/K es cíclico entonces G es abeliano.

Sean $g, h \in G$ y sea $\pi: G \rightarrow G/K$ el morfismo canónico. Como G/K es cíclico, existe $x \in G$ tal que $G/K = \langle xK \rangle$. Sean k, l tales que $\pi(g) = x^k$, $\pi(h) = x^l$. Entonces existen $z_1, z_2 \in K$ tales que $g = x^k z_1$, $h = x^l z_2$. Luego $[g, h] = [x^k, x^l] = 1$.

Ejercicio 31.12. Sea G un grupo y sea A un subgrupo de G . Demuestre que $\text{Core}_G(A) = \bigcap_{x \in G} xAx^{-1}$ es el mayor subgrupo normal de G contenido en A .

Hagamos actuar a G por multiplicación en las coclases de A : $g \cdot xA = gxA$. Esta acción induce un morfismo $\rho: G \rightarrow \mathbb{S}_{G/A}$ con núcleo

$$\ker \rho = \bigcap_{x \in G} xAx^{-1} = \text{Core}_G(A).$$

Es claro entonces que $\text{Core}_G(A)$ es un subgrupo normal de G contenido en A . Si K es un subgrupo normal de G tal que $K \subseteq A$, entonces $K = xKx^{-1} \subseteq xAx^{-1}$ para todo $x \in G$. Luego $K \subseteq \text{Core}_G(A)$.

theorem:Lucchini

Teorema 31.13 (Lucchini). Sea G un grupo finito y sea A un subgrupo cíclico propio. Si $K = \text{Core}_G(A)$ entonces $(A : K) < (G : A)$.

Demostración. Procederemos por inducción en $|G|$. Sea $\pi: G \rightarrow G/K$ el morfismo canónico. Observemos que $\text{Core}_{G/K} \pi(A)$ es trivial.

Supongamos primero que $K \neq 1$. Como $\pi(A)$ es un subgrupo cíclico propio de G/K y $K \subseteq A$, la hipótesis inductiva implica que

$$(A : K) = |\pi(A)| = (\pi(A) : \pi(K)) < (\pi(G) : \pi(A)) = \frac{(G : K)}{(A : K)} = (G : A).$$

Supongamos ahora que $K = 1$. Queremos demostrar que $|A| < (G : A)$. Supongamos entonces que $|A| \geq (G : A)$. Como $A \neq G$, $A \cap F(G) \neq 1$ por el corolario 31.6. En particular, $F(G) \neq 1$. Sea E un subgrupo minimal-normal de G tal que $E \subseteq F(G)$. Por el teorema 20.29, $E \cap Z(F(G)) \neq 1$. Luego, como $E \cap Z(F(G))$ es normal en G y E es minimal, $E \cap Z(F(G)) = E$, es decir $E \subseteq Z(F(G))$. En particular, E es abeliano y luego, por la minimalidad de E , existe un primo p tal que $x^p = 1$ para todo $x \in E$.

Afirmación. $A \cap F(G)$ es un subgrupo normal de EA .

Como E es normal en G , EA es un subgrupo de G . Como $A \cap F(G) \subseteq A$, $A \cap F(G)$ es un subgrupo de EA . Como $F(G)$ es normal en G , $a(A \cap F(G))a^{-1} = A \cap F(G)$ para todo $a \in A$. Por otro lado $E \subseteq Z(F(G))$ y $A \cap F(G) \subseteq F(G)$ implican que $x(A \cap F(G))x^{-1} = A \cap F(G)$ para todo $x \in E$.

Afirmación. $EA \neq G$.

Si $G = EA$ entonces, como $A \cap F(G)$ es un subgrupo normal de G contenido en A , se concluye que $1 \neq A \cap F(G) \subseteq K = 1$, una contradicción. para todo $g \in G$. Luego $1 \neq A \cap F(G) \subseteq K$, una contradicción pues $K = 1$.

Sea $p: G \rightarrow G/E$ el morfismo canónico. Por la correspondencia, existe un subgrupo normal M de G con $E \subseteq M$ tal que $p(M) = \text{Core}_{G/E}(p(A))$. Como $EA \neq G$, $p(A)$ es un subgrupo cíclico propio de $p(G)$. Como $p(A) \simeq A/A \cap E \simeq EA/E$ y $p(M) \simeq M/E$, la hipótesis inductiva implica que $(EA : M) < (G : EA)$ pues

$$\frac{|EA/E|}{|M/E|} = (p(A) : p(M)) < (p(G) : p(A)) = \frac{|G/E|}{|EA/E|}.$$

Afirmación. $MA = EA$.

Como $E \subseteq M$ entonces $EA \subseteq MA$. Recíprocamente, si $m \in M$ entonces, como $p(m) \in \text{Core}_{G/E}(p(A))$, en particular $p(m) \in p(A)$. Luego $m \in EA$.

Sea $B = A \cap M$. Al usar que $(AE : M) < (G : EA)$, que

$$(A : B) = |A/A \cap M| = |AM/M| = (EA : M)$$

y la hipótesis inductiva obtenemos

$$\begin{aligned}
(M : B) &= (M : A \cap M) = (MA : A) \\
&= (EA : A) = \frac{(G : A)}{(G : EA)} < \frac{(G : A)}{(AE : M)} = \frac{(G : A)}{(A : B)} \leq |B|
\end{aligned} \tag{31.1}$$

$$\text{eq: } (M:B) \leq |B|$$

pues $|A| \geq (G : A)$.

Afirmación. $M = EB$.

Como $E \cup B \subseteq M$ entonces $EB \subseteq M$. Recíprocamente, si $m \in M$ entonces $m = ea$ para algún $e \in E, a \in A$. Como $e^{-1}m = a \in A \cap M = B$ pues $E \subseteq M$ entonces $m \in EB$.

Afirmación. M es no abeliano.

Supongamos que M es abeliano. La función $f: M \rightarrow M, m \mapsto m^p$, es un morfismo de grupos tal que $E \subseteq \ker f$. Como $M = EB$, $f(M) \subseteq f(B) \subseteq B \subseteq A$. Como M es normal en G , $f(M)$ es normal en G . Luego $f(M) = 1$ pues $K = \text{Core}_G(A) = 1$ es el mayor subgrupo normal de G contenido en A ; en particular, como B es normal en $M = EB$, M/B es un p -grupo. Como $B \subseteq M$, $f(B) = 1$; además como $B \subseteq A$ es cíclico, $|B| \leq p$. Luego, por la fórmula (31.1), $(M : B) < |B| \leq p$. Esto implica que $M = B \subseteq A$ y que $M = E = 1$ (porque M es normal en G y $\text{Core}_G(A) = K = 1$ es el mayor subgrupo normal de G que contiene a A), una contradicción.

Afirmación. $Z(M)$ es cíclico.

Como M es no abeliano y $M/E = EB/E \simeq B/E \cap B$ es cíclico, $E \not\subseteq Z(M)$ (ejercicio 31.11), es decir $E \cap Z(M) \subsetneq E$. Luego

$$E \cap Z(M) = 1 \tag{31.2}$$

$$\text{equation: } E \cap Z(M)$$

por la minimalidad de E . Entonces

$$Z(M) = Z(M)/Z(M) \cap E \simeq p(Z(M)) \subseteq p(M) = \text{Core}_{G/E} p(A) \subseteq p(A)$$

y luego $Z(M)$ es cíclico pues $p(A)$ es cíclico.

Como $B \subseteq A$ es abeliano y $(M : B) < |B|$, $B \cap F(M) \neq 1$ por el corolario 31.6. Entonces $[E, F(M)] = 1$ (pues $E \subseteq Z(F(G))$ y $F(M) \subseteq F(G)$ por el corolario 23.9). Luego $B \cap F(M) \subseteq Z(M)$ pues $M = BE$, $[B \cap F(M), E] \subseteq [F(M), E] = 1$ y también $[B \cap F(M), B] = 1$ porque B es abeliano. Como $Z(M)$ es cíclico, $B \cap F(M)$ es característico en $Z(M)$. Luego, como $Z(M)$ es normal en G , $1 \neq B \cap F(M)$ es un subgrupo normal de G contenido en A , una contradicción. \square

Para terminar la sección veamos una aplicación del teorema de Lucchini.

Corolario 31.14 (Horosevskii). Sea $G \neq 1$ un grupo finito y sea $\sigma \in \text{Aut}(G)$. Entonces $|\sigma| < |G|$.

Demostración. Sea $A = \langle \sigma \rangle$. Como A actúa por automorfismos en G , podemos considerar el grupo $\Gamma = G \rtimes A$ con la operación

$$(g, \sigma^k)(h, \sigma^l) = (g\sigma^k(h), \sigma^{k+l}).$$

Identificamos A con $1 \times A$ y G con $G \times 1$. Como $K \cap G \subseteq A \cap G = 1$ y $A \cap C_\Gamma(G) = 1$,

$$K \subseteq A \cap C_\Gamma(G) = 1$$

pues si $k \in K$ y $g \in G$ entonces $gkg^{-1}k^{-1} \in G \cap K = 1$ (porque K y G son normales en Γ). Por el teorema de Lucchini 31.13, $(A : K) < (\Gamma : A)$, es decir

$$|\sigma| = |A| = (A : K) < (\Gamma : A) = |G|.$$

□

Capítulo 32

El subgrupo de Chermak–Delgado

CD

Definición 32.1. Sea G un grupo finito y H un subgrupo de G . Se define la **medida de Chermak–Delgado** de H como

$$m_G(H) = |H||C_G(H)|.$$

Ejemplo 32.2. Si G es un grupo abeliano y H es un subgrupo de G entonces $m_G(H) = |H||G|$.

Ejemplo 32.3. Sea $G = \mathbb{S}_3$. Los subgrupos de G son:

$$H_0 = 1, \quad H_1 = \langle (23) \rangle, \quad H_2 = \langle (12) \rangle, \quad H_3 = \langle (13) \rangle, \quad H_4 = \langle (123) \rangle, \quad H_5 = \mathbb{S}_3.$$

Un cálculo directo muestra que

$$m_G(H_j) = \begin{cases} 6 & \text{si } j \in \{0, 5\}, \\ 4 & \text{si } j \in \{1, 2, 3\}, \\ 9 & \text{si } j = 4. \end{cases}$$

lemma:CD1

Lema 32.4. Sean G un grupo finito y H un subgrupo de G . Entonces

$$m_G(H) \leq m_G(C_G(H)).$$

Si vale la igualdad, $H = C_G(C_G(H))$.

Demostración. Sea $C = C_G(H)$. Como $H \subseteq C_G(C)$,

$$m_G(C) = |C||C_G(C)| \geq |C||H| = m_G(H).$$

Si $m_G(H) = m_G(C_G(H))$ entonces $|H| = |C_G(C_G(H))|$ y luego $H = C_G(C_G(H))$ pues $H \subseteq C_G(C_G(H))$. \square

Lema 32.5. Sean G un grupo finito y H, K subgrupos de G . Sean $D = H \cap K$ y $J = \langle H, K \rangle$. Entonces

$$m_G(H)m_G(K) \leq m_G(D)m_G(J).$$

lemma:CD2

Si vale la igualdad, $J = HK$ y $C_G(D) = C_G(H)C_G(K)$.

Demostración. Sean $C_H = C_G(H)$, $C_K = C_G(K)$, $C_D = C_G(D)$, $C_J = C_G(J)$. Entonces $C_J = C_H \cap C_K$ y $C_H \cup C_K \subseteq C_D$. Como

$$|J| \geq |HK| = \frac{|H||K|}{|D|}, \quad |C_D| \geq |C_H C_K| = \frac{|C_H||C_K|}{|C_J|},$$

tenemos

$$m_G(D) = |D||C_D| \geq \frac{|H||K|}{|J|} \frac{|C_H||C_K|}{|C_J|} = \frac{m_G(H)m_G(K)}{m_G(J)}.$$

La segunda afirmación es evidente. \square

Sea G un grupo finito y sea \mathcal{L} una colección de subgrupos de G . Diremos que \mathcal{L} es un **reticulado** si dados $H, K \in \mathcal{L}$ se tiene que $H \cap K \in \mathcal{L}$ y $\langle H, K \rangle \in \mathcal{L}$.

Como el grupo G es finito, tiene sentido considerar el conjunto $\mathcal{L}(G)$ de subgrupos de G donde la medida de Chermak–Delgado alcanza su máximo valor, digamos M_G .

exercise:M_S

Ejercicio 32.6. Sea G un grupo finito y sea H un subgrupo de G . Demuestre que $M_H \leq M_G$.

Sabemos que existe algún subgrupo K de H tal que $M_H = m_H(K)$. Como $C_H(K) \subseteq C_G(K)$,

$$M_H = m_H(K) = |H||C_H(K)| \leq |H||C_G(K)| \leq m_G(H) \leq M_G.$$

example:D8_CD

Ejemplo 32.7. Sea $G = \mathbb{D}_8 = \langle r, s : r^4 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diedral de ocho elementos. En los subgrupos

$$G, \quad Z(G) = \{1, r^2\}, \quad A = \{1, r, r^2, r^3\}, \quad B = \{1, s, sr^2, r^2\}, \quad C = \{1, sr, sr^3, r^2\},$$

la medida de Chermak–Delgado vale 16, y este es el mayor valor posible que puede tomar esta medida. Luego $\mathcal{L}(G) = \{G, Z(G), A, B, C\}$ y $M_G = 16$.

```
gap> ChermakDelgado := function(group, subgroup)
> return Size(subgroup) \
> *Size(Centralizer(group, subgroup));
> end;
function( group, subgroup ) ... end
gap> gr := DihedralGroup(IsPermGroup, 8);
gap> r := gr.1;
gap> s := gr.2;
gap> ChermakDelgado(gr, Subgroup(gr, [r]));
16
```

```

gap> ChermakDelgado(gr, Subgroup(gr, [s*r, s*r^3]));
16
gap> ChermakDelgado(gr, Subgroup(gr, [s, s*r^2]));
16
gap> ChermakDelgado(gr, Subgroup(gr, [r^2]));
16
gap> List(AllSubgroups(gr), x->ChermakDelgado(gr, x));
[ 8, 16, 8, 8, 8, 8, 16, 16, 16, 16 ]

```

Teorema 32.8. *Sea G un grupo finito. Valen las siguientes afirmaciones:*

- 1) $\mathcal{L}(G)$ es un reticulado.
- 2) Si $H, K \in \mathcal{L}(G)$ entonces $\langle H, K \rangle = HK$.
- 3) Si $H \in \mathcal{L}(G)$ entonces $C_G(H) \in \mathcal{L}(G)$ y $C_G(C_G(H)) = H$.

theorem:reticulado

Demostración. Si $H, K \in \mathcal{L}(G)$ entonces $m_G(H) = m_G(K) = M_G$. Sean $D = H \cap K$ y $J = \langle H, K \rangle$. Por el lema 32.5,

$$M_G^2 = m_G(H)m_G(K) \leq m_G(D)m_G(J).$$

Como $m_G(D) \leq M_G$ y $m_G(J) \leq M_G$ por ser M_G el máximo valor posible, se concluye que $m_G(D) = m_G(J) = M_G$. Luego $\mathcal{L}(G)$ es un reticulado.

En particular, como $m_G(H)m_G(K) = m_G(D)m_G(J) = M_G^2$, se obtiene que $J = HK$ al aplicar el lema 32.5.

Por el lema 32.4,

$$M_G = m_G(H) \leq m_G(C_G(H)).$$

Como M_G es maximal, $m_G(C_G(H)) = M_G$ y luego $C_G(H) \in \mathcal{L}(G)$. Por el lema 32.4, $C_G(C_G(H)) = H$. \square

Como aplicación del teorema 32.8, se demuestra la existencia del **subgrupo de Chermak–Delgado**:

Corolario 32.9. *Sea G un grupo finito. Entonces existe un único subgrupo M minimal tal que $m_G(M)$ toma el mayor valor posible entre los subgrupos de G . Además M es característico, abeliano y $Z(G) \subseteq M$.*

Demostración. Por el teorema 32.8, $\mathcal{L}(G)$ es un reticulado. Sea

$$M = \bigcap_{H \in \mathcal{L}(G)} H \in \mathcal{L}(G).$$

Por el teorema 32.8 sabemos que $C_G(M) \in \mathcal{L}(G)$ y que $M = C_G(C_G(M)) \supseteq Z(G)$. Como $C_G(M) \in \mathcal{L}(G)$, $M \subseteq C_G(M)$ y luego M es abeliano. Además M es característico pues $f(M) \in \mathcal{L}(G)$ para todo $f \in \text{Aut}(G)$. \square

Ejemplo 32.10. Sea $G = \mathbb{D}_8$ el grupo diedral de ocho elementos. Por lo visto en el ejemplo 32.7, el subgrupo de Chermak–Delgado de G es $Z(G) \simeq C_2$.

corollary:ChermakDelgado

Teorema 32.11 (Chermak–Delgado). *Sea G un grupo finito. Entonces G tiene un subgrupo abeliano característico M tal que $(G : M) \leq (G : A)^2$ para todo subgrupo abeliano A .*

theorem:ChermakDelgado

Demostración. Sea M el subgrupo de Chermak–Delgado del corolario 32.9 y sea A un subgrupo abeliano de G . Como A es abeliano, $A \subseteq C_G(A)$. Luego

$$m_G(M) \geq m_G(A) = |A||C_G(A)| \geq |A|^2,$$

y entonces

$$(G : A)^2 = \frac{|G|^2}{|A|^2} \geq \frac{|G|^2}{m_G(M)} = \frac{|G|}{|M|} \frac{|G|}{|C_G(M)|} = \frac{|G|}{|M|} = (G : M).$$

□

Corolario 32.12. *Sea G un grupo finito y sea H un subgrupo de G tal que*

$$|H||C_G(H)| > |G|.$$

Entonces G no es simple no abeliano.

Demostración. Sea M el subgrupo de Chermak–Delgado de G . Entonces

$$m_G(M) \geq m_G(H) > |G|. \quad (32.1)$$

equation:mG

Esta desigualdad implica que $M \neq 1$ pues $m_G(M) = m_G(1) = |G|$. Si G fuera simple, $M = G$ sería abeliano. □

Corolario 32.13. *Sea G un grupo finito no abeliano y sea $P \in \text{Syl}_p(G)$ abeliano tal que $|P|^2 > |G|$. Entonces G no es simple.*

Demostración. Sea M el subgrupo de Chermak–Delgado. Como P es abeliano, por el teorema 32.11, $(G : M) \leq (G : P)^2 < |G|$, y luego $M > 1$. Si G fuera simple, entonces $M = G$ y luego G resultaría abeliano. □

Veamos una aplicación del teorema de la cremallera al reticulado de Chermak–Delgado.

lemma:L(G)L(S)

Lema 32.14. *Sea G un grupo finito. Sea $H \in \mathcal{L}(G)$ y sea S un subgrupo de G tal que $HC_G(H) \subseteq S$. Entonces $H \in \mathcal{L}(S)$.*

Demostración. Como $C_G(H) \subseteq S$, $C_G(H) = C_S(H)$. Vimos en el ejercicio 32.6 que $M_S \leq M_G$. Luego $M_G = M_S$ pues

$$M_G = m_G(H) = |H||C_G(H)| = |H||C_S(H)| = m_S(H) \leq M_S.$$

□

theorem:L(G)subnormal

Teorema 32.15. *Sea G un grupo finito. Todo $H \in \mathcal{L}(G)$ es subnormal en G .*

Demostración. Procederemos por inducción en $|G|$. El caso $|G| = 1$ es trivial. Sea $H \in \mathcal{L}(G)$ y sea $K = HC_G(H)$. Como H es normal en K , basta con demostrar que K es subnormal en G . Si $K = G$ no hay nada para hacer. Supongamos entonces que $K \neq G$.

Supongamos que K no es subnormal en G . Por hipótesis inductiva y por el teorema de la cremallera 31.1, existe un único subgrupo maximal M que contiene a K . Por el teorema 32.8, $C_G(H) \in \mathcal{L}(G)$ y $K = HC_G(H) \in \mathcal{L}(G)$. Por el lema 32.14, $H \in \mathcal{L}(M)$ y luego $K \in \mathcal{L}(M)$. Por hipótesis inductiva, K es subnormal en M . Veamos que M es normal en G . Sea $x \in G$. Como $m_G(xKx^{-1}) = m_G(K)$, el subgrupo $xKx^{-1} \in \mathcal{L}(G)$ y luego $K(xKx^{-1}) \in \mathcal{L}(G)$.

Si $K(xKx^{-1}) = G$ entonces, como existen $k_1, k_2 \in K$ tales que $k_1(xk_2x^{-1}) = x^{-1}$, se tiene que $x \in K$ pues $x^{-1} = k_2k_1 \in K$; esto implica que $xKx^{-1} \subseteq K$ y entonces $K = G$, una contradicción.

Como $K(xKx^{-1}) \neq G$, existe un subgrupo maximal N tal que $K(xKx^{-1}) \subseteq N$. Como $K \subseteq N$, $N = M$ pues M es el único maximal que contiene a K . Como además $xKx^{-1} \subseteq M$, $K \subseteq x^{-1}Mx$. Luego $x^{-1}Mx = M$ pues $x^{-1}Mx$ es un maximal que contiene a K y M es el único maximal que contiene a K . \square

Corolario 32.16. Si G un grupo simple finito no abeliano entonces $\mathcal{L}(G) = \{1, G\}$.

Demostración. Sea $K \in \mathcal{L}(G)$. Entonces K es subnormal en G por el teorema 32.15 y luego $K \in \{1, G\}$. Como $m_G(1) = m_G(G)$, el corolario queda demostrado. \square

Corolario 32.17. Sea $n \geq 5$. Entonces $\mathcal{L}(\mathbb{S}_n) = \{1, \mathbb{S}_n\}$.

Demostración. Sea $G = \mathbb{S}_n$ y sea $K \in \mathcal{L}(G)$. Por el teorema 32.15, K es subnormal en G . Si $K \neq G$ entonces se tiene una sucesión estrictamente creciente de subgrupos

$$K = K_1 \triangleleft K_2 \triangleleft \cdots \triangleleft K_{n-1} \triangleleft K_n = G.$$

Como K_{n-1} es normal en G , $K_{n-1} \in \{1, \mathbb{A}_n\}$ y luego $K = 1$. El corolario queda demostrado al observar que $m_G(1) = m_G(G)$. \square

Capítulo 33

El morfismo de transferencia

Sea G un grupo y sea H un subgrupo de índice finito. Vamos a definir un morfismo de grupos $G \rightarrow H/[H, H]$, el **morfismo de transferencia** de G en H . Fijemos un **transversal a izquierda**¹ T de H en G .

lemma:sigma

Lema 33.1. Sean G un grupo y H un subgrupo de índice n . Sean $S = \{s_1, \dots, s_n\}$ y $T = \{t_1, \dots, t_n\}$ transversales de H en G . Dado $g \in G$, existen únicos $h_1, \dots, h_n \in H$ y una permutación $\sigma \in \mathbb{S}_n$ tales que

$$gt_i = s_{\sigma(i)}h_i, \quad i \in \{1, \dots, n\}.$$

Demostración. Si $i \in \{1, \dots, n\}$ existe un único $j \in \{1, \dots, n\}$ tal que $gt_i \in s_jH$. Luego existe un único $h_i \in H$ tal que $gt_i = s_jh_i$. Al tomar $\sigma(i) = j$ queda entonces definida una función $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. Para ver que $\sigma \in \mathbb{S}_n$ basta ver que σ es inyectiva. Si $\sigma(i) = \sigma(k) = j$, como $gt_i = s_jh_i$ y $gt_k = s_jh_k$, tenemos que $t_i^{-1}t_k = h_i^{-1}h_k \in H$ y luego $i = k$ pues $t_iH = t_kH$. \square

definition:nu_T

Definición 33.2. Sea G un grupo y sea H un subgrupo de G de índice finito n . Si $T = \{t_1, \dots, t_n\}$ es un transversal de H en G , se define la función

$$v_T: G \rightarrow H/[H, H], \quad v_T(g) = \prod_{i=1}^n h_i$$

donde $gt_i = t_jh_i$.

lemma:nu_T

Lema 33.3. Sea G un grupo y sea H un subgrupo de G de índice finito. Si T y S son transversales de H en G , entonces $v_T = v_S$.

Demostración. Supongamos que $gs_i = s_{\sigma(i)}h_i$ para todo i y escribamos $s_i = t_ik_i$, $k_i \in H$. Entonces, si $l_i = k_{\sigma(i)}h_ik_i^{-1}$,

$$gt_i = gs_ik_i^{-1} = s_{\sigma(i)}h_ik_i^{-1} = t_{\sigma(i)}k_{\sigma(i)}h_ik_i^{-1} = t_{\sigma(i)}l_i$$

¹ Un transversal a izquierda de H en G es simplemente un conjunto de representantes de coclases a izquierda de H en G .

para todo $i \in \{1, \dots, n\}$. Además

$$s_{\sigma(i)}^{-1} g s_i = k_{\sigma(i)}^{-1} t_{\sigma(i)}^{-1} g t_i k_i.$$

Como $H/[H, H]$ es un grupo abeliano, tenemos

$$\begin{aligned} v_S(g) &= \prod_{i=1}^n s_{\sigma(i)}^{-1} g s_i = \prod_{i=1}^n k_{\sigma(i)}^{-1} t_{\sigma(i)}^{-1} g t_i k_i \\ &= \prod_{i=1}^n k_{\sigma(i)}^{-1} \prod_{i=1}^n k_i \prod_{i=1}^n t_{\sigma(i)}^{-1} g t_i = \prod_{i=1}^n t_{\sigma(i)}^{-1} g t_i = v_T(g). \end{aligned}$$

□

El lema 33.3 demuestra que si H es un subgrupo de G de índice finito, queda bien definida la función

$$v: G \rightarrow H/[H, H], \quad v(g) = v_T(g),$$

donde T es algún transversal de H en G .

theorem:transfer

Teorema 33.4. Sea G un grupo y sea H un subgrupo de G de índice finito. Entonces $v(xy) = v(x)v(y)$ para todo $x, y \in G$.

Demostración. Sea $T = \{t_1, \dots, t_n\}$ un transversal de H en G . Sean $x, y \in G$. Por el lema 33.1 existen únicos $h_1, \dots, h_n, k_1, \dots, k_n \in H$ y existen $\sigma, \tau \in \mathbb{S}_n$ tales que $xt_i = t_{\sigma(i)} h_i$, $yt_i = t_{\tau(i)} k_i$. Como

$$xyt_i = xt_{\tau(i)} k_i = t_{\sigma\tau(i)} h_{\tau(i)} k_i,$$

y el grupo $H/[H, H]$ es abeliano,

$$v(xy) = \prod_{i=1}^n h_{\tau(i)} k_i = \prod_{i=1}^n h_{\tau(i)} \prod_{i=1}^n k_i = v(x)v(y).$$

□

El teorema 33.4 afirma que v es un morfismo de grupos. Queda entonces justificada la siguiente definición:

Definición 33.5. Sea G un grupo y sea H un subgrupo de índice finito. El **morfismo de transferencia** es el morfismo $v: G \rightarrow H/[H, H]$, $v(g) = v_T(g)$, donde T es algún transversal de H en G .

Ejemplo 33.6. Sea p un número primo. Sean $G = \mathbb{F}_p^\times$ y $H = \{-1, 1\}$. Entonces $(G:H) = \frac{p-1}{2}$. Calculemos el morfismo de transferencia:

$$v: G \rightarrow H, \quad v(x) = x^{\frac{p-1}{2}} = \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ es un cuadrado,} \\ -1 & \text{en otro caso.} \end{cases}.$$

Elegimos un transversal $T = \{1, 2, \dots, \frac{p-1}{2}\}$. Para $x \in G, t \in T$ definimos

$$\varepsilon(x, t) = \begin{cases} 1 & \text{si } xt \in T, \\ -1 & \text{si } xt \notin T. \end{cases}$$

Al calcular el morfismo de transferencia obtenemos el **lema de Gauss**:

$$\left(\frac{x}{p}\right) = \prod_{t \in T} \varepsilon(x, t).$$

theorem:P_noabeliano

Teorema 33.7. Sea G un grupo finito. Sea p un primo que divide al orden de $[G, G] \cap Z(G)$. Si $P \in \text{Syl}_p(G)$ entonces P es no abeliano.

Demostración. Supongamos que P es abeliano y sea $T = \{t_1, \dots, t_n\}$ un transversal de P en G . Como $[G, G] \cap Z(G)$ es un subgrupo normal de G , podemos suponer que $P \cap [G, G] \cap Z(G) \neq 1$. Sea $z \in P \cap [G, G] \cap Z(G)$ tal que $z \neq 1$.

Sea $v: G \rightarrow P$ el morfismo de transferencia. Vamos a calcular $v(z)$ con el lema 33.1. Para cada $i \in \{1, \dots, n\}$ sean $x_1, \dots, x_n \in P$ y sea $\sigma \in \mathbb{S}_n$ tales que $zt_i = t_{\sigma(i)}x_i$. Como $z \in Z(G)$, se tiene $t_i = t_{\sigma(i)}x_i z^{-1}$ y luego la unicidad del lema 33.1 implica que $\sigma = \text{id}$ y $x_i = z$ para todo i . Luego

$$v(z) = z^{|T|} = z^{(G:P)}.$$

Como P es abeliano, $[G, G] \subseteq \ker v$. Luego $v(z) = 1$. Esto es una contradicción pues $1 \neq z \in P$ y $z^{(G:P)} = 1$ implica que z tiene orden no divisible por p . \square

lemma:evaluation

Lema 33.8. Sea G un grupo y sea H un subgrupo de índice n . Sea $T = \{t_1, \dots, t_n\}$ un transversal de H en G . Para cada $g \in G$ existen $s_1, \dots, s_m \in T$ y enteros positivos n_1, \dots, n_m (que dependen de g) tales que $s_i^{-1} g^{n_i} s_i \in H$, $n_1 + \dots + n_m = n$ y

$$v(g) = \prod_{i=1}^m s_i^{-1} g^{n_i} s_i.$$

Demostración. Para cada i existen $h_1, \dots, h_n \in H$ y $\sigma \in \mathbb{S}_n$ tales que $gt_i = t_{\sigma(i)}h_i$. Escribimos σ como producto de ciclos disjuntos

$$\sigma = \alpha_1 \cdots \alpha_m.$$

Para cada $i \in \{1, \dots, n\}$, escribamos $\alpha_i = (j_1 \cdots j_{n_i})$. Como

$$gt_{j_k} = t_{\sigma(j_k)}h_{j_k} = \begin{cases} t_{j_1}h_{n_i} & \text{si } i = n_i, \\ t_{j_{k+1}}h_k & \text{en otro caso,} \end{cases}$$

entonces

$$t_{j_1}^{-1} g^{n_i} t_{j_1} = t_{j_1}^{-1} g g^{n_i-1} t_{j_1} = t_{j_1}^{-1} g t_{j_r} h_{j_{r-1}} \cdots h_{j_1} = h_{j_r} \cdots h_{j_1} \in H,$$

y definimos $s_i = t_{j_i}$. Como $v(g) = h_1 \cdots h_n$, de aquí se deduce inmediatamente el lema. \square

proposition: $v(g) = g^n$

Proposición 33.9. Sea G un grupo y sea H un subgrupo abeliano de índice n tal que $H \subseteq Z(G)$. Entonces $v(g) = g^n$ para todo $g \in G$.

Demostración. Sea $g \in G$. Por el lema anterior (lema 33.8) existen $s_1, \dots, s_m \in H$ tales que $s_i^{-1} g^{n_i} s_i \in H$ y $v(g) = \prod_{i=1}^m s_i^{-1} g^{n_i} s_i$. Como H es normal en G por ser central,

$$g^{n_i} = s_i(s_i^{-1} g^{n_i} s_i)s_i^{-1} \in H \subseteq Z(G).$$

Luego

$$v(g) = \prod_{i=1}^m s_i^{-1} g^{n_i} s_i = \prod_{i=1}^m g^{n_i} = g^{\sum_{i=1}^m n_i} = g^n.$$

\square

Corolario 33.10. Si un grupo G tiene un subgrupo H de índice n tal que $H \subseteq Z(G)$ entonces $g \mapsto g^n$ es un morfismo de grupos.

Demostración. La función $g \mapsto g^n$ es el morfismo de transferencia, ver la proposición 33.9 y el teorema 33.4. \square

corollary: $[x, y]^n = 1$

Corolario 33.11. Sea G un grupo tal que $(G : Z(G)) = n$. Si $x, y \in G$ entonces $[x, y]^n = 1$.

Demostración. Como $Z(G)$ es abeliano, el núcleo del morfismo de transferencia $v: G \rightarrow Z(G)$, $v(g) = g^n$, contiene al conmutador $[G, G]$. \square

corollary: semidirecto

Corolario 33.12. Sea G un grupo finito y sea H un subgrupo abeliano de índice n , donde n es coprimo con $|H|$. Sea $N = \ker(v: G \rightarrow H)$. Entonces $G \simeq N \rtimes H$.

Demostración. Como H es abeliano, $H = H/[H, H]$ y el morfismo de transferencia es $v: G \rightarrow H$. Por el lema 33.8, podemos escribir

$$v(h) = \prod_{i=1}^m s_i^{-1} h^{n_i} s_i = \prod_{i=1}^m h^{n_i} = h^{\sum_{i=1}^m n_i} = h^n.$$

La composición $H \hookrightarrow G \xrightarrow{v} H$ es morfismo de grupos.

Vamos a demostrar que es un isomorfismo. Es inyectiva pues si $h^n = 1$ entonces $|h|$ divide a $|H|$ y divide a n ; y como n y $|H|$ son coprimos, $h = 1$. Veamos que es sobreyectiva. Como n y $|H|$ son coprimos, existe $m \in \mathbb{Z}$ tal que $nm \equiv 1 \pmod{|H|}$. Si $h \in H$ entonces $h^m \in H$ y $v(h^m) = h^{nm} = h$.

Tenemos entonces que $G \simeq N \rtimes H$ pues N es normal en G , $N \cap H = 1$ y $G = NH$ (pues $|NH| = |N||H|$ y $G/N \simeq H$). \square

Corolario 33.13 (Frobenius). Sea H un subgrupo central de un grupo finito G . Si $|H|$ y $|G/H|$ son coprimos entonces $G \simeq H \times G/H$.

Demostración. Es consecuencia inmediata del corolario 33.12 pues H es normal por ser un subgrupo central. \square

Capítulo 34

Un teorema de Schur

lemma: [s, t]

Lema 34.1. Sea G un grupo y sea T un transversal de $Z(G)$ en G . Entonces todo conmutador de G es de la forma $[s, t]$, $s, t \in T$. En particular, G tiene finitos conmutadores si $Z(G)$ es de índice finito.

Demostración. Todo elemento de G puede escribirse como sx , $s \in T$, $x \in Z(G)$. Para demostrar la primera afirmación basta observar que

$$[sx, ty] = [s, t]$$

pues $x, y \in Z(G)$. La segunda afirmación es evidente ya que $|T| = (G : Z(G))$. \square

theorem:Dietzmann

Teorema 34.2 (Dietzmann). Sea G un grupo y sea $X \subseteq G$ un subconjunto finito de G cerrado por conjugación. Si existe $n \in \mathbb{N}$ tal que $x^n = 1$ para todo $x \in X$, entonces $\langle X \rangle$ es un subgrupo finito de G .

Demostración. Sea $S = \langle X \rangle$. Como $x^{-1} = x^{n-1}$, todo elemento de S puede escribirse como producto (finito) de elementos de X .

Fijemos $s \in S$. Vamos a demostrar que si $x \in X$ aparece $k \geq 1$ veces en la representación de s , podemos escribir a s como producto de m elementos de X donde los primeros k son iguales a x . Supongamos que

$$s = x_1 x_2 \cdots x_{t-1} x x_{t+1} \cdots x_m,$$

donde cada $x_j \neq x$ para todo $j \in \{1, \dots, t-1\}$. Entonces

$$s = x(x^{-1}x_1x)(x^{-1}x_2x) \cdots (x^{-1}x_{t-1}x)x_{t+1} \cdots x_m$$

es producto de m elementos de X pues X es cerrado por conjugación, y el primer elemento es nuestro x . Este mismo argumento implica que s puede escribirse como

$$s = x^k y_{k+1} \cdots y_m,$$

donde los y_j son elementos de $X \setminus \{x\}$.

Sea $s \in S$ y escribamos a s como producto de m elementos de X , donde m es el mínimo posible. Para ver que S es finito basta ver que $m \leq (n-1)|X|$.

Si suponemos que $m > (n-1)|X|$, al menos un $x \in X$ aparecería n veces en la representación de s . Sin pérdida de generalidad, podríamos escribir

$$s = x^n x_{n+1} \cdots x_m = x_{n+1} \cdots x_m,$$

una contradicción a la minimalidad de m . \square

theorem:Schur_commutador

Teorema 34.3 (Schur). *Si $Z(G)$ tiene índice finito en G entonces $[G, G]$ es finito.*

Demostración. Sea $X = \{[x, y] : x, y \in G\}$. Por el lema 34.1), X es finito. Además X es cerrado por conjugación pues

$$g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

para todo $g, x, y \in G$. Si $n = (G : Z(G))$ entonces $x^n = 1$ para todo $x \in X$ por el corolario 33.11. Luego el teorema queda demostrado al aplicar el teorema 34.2. \square

Corolario 34.4 (Sury). *Si el conjunto de conmutadores de un grupo G es finito, entonces $[G, G]$ es también finito.*

Demostración. Sea C el conjunto de conmutadores de G y sea H el subgrupo de G generado por C . Sabemos que H es finitamente generado, digamos por los elementos h_1, \dots, h_n . Como $h \in Z(H)$ si y sólo si $h \in C_H(H_i)$ para todo $i \in \{1, \dots, n\}$, se tiene que $Z(H) = \cap_{i=1}^n C_H(h_i)$. Además, si $h \in H$, entonces $hh_ih^{-1} = ch_i$ para algún $c \in C$. Luego la clase de conjugación de cada h_i tiene a lo sumo tantos elementos como C . Esto implica que

$$|H/Z(H)| = |H/\cap_{i=1}^n C_H(H_i)| \leq \prod_{i=1}^n (H : C_H(h_i)) \leq |C|^n.$$

Como entonces $H/Z(H)$ es finito, $[H, H]$ es finito. Luego $[G, G] = \langle C \rangle \subseteq [H, H]$ es también un grupo finito. \square

El corolario anterior puede utilizarse también para dar una demostración alternativa del teorema que demostraremos elementalmente a continuación.

Teorema 34.5 (Hilton–Niroomand). *Sea G un grupo finitamente generado. Si $[G, G]$ es finito y $G/Z(G)$ está generado por n elementos, entonces*

$$|G/Z(G)| \leq |[G, G]|^n.$$

Demostración. Supongamos que $G/Z(G) = \langle x_1Z(G), \dots, x_nZ(G) \rangle$. Sea

$$f: G/Z(G) \rightarrow [G, G] \times \cdots \times [G, G], \quad y \mapsto ([x_1, y], \dots, [x_n, y]).$$

Primero observamos que f está bien definida: si $y \in G$ y $z \in Z(G)$ entonces

$$f(yz) = [x_i, yz] = [x_i, y] = f(y).$$

Ahora veamos que f es inyectiva: Supongamos que $f(xZ(G)) = f(yZ(G))$. Entonces $[x_i, x] = [x_i, y]$ para todo $i \in \{1, \dots, n\}$. Para cada i calculamos

$$\begin{aligned} [x^{-1}y, x_i] &= x^{-1}[y, x_i]x[x^{-1}, x_i] \\ &= x^{-1}[y, x_i][x_i, x]x = x^{-1}[x_i, y]^{-1}[x_i, x]x = x^{-1}[x_i, y]^{-1}[x_i, y]x = 1. \end{aligned}$$

Luego $x^{-1}y \in Z(G)$ pues, como todo $g \in G$ puede escribirse como $g = x_k z$ para algún $k \in \{1, \dots, n\}$ y algún $z \in Z(G)$, se tiene que $[x^{-1}y, g] = [x^{-1}y, x_k z] = [x^{-1}y, x_k] = 1$. Esto implica que f es inyectiva y luego $|G/Z(G)| \leq |[G, G]|^n$. \square

Veamos una aplicación del morfismo de transferencia a grupos infinitos.

Teorema 34.6. *Sea G un grupo sin torsión que contiene un subgrupo de índice finito isomorfo a \mathbb{Z} . Entonces $G \simeq \mathbb{Z}$.*

Demostración. Podemos suponer que G contiene un subgrupo normal de índice finito isomorfo a \mathbb{Z} pues si H un subgrupo de G de índice finito isomorfo a \mathbb{Z} , $K = \bigcap_{x \in G} xHx^{-1}$ es normal en G , K es no trivial (pues $K = \text{Core}_G(H)$ y G no tiene torsión) y luego $K \simeq \mathbb{Z}$ (pues $K \subseteq H$) y $(G : K) = (G : H)(H : K)$ es finito.

La acción de G en K por conjugación induce un morfismo $\varepsilon : G \rightarrow \text{Aut}(K)$. Como $\text{Aut}(K) = \{-1, 1\}$ pues $K \simeq \mathbb{Z}$, hay que considerar dos casos.

Supongamos primero que $\varepsilon = \text{id}$. Como entonces $K \subseteq Z(G)$, sea $\nu : G \rightarrow K$ el morfismo de transferencia. Por la proposición 33.9, $\nu(g) = g^n$, donde n es el índice de K en G . Como G no tiene torsión, ν es inyectiva. Luego $G \simeq \mathbb{Z}$ por ser isomorfo a un subgrupo de K .

Supongamos ahora que $\varepsilon \neq \text{id}$. Sea $N = \ker \varepsilon \neq G$. Como $K \simeq \mathbb{Z}$ es abeliano, $K \subseteq N$. Al aplicar el resultado del párrafo anterior al caso $\varepsilon|_N = 1$, se concluye que $N \simeq \mathbb{Z}$ pues N posee un subgrupo de índice finito isomorfo a \mathbb{Z} . Sea $g \in G \setminus N$. Como N es normal en G , g actúa por conjugación en N y entonces se tiene un morfismo de grupos $c_g \in \text{Aut}(N) \simeq \{-1, 1\}$. Como $K \subseteq N$ y g actúa de forma no trivial en K , $c_g(n) = gn g^{-1} = n^{-1}$ para todo $n \in N$. Como $g^2 \in N$, entonces

$$g^2 = gg^2g^{-1} = g^{-2}.$$

Luego $g^4 = 1$, una contradicción porque $g \neq 1$ y G no tiene torsión. \square

Capítulo 35

El teorema del complemento normal

lemma:normal_complement

Lema 35.1. Sea G un grupo finito y sea p un primo que divide al orden de G . Sea $P \in \text{Syl}_p(G)$. Si $g, h \in C_G(P)$ son conjugados en G entonces son conjugados en $N_G(P)$.

Demostración. Sea $x \in G$ tal que $g = xhx^{-1}$. Entonces $g \in C_G(xPx^{-1})$. Luego P y xPx^{-1} son subgrupos de Sylow de $C_G(g)$. Por el teorema de Sylow, existe $c \in C_G(g)$ tal que $P = cxP(cx)^{-1}$. Tenemos $cx \in N_G(P)$ y

$$(cx)h(cx)^{-1} = c(xhx^{-1})c^{-1} = cgc^{-1} = g.$$

□

Definición 35.2. Sea G un grupo finito y sea p un primo que divide al orden de G . Un p -**complemento normal** es un subgrupo normal N de orden coprimo con p y tal que $(G : N)$ es una potencia de p .

Definición 35.3. Un grupo finito se dice p -**nilpotente** si tiene un p -complemento normal.

Proposición 35.4. Si G tiene un p -complemento normal N , entonces N es un subgrupo característico de G .

Demostración. Supongamos que $|G| = p^\alpha n$, donde n es coprimo con p , y sea $\pi: G \rightarrow G/N$ el morfismo canónico. Por hipótesis, N tiene orden n . Vamos a demostrar que N es el único subgrupo de G de orden n . Si K es un subgrupo de G de orden n , entonces $\pi(K) \simeq K/K \cap N$ y luego el orden de $\pi(K)$ divide a m . Pero además el orden de $\pi(K)$ divide al primo p pues $\pi(K) \leq G/N$. Luego $\pi(K)$ es trivial y entonces $K = N$ y luego G tiene un único subgrupo de orden n . En particular, N es un subgrupo característico de G . □

inside:normal_complement

Teorema 35.5 (Burnside). Sea G un grupo finito y sea p un primo que divide a $|G|$. Sea $P \in \text{Syl}_p(G)$ tal que $P \subseteq Z(N_G(P))$. Entonces G es p -nilpotente.

Demostración. Como P es abeliano, sea $v: G \rightarrow P$ el morfismo de transferencia. Sea $g \in P$. Por el lema 33.8 existen $s_1, \dots, s_m \in G$ y existen n_1, \dots, n_m tales que $n_1 + \dots + n_m = n$, $s_i^{-1} g^{n_i} s_i \in P$ y

$$v(g) = \prod_{i=1}^m s_i^{-1} g^{n_i} s_i.$$

Como P es abeliano, $P \subseteq C_G(P)$. Por el lema 35.1, existe $c_i \in N_G(P)$ tal que

$$s_i^{-1} g^{n_i} s_i = c_i^{-1} g^{n_i} c_i,$$

y luego $s_i^{-1} g^{n_i} s_i = g_i^{n_i}$ pues $P \subseteq Z(N_G(P))$. Tenemos entonces que $v(g) = g^n$, donde $n = (G : P)$. Como n y $|P|$ son coprimos, existen $r, s \in \mathbb{Z}$ tales que $rn + s|P| = 1$. Esto implica que $v|_P$ es sobreyectiva pues

$$g = (g^r)^n = v(g^r).$$

Por el teorema de isomorfismos, $P/\ker v \cap P \simeq v(P) = P$. Luego $\ker v \cap P = 1$. Además $v(G) = v(P)$ pues $P \supseteq v(G) \supseteq v(P) = P$.

Veamos que $\ker v$ es un p -complemento normal en G . Es claro que $\ker v$ es normal en G . Como $(G : \ker v) = |v(G)| = |P|$ y P es un p -subgrupo de Sylow, se concluye que $\ker v$ tiene orden coprimo con p . \square

lemma:NC

Lema 35.6. Sea G un grupo y H un subgrupo de G . Entonces $C_G(H)$ es un subgrupo normal de $N_G(H)$ y $N_G(H)/C_G(H)$ es isomorfo a un subgrupo de $\text{Aut}(H)$.

Demostración. Sea $\phi: N_G(H) \rightarrow \text{Aut}(H)$, $\phi(g) = c_g|_H$, donde $c_g(h) = ghg^{-1}$. La función ϕ está bien definida (pues su dominio es $N_G(H)$) y es morfismo de grupos. Como $\ker \phi = C_G(H)$, se tiene que $C_G(H)$ es normal en $N_G(H)$. Por el primer teorema de isomorfismo, $N_G(H)/C_G(H) \simeq \phi(N_G(H)) \leq \text{Aut}(H)$. \square

corollary:Sylow_ciclico

Corolario 35.7. Sea G un grupo finito y sea p el menor primo que divide a $|G|$. Si algún $P \in \text{Syl}_p(G)$ es cíclico, G es p -nilpotente.

Demostración. Supongamos que $|P| = p^m$. Por el lema 35.6, $N_G(P)/C_G(P)$ es isomorfo a un subgrupo de $\text{Aut}(P)$. Como P es cíclico, $|N_G(P)/C_G(P)|$ divide a

$$|\text{Aut}(P)| = \phi(|P|) = p^{m-1}(p-1).$$

Como $P \subseteq C_G(P)$ por ser P abeliano, p es coprimo con $|N_G(P)/C_G(P)|$. Luego $|N_G(P)/C_G(P)|$ divide a $p-1$. Pero $p-1$ y $|G|$ son coprimos, pues p es el menor primo que divide a $|G|$. Como además $|N_G(P)/C_G(P)|$ divide al orden de G , se concluye que $|N_G(P)/C_G(P)| = 1$, es decir: $N_G(P) = C_G(P)$.

Como P es abeliano, $P \subseteq Z(C_G(P)) = Z(N_G(P))$. El teorema de Burnside 35.5 implica entonces que G es p -nilpotente. \square

Ejercicio 35.8. Sea G un grupo finito tal que todos sus subgrupos de Sylow son cíclicos. Entonces G es resoluble.

Vamos a demostrar algo más fuerte:

Sylow_ciclicos:resoluble

Corolario 35.9. *Sea G un grupo finito tal que todos sus subgrupos de Sylow son cíclicos. Entonces G es superresoluble.*

Demostración. Supongamos que G es no trivial y hagamos inducción en $|G|$. Si p es el menor primo que divide a $|G|$, por el corolario 35.7 el grupo G tiene un p -complemento normal N . Por hipótesis inductiva, N es resoluble. Como G/N es un p -grupo, es resoluble. Luego G es resoluble. \square

Corolario 35.10. *Sea G un grupo finito cuyo orden es libre de cuadrados. Entonces G es resoluble.*

Demostración. Es consecuencia del corolario 35.9 pues en este caso todo subgrupo de Sylow es cíclico. \square

Corolario 35.11. *Sea G un grupo finito simple no abeliano y sea p el menor primo que divide a $|G|$. Entonces p^3 divide a $|G|$ o bien 12 divide a $|G|$.*

Demostración. Sea $P \in \text{Syl}_p(G)$. Por el corolario 35.7, P no es cíclico, y entonces $|P| \geq p^2$. Si p^3 no divide a $|G|$, $P \simeq C_p \times C_p$ es un \mathbb{F}_p -espacio vectorial de dimensión dos. Como $|N_G(P)/C_G(P)|$ divide al orden de G , los divisores primos de $|N_G(P)/C_G(P)|$ son $\geq p$. Además, como $N_G(P)/C_G(P)$ es isomorfo a un subgrupo de $\text{Aut}(P)$ por el lema 35.6 y $\text{Aut}(P) \simeq \text{GL}_2(p)$ tiene orden $(p^2 - 1)(p^2 - p) = p(p+1)(p-1)^2$, $|N_G(P)/C_G(P)|$ divide a $p(p+1)(p-1)^2$. Como P es abeliano, $P \subseteq C_G(P)$. Entonces $|N_G(P)/C_G(P)|$ es coprimo con p y luego $|N_G(P)/C_G(P)|$ divide a $(p+1)(p-1)^2$. Como p es el menor primo que divide a $|G|$, los números $p-1$ y $|N_G(P)/C_G(P)|$ son coprimos, y entonces $|N_G(P)/C_G(P)|$ divide a $p+1$. Además, por el teorema de Burnside 35.5, $|N_G(P)/C_G(P)| \neq 1$. Esto implica que $p=2$ pues si p es impar el menor primo que divide a $|N_G(P)/C_G(P)|$ es $\geq p+2$. Como entonces $p=2$, se concluye que $|N_G(P)/C_G(P)|=3$ y luego $|G|$ es divisible por $12=2^2 \cdot 3$. \square

theorem: [GG]PZNG(P)=1

Teorema 35.12. *Sea G un grupo finito y sea P un subgrupo de Sylow abeliano. Entonces $[G, G] \cap P \cap Z(N_G(P)) = 1$.*

Demostración. Sea $x \in [G, G] \cap P \cap Z(N_G(P))$ y sea $v: G \rightarrow P$ el morfismo de transferencia. Por el lema 33.8 existen $s_1, \dots, s_m \in G$ y existen n_1, \dots, n_m tales que $n_1 + \dots + n_m = (G:P)$, $s_i^{-1} g^{n_i} s_i \in P$ y

$$v(x) = \prod_{i=1}^m s_i^{-1} x^{n_i} s_i.$$

Como P es abeliano, $P \subseteq C_G(P)$. Entonces x^{n_i} y $s_i^{-1} x^{n_i} s_i$ son conjugados en $N_G(P)$ por el lema 35.1. Como x^{n_i} es central en $N_G(P)$ y $[G, G] \subseteq \ker v$, se concluye que $x=1$ pues $1 = v(x) = x^{(G:P)}$ y $x \in P$. \square

Corolario 35.13. *Sea G un grupo finito no abeliano y sea $P \in \text{Syl}_2(G)$ tal que $P \simeq C_{a_1} \times \dots \times C_{a_k}$ con $a_1 > a_2 \geq a_3 \geq \dots \geq a_k \geq 2$. Entonces G no es simple.*

Demostración. Sea $S = \{x^{n/2} : x \in P\}$. Es fácil ver que S es un subgrupo de P y que S es característico en P , es decir: $f(S) \subseteq S$ para todo $f \in \text{Aut}(P)$. Como $S \simeq C_2$, podemos escribir $S = \{1, s\}$. Entonces $s \in Z(N_G(P))$ pues $gs g^{-1} \in S$ para todo $g \in N_G(P)$. Por el teorema 35.12, $s \notin [G, G]$ y luego $[G, G] \neq G$. Si G fuera simple, G sería abeliano pues $[G, G] = 1$. \square

Vimos en el corolario 35.9 que todo grupo tal que todos sus subgrupos de Sylow son cíclicos es resoluble.

Definición 35.14. Un Z -grupo es un grupo finito G tal que todos sus subgrupos de Sylow son cíclicos.

Un grupo G se dice *meta-cíclico* si G tiene un subgrupo normal N cíclico tal que G/N es cíclico.

Lema 35.15. Si G es un grupo resoluble, entonces $C_G(F(G)) = F(G)$.

Demostración. \square

theorem:Z=>metacyclic

Teorema 35.16. Todo Z -grupo es meta-cíclico.

Demostración. Sea G un Z -grupo. Por el corolario 35.9, G es resoluble y entonces, por el lema, el subgrupo de Fitting $F(G)$ satisface $C_G(F(G)) \subseteq F(G)$.

Demostremos que $F(G)$ es cíclico. En efecto, como $F(G)$ es nilpotente, $F(G)$ es producto directo de sus subgrupos de Sylow. Como todo subgrupo de Sylow de $F(G)$ es un p -subgrupo de G , todo Sylow de $F(G)$ es cíclico (por estar contenido en algún subgrupo de Sylow de G).

Como $F(G)$ es cíclico, $F(G)$ es en particular abeliano y luego $F(G) \subseteq C_G(F(G))$. Si G actúa en $F(G)$ por conjugación, se tiene un morfismo $\gamma: G \rightarrow \text{Aut}(F(G))$ tal que $\ker \gamma = C_G(F(G)) = F(G)$ (pues $\gamma_g(x) = gxg^{-1}$). En particular, $G/F(G)$ es abeliano por ser isomorfo a un subgrupo del grupo abeliano $\text{Aut}(F(G))$. Como además los subgrupos de Sylow de $G/F(G)$ son cíclicos (pues son cocientes de los subgrupos de Sylow de G), $G/F(G)$ es cíclico. \square

Algunas soluciones

5.21 Sabemos que G tiene k clases de isomorfismos de módulos simples y que exactamente m son de dimensión uno. Luego $n = \sum_{i=1}^k n_i^2 \geq m + 4(m - k)$.

Grupos nilpotentes

20.6 Por inducción se demuestra que $G^{(i)} \subseteq \gamma_i(G)$ para todo $i \geq 1$. Luego si existe c tal que $\gamma_{c+1}(G)$ entonces G es resoluble pues $G^{(c+1)} = \{1\}$.

20.11 Todas las afirmaciones se demuestran fácilmente por inducción. El paso inductivo para la primera es el siguiente: si $f \in \text{Aut}(G)$ entonces

$$f(\gamma_{i+1}(G)) = f([G, \gamma_i(G)]) = [f(G), f(\gamma_i(G))] \subseteq [G, \gamma_i(G)] = \gamma_{i+1}(G).$$

Para la segunda:

$$\gamma_{i+1}(G) = [G, \gamma_i(G)] \subseteq [G, \gamma_{i-1}(G)] = \gamma_i(G).$$

Similarmente, el paso inductivo para demostrar la tercera afirmación:

$$f(\gamma_{i+1}(G)) = f([G, \gamma_i(G)]) = [f(G), f(\gamma_i(G))] = [H, \gamma_i(H)] = \gamma_{i+1}(H).$$

20.12 Por inducción se demuestra fácilmente que $\gamma_i(H \times K) \subseteq \gamma_i(H) \times \gamma_i(K)$ para todo $i \geq 1$.

20.28 Sea $\pi: G \rightarrow G/K$. Usar π^{-1} para levantar una serie central de G/K y obtener una serie central para G .

?? Como $M \cap Z(G)$ es normal en G , la minimalidad de M implica que hay dos posibilidades: $M \cap Z(G)$ es trivial o bien $M = M \cap Z(G) \subseteq Z(G)$. Por el teorema 20.29, $M \cap Z(G) \neq \{1\}$.

?? Sea $x \in N_G(M)$. Como $P \subseteq M$ y M es normal en $N_G(M)$, $xPx^{-1} \subseteq M$. Como P y xPx^{-1} son p -subgrupos de Sylow de M , existe $m \in M$ tal que

$$mPm^{-1} = xPx^{-1}.$$

Luego $x \in M$ pues $m^{-1}x \in N_G(P) \subseteq M$.

20.45 Para demostrar que (1) \implies (2) simplemente usamos el lema 20.18. Para demostrar que (2) \implies (3) hacemos lo siguiente: si M es un subgrupo maximal, como $M \subsetneq N_G(M)$ por hipótesis, $N_G(M) = G$ por maximalidad. Finalmente demostramos que (3) \implies (1). Sea $P \in \text{Syl}_p(G)$. Si P no es normal en G , $N_G(P) \neq G$ y entonces existe un subgrupo maximal M tal que $N_G(P) \subseteq M$. Como M es normal en G , el ejercicio ?? implica que $M = N_G(M) = G$, una contradicción. Luego P es normal en G y entonces G es nilpotente por el teorema 20.43.

20.47

- 1) Sabemos que $Z(G) \neq 1$. Sea $g \in Z(G)$ tal que $g \neq 1$. Supongamos que el orden de g es p^k para algún $k \geq 1$. Entonces $g^{p^{k-1}}$ tiene orden p y luego genera un subgrupo central de orden p .
- 2) Procederemos por inducción en n . Si $n = 1$ el resultado es trivial. Supongamos entonces que el resultado vale para un cierto $n \geq 2$. Por el punto anterior, G posee un subgrupo normal N de orden p . Luego G/N tiene orden p^{n-1} . Sea $\pi: G \rightarrow G/N$ el morfismo canónico. Por hipótesis inductiva, para cada $j \in \{0, \dots, n-1\}$. Por el teorema de la correspondencia, cada subgrupo normal S_j de G/N de orden p^j se corresponde con un subgrupo $\pi^{-1}(S_j)$ de G de orden p^{j+1} pues, como π es sobreyectiva, se tiene $\pi(\pi^{-1}(S_j)) = S_j$, y luego

$$p^j = |S_j| = |\pi(\pi^{-1}(S_j))| = \frac{|\pi^{-1}(S_j)|}{|\pi^{-1}(S_j) \cap N|} = \frac{|\pi^{-1}(S_j)|}{|N|} = \frac{|\pi^{-1}(S_j)|}{p}.$$

20.48 Veamos que (1) \implies (2). Sabemos que G es producto directo de sus subgrupos de Sylow, digamos $G = \prod_{i=1}^k S_i$, donde los S_i son los distintos subgrupos de Sylow de G . Sean $x = (x_1, \dots, x_k), y = (y_1, \dots, y_k) \in G$. Como $|x|$ y $|y|$ son coprimos, para cada $i \in \{1, \dots, k\}$ se tiene $x_i = 1$ o $y_i = 1$. Luego

$$[x, y] = ([x_1, y_1], [x_2, y_2], \dots, [x_k, y_k]) = 1.$$

Demostremos ahora que (2) \implies (1). Supongamos que $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, donde los p_j son primos distintos y para cada j sea $P_j \in \text{Syl}_{p_j}(G)$. Como elementos de órdenes coprimos conmutan, la función $P_1 \times \cdots \times P_k \rightarrow G$, $(x_1, \dots, x_k) \mapsto x_1 \cdots x_k$, es un morfismo inyectivo de grupos. Como entonces $G \simeq P_1 \times \cdots \times P_k$, y cada P_j es nilpotente, G es nilpotente.

Para demostrar que (1) \implies (3) simplemente hay que observar que todo cociente de G es nilpotente y luego utilizar el teorema 20.29. Demostremos que (3) \implies (1). Como todo cociente no trivial de G tiene centro no trivial, en particular $Z_1 = Z(G)$ es no trivial. Si $Z_1 = G$ entonces G es abeliano y no hay nada para demostrar. Si

$Z_1 \neq G$ entonces $G/Z_1 \neq 1$; luego $Z(G/Z_1) \neq 1$. Si $\pi_1: G \rightarrow G/Z_1$ es el morfismo canónico, $Z_2 = \pi_1^{-1}(Z(G/Z_1))$. Inductivamente, si tenemos construido el subgrupo Z_i , $Z_i \neq G$ y $\pi_i: G \rightarrow G/Z_i$ es el morfismo canónico, se define el subgrupo $Z_{i+1} = \pi_i^{-1}(Z(G/Z_i))$. Por construcción, $Z_i \subseteq Z_{i+1}$ para todo i . Como G es finito, existe k tal que $Z_k = G$ y luego G es nilpotente.

Demostremos que (1) \implies (4). Esta implicación es consecuencia inmediata del ejercicio ???. Como G es nilpotente, G producto directo de sus p -grupos de Sylow. Si $d = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ es un divisor del orden de G , basta tomar $H = H_1 \times \cdots \times H_k$, donde cada H_j es un subgrupo normal del p_j -subgrupo de Sylow de G de orden $p_j^{\alpha_j}$. Para demostrar que (4) \implies (1) simplemente se aplica la hipótesis a cada p -subgrupo de G de orden maximal.

Derivaciones

25.6 Sea $N = \iota(K) = \ker p$.

- 1) Veamos que las $\ell(x)N$ son disjuntas. Si $\ell(x)N = \ell(y)N$, existe $n \in N$ tal que $\ell(x) = \ell(y)n$. Luego

$$x = p(\ell(x)) = p(\ell(y)n) = p(\ell(y))p(n) = y.$$

Sea $g \in G$ y sea $x = p(g) \in Q$. Como $x = p(\ell(x))$ y p es morfismo de grupos, $x^{-1} = p(\ell(x)^{-1})$. Luego $g = \ell(x)(\ell(x)^{-1}g)$ y $\ell(x)^{-1}g \in N$ pues

$$p(\ell(x)^{-1}g) = p(\ell(x)^{-1})p(g) = x^{-1}x = 1.$$

- 2) Sea L un transversal a N en G . Si $x \in Q$ entonces existe $g \in G$ tal que $x = p(g)$. Sea $\ell(x) \in L \subseteq G$ tal que $gN = \ell(x)N$. Como $g^{-1}\ell(x) \in N = \ker p$, se concluye que $p(\ell(x)) = x$ pues

$$x^{-1}p(\ell(x)) = p(g)^{-1}p(\ell(x)) = p(g^{-1}\ell(x)) = 1.$$

- 3) Sean $x, y \in Q$ y sean $g, h \in G$ tales que $x = p(g)$, $y = p(h)$. Como por definición $gN = \ell(x)N$, $hN = \ell(y)N$ y p es morfismo de grupos,

$$\ell(xy)N = (gh)N = (gN)(hN) = \ell(x)\ell(y)N.$$

25.10 La primera afirmación es fácil pues, como

$$\varphi(1) = \varphi(11) = \varphi(1)(1 \cdot \varphi(1)) = \varphi(1)^2,$$

se concluye que $\varphi(1) = 1$.

Veamos que $\ker \varphi$ es un subgrupo. Como $\varphi(1) = 1$, K es no vacío. Sean $x, y \in \ker \varphi$. Como $1 = \varphi(y^{-1}y) = \varphi(y^{-1})(y^{-1} \cdot \varphi(y))$, se tiene que

$$\varphi(y^{-1}) = (y^{-1} \cdot \phi(y))^{-1}.$$

Similarmenle se demuestra que

$$\varphi(y^{-1}) = y^{-1} \cdot \phi(y)^{-1}.$$

De estas fórmulas se deduce que si $x \in \ker \varphi$ entonces $x^{-1} \in \ker \varphi$. Luego $\ker \varphi$ es un subgrupo pues si $x, y \in \ker \varphi$, $\varphi(xy) = \varphi(x)(x \cdot \varphi(y)) = 1(x \cdot 1) = 1$.

Extensiones y cohomología

27.10 Pues para todo $a \in A = C^0(G, A)$ se tiene que $da = 0$ si y sólo si $a \in A^G$.

27.22 Veamos que $\ker \beta = 1$. Sea $g \in G$ tal que $\beta(g) = 1$. Como $g \in \ker p = \iota(K)$ pues $p(g) = p_1\beta(g) = p_1(1) = 1$, existe $k \in K$ tal que $g = \iota(k)$. Entonces $1 = \beta(g) = \beta\iota(k) = \iota_1\alpha(k)$. Como ι_1 y α son morfismos inyectivos, $k = 1$ y luego $g = 1$.

Veamos ahora que $\beta(G) = G_1$. Sea $g_1 \in G_1$. Como p es sobreyectiva, $p_1(g_1) = p(g)$ para algún $g \in G$. Como $\beta(g)g_1^{-1} \in \ker p_1 = \iota_1(K_1)$ y α es epimorfismo, existe $k \in K$ tal que $\beta(g)g_1^{-1} = \iota_1(\alpha(k)) = \beta(\iota(k))$. Luego $\beta(g\iota(k)^{-1}) = g_1$.

Referencias

1. J. L. Alperin. The main problem of block theory. In *Proceedings of the Conference on Finite Groups (Univ. Utah, Park City, Utah, 1975)*, pages 341–356, 1976.
2. B. Amberg, S. Franciosi, and F. de Giovanni. *Products of groups*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1992. Oxford Science Publications.
3. H. U. Besche, B. Eick, and E. A. O’Brien. The groups of order at most 2000. *Electron. Res. Announc. Amer. Math. Soc.*, 7:1–4, 2001.
4. H. U. Besche, B. Eick, and E. A. O’Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.
5. S. R. Blackburn, P. M. Neumann, and G. Venkataraman. *Enumeration of finite groups*, volume 173 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2007.
6. J. H. Conway, H. Dietrich, and E. A. O’Brien. Counting groups: gnus, moas, and other exotica. *Math. Intelligencer*, 30(2):6–18, 2008.
7. M. du Sautoy and M. Vaughan-Lee. Non-PORC behaviour of a class of descendant p -groups. *J. Algebra*, 361:287–312, 2012.
8. B. Fein, W. M. Kantor, and M. Schacher. Relative Brauer groups. II. *J. Reine Angew. Math.*, 328:39–57, 1981.
9. W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.
10. P. Flavell. Finite groups in which every two elements generate a soluble subgroup. *Invent. Math.*, 121(2):279–285, 1995.
11. G. Gonthier, A. Asperti, J. Avigad, and et al. A machine-checked proof of the odd order theorem. In *Interactive theorem proving*, volume 7998 of *Lecture Notes in Comput. Sci.*, pages 163–179. Springer, Heidelberg, 2013.
12. R. Guralnick and D. Wan. Bounds for fixed point free elements in a transitive group and applications to curves over finite fields. *Israel J. Math.*, 101:255–287, 1997.
13. R. M. Guralnick, M. W. Liebeck, E. A. O’Brien, A. Shalev, and P. H. Tiep. Surjective word maps and Burnside’s $p^a q^b$ theorem. *Invent. Math.*, 213(2):589–695, 2018.
14. R. M. Guralnick and G. R. Robinson. On the commuting probability in finite groups. *J. Algebra*, 300(2):509–528, 2006.
15. R. M. Guralnick and J. S. Wilson. The probability of generating a finite soluble group. *Proc. London Math. Soc. (3)*, 81(2):405–427, 2000.
16. G. Higman. Enumerating p -groups. I. Inequalities. *Proc. London Math. Soc. (3)*, 10:24–30, 1960.
17. G. Higman. Enumerating p -groups. II. Problems whose solution is PORC. *Proc. London Math. Soc. (3)*, 10:566–582, 1960.
18. I. M. Isaacs. Characters of solvable and symplectic groups. *Amer. J. Math.*, 95:594–635, 1973.

19. I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.
20. I. M. Isaacs. *Characters of solvable groups*, volume 189 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2018.
21. I. M. Isaacs, G. Malle, and G. Navarro. A reduction theorem for the McKay conjecture. *Invent. Math.*, 170(1):33–101, 2007.
22. I. M. Isaacs and G. Navarro. New refinements of the McKay conjecture for arbitrary finite groups. *Ann. of Math. (2)*, 156(1):333–344, 2002.
23. M. W. Liebeck. Applications of character theory of finite simple groups. In *Local representation theory and simple groups*, EMS Ser. Lect. Math., pages 323–352. Eur. Math. Soc., Zürich, 2018.
24. M. W. Liebeck, E. A. O’Brien, A. Shalev, and P. H. Tiep. The Ore conjecture. *J. Eur. Math. Soc. (JEMS)*, 12(4):939–1008, 2010.
25. G. Malle. The proof of Ore’s conjecture (after Ellers-Gordeev and Liebeck-O’Brien-Shalev-Tiep). *Astérisque*, (361):Exp. No. 1069, ix, 325–348, 2014.
26. G. Malle and B. Späth. Characters of odd degree. *Ann. of Math. (2)*, 184(3):869–908, 2016.
27. P. M. Neumann. A lemma that is not Burnside’s. *Math. Sci.*, 4(2):133–141, 1979.
28. J. Pakianathan and K. Shankar. Nilpotent numbers. *Amer. Math. Monthly*, 107(7):631–634, 2000.
29. L. Pyber. Enumerating finite groups of given order. *Ann. of Math. (2)*, 137(1):203–220, 1993.
30. J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.
31. J.-P. Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440, 2003.
32. C. C. Sims. Enumerating p -groups. *Proc. London Math. Soc. (3)*, 15:151–166, 1965.
33. N. M. Stephens. On the Feit-Thompson conjecture. *Math. Comp.*, 25:625, 1971.
34. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, 74:383–437, 1968.
35. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. II. *Pacific J. Math.*, 33:451–536, 1970.
36. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. III. *Pacific J. Math.*, 39:483–534, 1971.
37. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. IV, V, VI. *Pacific J. Math.*, 48, 1973.

Índice alfabético

- 1-coborde, 171
- 1-cociclo, 170
- G -módulo, 179
- π -grupo, 187
- π -número, 187
- π -subgrupo, 187
- p -complemento, 129
- p -nilpotente, 219
- p -radical
 - de un grupo, 157
- Acción
 - 2-transitiva, 76
- Baer
 - teorema de, 198
- Bimódulo, 90
- Brodkey
 - teorema de, 199
- Burnside
 - Teorema de, 104
 - teorema de, 71
 - teorema del complemento normal de, 219
- Character
 - real, 103
- Caracteres
 - matriz de, 43
 - tabla de, 43
- Carácter
 - de una representación, 39
- Centralizador, 135
- Chermak–Delgado
 - medida de, 205
 - subgrupo de, 207
 - teorema de, 208
- Clase de conjugación
 - real, 103
- Clausura normal, 128
- Coborde, 179, 180
- Cocadena, 179
- Cociclo, 180
- Cociclos
 - cohomólogos, 180
- Cohomología, 180
- Cohomólogos
 - cociclos, 180
- Complemento normal, 219
- Condición normalizadora, 134
- Conjetura
 - de Feit–Thompson, 110
 - de Isaacs–Navarro, 54
 - de McKay, 52
 - de Ore, 68
- Cremallera
 - teorema de, 197
- Dato
 - para una extensión, 182
- Dedekind
 - lema de, 152
- Derivación, 170
 - interior, 171
- Desarreglos, 77
- Desigualdad
 - de Cauchy–Schwartz, 81
- Dual
 - de una representación, 38
- Elemento
 - algebraico, 4
 - nil, 17
- Entero algebraico, 47
- Equivalencia

- de extensiones, 182
- Extensión, 169
 - que se parte, 169
- Factor, 182
- Fitting
 - subgrupo de, 157
- Fratini
 - argumento de, 127
 - subgrupo de, 151
 - teorema de, 153
- Frobenius
 - complemento de, 98
 - grupo de, 98
 - núcleo de, 98, 100
 - Teorema de, 98, 101
 - teorema de, 50
- Función
 - central, 41
 - de clases, 41
- Gaschütz
 - teorema de, 153
- Gauss
 - lema de, 212
- Grado
 - de una representación, 31
- Grupo
 - lagrangiano, 177
 - meta-cíclico, 222
 - metabeliano, 119
 - nilpotente, 132
 - perfecto, 135
 - que satisface la condición maximal para subgrupos, 165
 - súper-resoluble, 161
- Hall
 - subgrupo de, 187
 - teorema de, 154, 187, 188
- Hall, P., 131
- Horosevskii
 - teorema de, 202
- Ideal
 - de aumentación, 25
 - nilpotente, 14
- Identidad
 - de Euler, 111
 - de Fibonacci, 111
 - de Hall–Witt, 131
 - de Hamilton, 111
 - de Jacobi, 131
- Involución, 80
- Isomorfismo
 - de extensiones, 182
- Jaboci, G., 131
- Lema
 - de Dedekind, 152
 - de Hall, 143
 - de los no-generadores, 152
 - de los tres subgrupos, 131
 - de Nakayama, 14
 - de Schur, 4
- Levantamiento, 169
- Lucchini
 - teorema de, 200
- Maschke
 - teorema de, 26
- Medida de Chermak–Delgado, 205
- Morfismo
 - de extensiones, 181
 - de álgebras, 3
- Morfismo de transferencia, 211
- Módulo
 - inducido, 92
 - semisimple, 4
 - simple, 4
- Normalizador, 135
- Núcleo
 - de un caracter, 85
- Número
 - cíclico, 145
- Orbital, 75
- Parte
 - antisimétrica, 79
 - simétrica, 79
- Parte irreducible
 - de un caracter, 89
- Producto tensorial
 - de bimódulos, 91
 - de espacios vectoriales, 35
 - de representaciones, 38
 - de transformaciones lineales, 36
 - propiedad universal, 36
- Proyección, 26
- Radical
 - de Jacobson, 13
- Rango, 75
- Representaciones
 - equivalentes, 32

- Representación
 - completamente reducible, 34
 - de un grupo, 31
 - dual, 38
 - fiel, 32
 - irreducible, 33
 - regular de un álgebra, 4
 - trivial, 35
- Restricción, 88
- Schur
 - teorema de, 51
- Schur–Zassenhaus
 - teorema de, 174, 175
- Serie
 - central, 136
 - central ascendente, 135
 - central descendente, 132
 - derivada, 107
- Subespacio invariante, 33
- Subgrupo
 - característico, 125
 - de Chermak–Delgado, 207
 - de Fitting, 157
 - de Frattini, 151
 - de Hall, 187
 - elemental abeliano, 125
 - minimal-normal, 125
 - subnormal, 193
- Subrepresentación, 33
- Sylow
 - base de, 190
 - sistema de, 189
- Sysak, Y., 171
- Tabla de caracteres, 55
- Teorema
 - 5/8, 73
 - de Artin–Wedderburn, 9
 - de Baer, 198
 - de Brauer–Fowler, 82
 - de Brodkey, 199
 - de Burnside, 65, 71, 108, 109, 145
 - de Cameron–Cohen, 77
 - de Chermak–Delgado, 208
 - de Dixon, 74
 - de Erdős–Turan, 73
 - de Fein–Kantor–Schacher, 77
 - de Feit–Thompson, 109
 - de Frattini, 153
 - de Frobenius, 98, 101
 - de Gaschütz, 153
 - de Grün, 135
 - de Guralnick–Robinson, 75
 - de Guralnick–Wan, 78
 - de Guralnick–Wilson, 75
 - de Hall, 154, 187, 188
 - de Higman–Sims, 149
 - de Hirsch, 136
 - de Hurwitz, 113
 - de Itô, 52
 - de Jordan, 76
 - de Kegel–Wielandt, 109
 - de Kolchin, 21
 - de la Cremallera, 197
 - de Liebeck–O’Brien–Shalev–Tiep, 68
 - de los conmutadores de Frobenius, 67
 - de Malle–Späth, 53
 - de Malle–Späth, 53
 - de Maschke, 26
 - de Pyber, 150
 - de reciprocidad de Frobenius, 93
 - de Schur, 51
 - de Schur–Zassenhaus, 174, 175
 - de Sysak, 171
 - de Wedderburn, 11, 19
 - de Wielandt, 153
 - de Wildon, 77
 - de Zenkov, 198
 - primera ortogonalidad Schur, 44
 - segunda ortogonalidad Schur, 45
- Teorema de
 - Baumslag–Wiegold, 142
 - Burnside, 104
 - Frobenius, 50
 - Hilton–Niroomand, 216
 - Horosevskii, 202
 - Lucchini, 200
 - Solomon, 46
- Teorema del complemento normal, 219
- Transversal, 92, 211
- Wielandt
 - teorema de, 153
- Witt, E., 131
- Z-grupo, 222
- Zenkov
 - teorema de, 198
- Álgebra, 3
 - algebraica, 4
 - asociativa, 3
 - conmutativa, 3
 - de grupo, 25
 - de matrices, 3
 - de polinomios, 3
 - de polinomios truncados, 4

dimensión, 3
ideal de un, 3
nil, 17

semisimple, 6
simple, 10
Índice de nilpotencia, 132