

Leandro Vendramin

Teoría de grupos

– Primer cuatrimestre de 2021 –

3 de abril de 2021

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. Representaciones de grupos	25
5. El teorema de Maschke	33
6. Teoría de caracteres	39
7. El grado de un caracter	47
8. Ejemplos de tablas de caracteres	55
9. Conmutadores	61
10. El teorema de Cauchy-Frobenius-Burnside	65
11. El teorema de Brauer-Fowler	73
12. Inducción y restricción	75
13. El teorema de Frobenius	87
14. Algunos teoremas de Burnside	93
15. Un teorema de Hurwitz	99

Referencias	105
Índice alfabético	107

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 $M = S_i \oplus T$. 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 $(1 - ab)c = 1$,

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

Similarmenete, 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 $x_1, \dots, x_m \in I$.

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

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 B dada por el lema anterior. Sea J un ideal nilpotente de B . Como $J \cap I \subseteq I$ es un ideal nilpotente de A , $J \cap I = \{0\}$. 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, no tiene ideales propios no nulos. Luego $J = \{0\}$ y entonces B no tiene ideales nilpotentes. 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

Recordemos que una matriz a se dice nilpotente si $a^n = 0$ para algún $n \in \mathbb{N}$. Necesitamos un lema:

lem:base_de_nilpotentes

Lema 3.3. *El espacio vectorial $M_n(\mathbb{C})$ no posee una base formada por matrices nilpotentes.*

Demostración. Supongamos que existen matrices nilpotentes 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

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

Para cada $i \in \{1, \dots, n^2\}$ sabemos que $\text{traza}(A_i) = 0$ pues A_i es nilpotente. 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

Antes de demostrar el teorema de Kolchin, necesitamos el siguiente resultado sobre álgebras.

Teorema 3.4 (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.

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, si $a_1 a_2 \dots a_N \in A$, entonces

$$\pi(a_1 a_2 \dots a_N) = \pi(a_1) \pi(a_2) \dots \pi(a_N) = 0,$$

pues $(A/J(A))^N = \{0\}$. Luego $a_1 a_2 \dots a_N \in J(A)$, que implica $a_1 a_2 \dots a_N = 0$ pues $J(A)^N = \{0\}$.

Si $J(A) = \{0\}$, entonces, como A es semisimple, el teorema de Mollien implica que existen enteros positivos n_1, \dots, n_k tales que $A \simeq M_{n_1}(\mathbb{C}) \times \dots \times M_{n_k}(\mathbb{C})$. Como A posee una base formada por elementos nil, $M_{n_1}(\mathbb{C}) \times \dots \times M_{n_k}(\mathbb{C})$ también, es decir $M_{n_1}(\mathbb{C}) \times \dots \times M_{n_k}(\mathbb{C})$ posee una base formada por matrices nilpotentes, una contradicción al lema anterior. \square

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

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

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 .

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 es transitiva, pues si (W_1, \dots, W_n) es una bandera completa en V , la matriz $g = (w_1 | \dots | w_n)$ cuyas columnas son los w_j es inversible, pues $\{w_1, \dots, w_n\}$ es una base de V , 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 3.5. $B = U \rtimes T$.

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 $\mathbf{GL}_n(K)$ es un **grupo unipotente** si todo $g \in G$ es unipotente.

Proposición 3.6. 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 $(g - I)^n = 0$, 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 3.7 (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 $gw + \langle v \rangle = gw' + \langle v \rangle$. Por hipótesis inductiva, G 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 \mathcal{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 $i \in \{0, \dots, n-1\}$. Falta ver que G estabiliza a (W_1, \dots, W_n) . Sea $g \in G$. Trivialmente tenemos que $gW_0 \subseteq W_0$ pues $gv = v$. Si $j \geq 1$, entonces existen $\lambda_1, \dots, \lambda_j \in \mathbb{C}$ tales que

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

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

Representaciones de grupos

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

Si G es un grupo finito, un morfismo de grupos $\rho: G \rightarrow \mathbf{GL}(V)$, $g \mapsto \rho_g$, donde V es un espacio vectorial complejo de dimensión finita, se dice 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 n , al fijar una base para V podemos considerar $\rho: G \rightarrow \mathbf{GL}(V) \simeq \mathbf{GL}_n(\mathbb{C})$. Observemos que toda representación de un grupo finito será de dimensión finita.

Ejemplo 4.1. 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 4.2. 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 4.3. 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 4.4. 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 4.5. Sea X un G -conjunto y sea $V = \mathbb{C}X$ el espacio vectorial con base $\{x : x \in X\}$. Entonces

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

es una representación de grado $|X|$.

Ejemplo 4.6. El signo $\text{sign} : \mathbb{S}_n \rightarrow \mathbf{GL}_1(\mathbb{C}) = \mathbb{C}$ es una representación de \mathbb{S}_n .

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

Ejemplo 4.7. 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

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

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 4.8. 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

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 4.9. 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 contexto de la teoría de representaciones. Sea $\phi: V \rightarrow \mathbf{GL}(V)$ 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 .

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 4.10. Toda representación de grado uno es irreducible.

En el siguiente ejemplo trabajaremos sobre los números reales.

Ejemplo 4.11. 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 $\mathbb{R}^{3 \times 1}$ por multiplicación de matrices. El conjunto

$$N = \{(x, y, z)^T \in \mathbb{R}^{3 \times 1} : x + y + z = 0\}$$

es un subespacio G -invariante de \mathbb{R}^3 . Veamos que N es irreducible. Si N contiene un subespacio G -invariante, 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 4.12. ¿Qué pasa en el ejemplo anterior sobre los números complejos?

pro:deg2

Proposición 4.13. Sea $\phi: G \rightarrow \mathbf{GL}(V)$ una representación de grado dos. Entonces ϕ es irreducible si y sólo si no existe autovector común para todos los ϕ_g , $g \in G$.

Demostración. Supongamos que ϕ no es irreducible. Existe $W \subseteq V$ subespacio 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 4.14. 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 4.13 nos dice que esta representación es irreducible pues las matrices $\phi_{(12)}$ y $\phi_{(23)}$ no tienen autovectores en común.

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.

proposition:Lin(G)

Proposición 4.15. 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, $\rho \circ \pi = \phi$. \square

Diremos que un caracter χ es **lineal** si $\chi(1) = 1$. Los caracteres lineales son representaciones de grado uno.

Ejemplo 4.16. 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 caracteres lineales. Uno de esos caracteres es el trivial, el otro es el signo.

Veamos algunos ejemplos generales de representaciones:

Ejemplo 4.17. El morfismo trivial $\rho: G \rightarrow \mathbb{C}, g \mapsto 1$, 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 4.18. 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 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 4.19. 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, $\bar{\beta}(u \otimes v) = \beta(u, v)$. \square

xca:tensorial_unicidad

Ejercicio 4.20. 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 4.21. 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 4.22. 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 4.23. 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 4.24. Demuestre que $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$.

xca:UxK

Ejercicio 4.25. Demuestre que $U \otimes K \simeq K \simeq K \otimes U$.

lem:U_LI

Lema 4.26. 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 $i \in \{1, \dots, n\}$ y sea $f_i: U \rightarrow K$, $f_i(u_j) = \delta_{ij}$. Como la función $U \times V \rightarrow V$, $(u, v) \mapsto f_i(u)v$, es bilineal, existe una función $\alpha_i: U \otimes V \rightarrow V$ 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 4.27. Demuestre que si $u \otimes v = 0$ y $v \neq 0$, entonces $u = 0$.

Teorema 4.28. 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 $0 = \sum_k u_{i_k} \left(\sum_l \lambda_{kl} v_{j_l} \right)$ y luego, como los u_{i_k} son linealmente independientes, el lema 4.26 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 4.29. 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

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

Ahora sí, el ejemplo que estábamos esperando.

Ejercicio 4.30. 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 4.31. *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*

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

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

Demostración. Calculamos

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

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

Ejercicio 4.32. Sea G un grupo finito. Si V y W son $\mathbb{C}[G]$ -módulos de dimensión finita, entonces $U^* \otimes V \simeq \text{Hom}_{\mathbb{C}}(U, V)$ como $\mathbb{C}[G]$ -módulos.

Capítulo 5

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 5.1. 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 5.2. Sea $G = C_n$ el grupo cíclico de orden n (escrito multiplicativamente). Demuestre que $K[G] \simeq K[X]/(X^n - 1)$.

Proposición 5.3. 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 5.4. *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 $\phi: K[G] \rightarrow A$ de álgebras tal que la restricción $\phi|_G$ de ϕ al grupo G es igual a f , es decir $\phi|_G = f$.*

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

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

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 5.5. 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 5.6 (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 $\mathbb{C}[K]$ -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 $\mathbb{C}[K]$ -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

La misma demostración del teorema de Maschke vale para el álgebra de grupo real o racional. La descomposición de un módulo sobre el álgebra de grupo dependerá fuertemente del cuerpo sobre el que se trabaje.

Ejemplo 5.7. 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 5.8. 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 5.9. 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. Si $l \in K$, 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 .

Nos falta demostrar que V es el producto directo de U y N . 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 5.10. *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 5.11. *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

Corolario 5.12. Si G es un grupo finito de orden n con k clases de conjugación y $m = (G : [G, G])$, entonces $n + 3m \geq 4k$.

Demostración. Sabemos que G tiene k clases de isomorfismos de módulos simples y que exactamente m son de dimensión uno. Luego $n = \sum_{i=1}^k n_i^2 \geq m + 4(m - k)$. \square

Ejemplo 5.13. 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 5.14. Vimos en el ejemplo 4.14 que \mathbb{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 \mathbb{S}_3 tiene tres clases de conjugación, de donde se sigue inmediatamente que $n_1 = n_2 = 1$ y $n_3 = 2$. En conclusión,

$$\mathbb{C}[\mathbb{S}_3] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$$

como álgebras.

pro:nunca_SS

Proposición 5.15. Sea K un cuerpo. Si G es un grupo infinito, entonces $K[G]$ no es semisimple.

Demostración. Sea $A = K[G]$ y supongamos que A es semisimple. Si I es el ideal de aumentación de A , existe un ideal no nulo J de A tal que $A = I \oplus J$. Existen entonces $e \in I$, $f \in J$ tales que $1 = e + f$. Si $x \in I$, entonces $x = xe + xf$ y luego $xf = x - xe \in I \cap J = \{0\}$. Como entonces $x = xe$ para todo $x \in I$, en particular $e = e^2$. Análogamente vemos que $f^2 = f$. Además $ef = 0$ pues $ef \in I \cap J = \{0\}$. Como I es el ideal de aumentación y $If = (Ae)f = A(ef) = 0$, se concluye que $(g - 1)f = 0$ para todo $g \in G$ pues $g - 1 \in I$. Si suponemos que $f = \sum_{h \in G} \lambda_h h$, entonces

$$f = gf = \sum_{h \in G} \lambda_h (gh) = \sum_{h \in G} \lambda_{g^{-1}h} h.$$

Luego $\lambda_h = \lambda_{g^{-1}h}$ para todo $g, h \in G$, una contradicción pues como $f \neq 0$ la suma que define a f es infinita. \square

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 $e_j = f^{-1}(I_j)$, donde I_j la matriz identidad de $M_{n_j}(\mathbb{C})$. Supongamos que $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. 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 $U \oplus V$. 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 del lema 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

Lema 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. 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 ψ 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 ψ_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

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

□

Como consecuencia del lema anterior tenemos que el producto de dos caracteres es un caracter. 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 $\text{Hom}_{\mathbb{C}[G]}(U,V)$ 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** 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

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

para todo $v \in V$. 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, $\dim V = \text{traza}(\alpha) = \frac{1}{|G|} \sum_{g \in G} \text{traza}(\rho_g) = \frac{1}{|G|} \sum_{g \in G} \chi(g)$. \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

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

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_s 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** de G como la matriz $X \in \mathbb{C}^{s \times s}$ 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.

Teorema 6.13 (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

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 6.14. 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

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

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 6.15. 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 6.16. 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,

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

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 6.17. 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 6.18 (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

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

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

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

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 $(m : n) = 1$ 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

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

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 $\chi(g) = \text{traza } \rho_g = \lambda_1 + \dots + \lambda_k \in \mathbb{A}$. \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

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

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 $xz_{k-1} = x^k = -a_0 - \dots - a_{k-1}x^{k-1}$.

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

theorem:algebraic

Teorema 7.7. 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 7.8 (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 7.7. 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 7.9. Sea p un primo. Demuestre que todo grupo de orden p^2 es abeliano.

xca:pq

Ejercicio 7.10. 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 7.11. 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 7.12. 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 7.13. 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 7.14 (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. Como

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

el subgrupo

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

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 7.15 (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 [21, §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 7.16 (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 [11].

Se sabe que la conjetura es verdadera para varias clases de grupos. Isaacs la demostró para grupos resolubles, ver por ejemplo [11, 13]. Malle y Späth demostraron que la conjetura de McKay es cierta para el primo $p = 2$.

Teorema 7.17 (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 [19] 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 [14].

Podemos verificar computacionalmente algunos casos 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:

Conjetura 7.18 (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

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

Se sabe que la conjetura de Isaacs–Navarro es verdadera para varias clases de grupos, por ejemplo para grupos resolubles, para los grupos simples esporádicos y para el grupo simétrico, ver por ejemplo [15] y las referencias allí contenidas.

Para verificar la conjetura de Isaacs–Navarro en algunos ejemplos de orden pequeño utilizaremos 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

Ejemplo 8.2. La proposición anterior nos permite calcular por ejemplo 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

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

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

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

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 caracter 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

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

Similarmente, 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

Ejemplo 8.5. Calculemos ahora la tabla de caracteres de \mathbb{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 ,

$$0 = \chi_L((12)(34)) = 1 + 1 + 1 + 3\chi_4((12)(34)),$$

$$0 = \chi_L((123)) = 1 + \omega + \omega^2 + 3\chi_4((123)),$$

$$0 = \chi_L((132)) = 1 + \omega + \omega^2 + 3\chi_4((132)),$$

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

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 4.15, 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

$$0 = \chi_L(x) = 1 + 1 + 1 + 1 + 2\chi_5(x),$$

$$0 = \chi_L(a) = 1 + 1 + -1 - 1 + 2\chi_5(a),$$

$$0 = \chi_L(b) = 1 - 1 + 1 - 1 + 2\chi_5(b),$$

$$0 = \chi_L(c) = 1 - 1 - 1 + 1 + 2\chi_5(c),$$

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

Capítulo 9

Conmutadores

Sea G un grupo finito y sean C_1, \dots, C_s sus clases de conjugación. Vimos en el teorema 7.7 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 la clase de conjugación de g en 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 [17]. 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 [18].

Para otras aplicaciones de la teoría de caracteres a los grupos simples finitos referiremos a [16].

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 [20].

Teorema 10.1 (Cauchy–Frobenius–Burnside). *Supongamos que el grupo 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

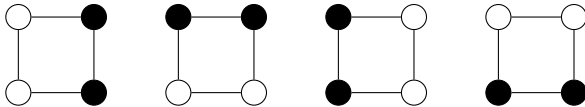
$$v = \sum_{x \in X} \lambda_x x = \sum_{i=1}^m \lambda_{x_i} \sum_{y \in G \cdot x_i} y = \sum_{i=1}^m (\lambda_{x_i} |G \cdot x_i|) v_i. \quad \square$$

En [22] 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

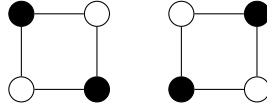

(10.1)

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 $|X| = 16$.

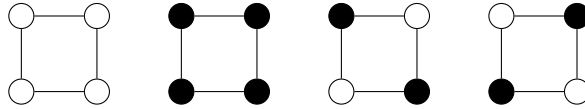
Hacemos actuar a G en X por rotaciones de 90° en sentido antihorario. Los coloreos que vimos en (10.1) están todos en una misma órbita. Otra de las órbitas del conjunto X está formada por



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,

$$k = \frac{1}{2}(|Z(G)| + |G|) \leq \frac{1}{2} \left(\frac{1}{4} + 1 \right) |G|,$$

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 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 [9].

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 [24, 25, 26, 27], 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 [5]. El siguiente resultado de [10] 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 χ , 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 [22] 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 [3].

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 $g \in G$ de orden una potencia de p sin puntos fijos.*

No veremos la demostración en este curso.

Supongamos que G es un grupo finito que actúa fielmente 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 $G \leq \mathbb{S}_n$, 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 [7].

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

Teorema 11.1 (Brauer–Fowler). *Sea G un grupo finito y simple y sea x una involución. Si $|C_G(x)| = n$, entonces $|G| \leq (n^2)!$.*

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

$$\begin{aligned} U \text{ es un } \mathbb{C}[G]\text{-submódulo} &\iff g \cdot U \subseteq U \text{ para todo } g \in G \\ &\iff \rho(g)(U) \subseteq U \text{ para todo } g \in U \\ &\iff \tilde{\rho}(gN)(U) \subseteq U \text{ para todo } g \in U. \end{aligned}$$

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,

$$\mathbf{PSL}(2, 7) = \mathbf{SL}(2, 7) / Z(\mathbf{SL}(2, 7))$$

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 $\theta \in \text{Hom}_{K[G]}(\text{Ind}_H^G V, U)$, 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 [12], 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 $\overline{\chi_i} = \chi_{\alpha(i)}$ 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,

$$\rho_\alpha X = \overline{X} = X \rho_\beta.$$

Como X es una matriz inversible, $\rho_\alpha = X \rho_\beta X^{-1}$. Luego

$$n = \chi_\rho(\alpha) = \text{traza } \rho_\alpha = \text{traza } \rho_\beta = \chi_\rho(\beta) = m.$$

□

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. □

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

$$1, \chi_1, \overline{\chi_1}, \dots, \chi_k, \overline{\chi_k}, \quad r = 1 + 2k.$$

Para cada $j \in \{1, \dots, k\}$ sea $d_j = \chi_j(1)$. Como cada d_j divide a $|G|$ por el teorema 7.8 de Frobenius y $|G|$ es impar, los d_j son números impares, digamos $d_j = 1 + 2m_j$. Entonces

$$\begin{aligned}
|G| &= 1 + \sum_{j=1}^k 2d_j^2 = 1 + \sum_{j=1}^k 2(2m_j + 1)^2 \\
&= 1 + \sum_{j=1}^k 2(4m_j^2 + 4m_j + 1) = 1 + 2k + 8 \sum_{j=1}^k m_j(m_j + 1).
\end{aligned}$$

Luego $|G| \equiv r \pmod{16}$ pues $r = 1 + 2k$ y cada $m_j(m_j + 1)$ es un número par. \square

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 14.8. Todo grupo abeliano es resoluble.

Ejemplo 14.9. El grupo $\mathbf{SL}_2(3)$ es resoluble. La serie derivada de $\mathbf{SL}_2(3)$ es

$$\mathbf{SL}_2(3) \supseteq Q_8 \supseteq C_4 \supseteq C_2 \supseteq 1.$$

Veamos el código:

```
gap> IsSolvable(SL(2,3));
true
gap> List(DerivedSeries(SL(2,3)), StructureDescription);
[ "SL(2,3)", "Q8", "C2", "1" ]
```

Ejemplo 14.10. Un grupo simple no abeliano no es resoluble.

theorem:resoluble

Teorema 14.11. 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 14.12. Sea $n \geq 5$. El grupo \mathbb{S}_n no es resoluble pues \mathbb{A}_n no es resoluble.

Ejemplo 14.13. Si H y K son grupos resolubles entonces $H \times K$ es resoluble.

Proposición 14.14. 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 14.11. \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 14.15. 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 14.16 (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 14.17 (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,

$$\begin{aligned} 0 &= \sum_{\chi \in \text{Irr}(G)} \chi(1)\chi(g) \\ &= \sum_{p|\chi(1)} \chi(1)\chi(g) + \sum_{p \nmid \chi(1)} \chi(1)\chi(g) + 1, \end{aligned} \tag{14.2} \quad \boxed{\text{eq:Burnside}}$$

donde el uno corresponde a la representación trivial de G . Al mirar (14.2) módulo p vemos que 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 14.18 (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 14.19 (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 14.20 (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* [4]. En [6] 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–Thompson 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 [23] 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 14.21 (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 [8].

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 15

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

$$\begin{aligned} z_1 &= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, & z_2 &= x_2y_1 + x_1y_2 - x_4y_3 + x_3y_4, \\ z_3 &= x_3y_1 + x_4y_2 + x_1y_3 - x_2y_4, & z_4 &= x_4y_1 - x_3y_2 + x_2y_3 - x_1y_4. \end{aligned} \quad (15.1) \quad \boxed{\text{eq:Hamilton}}$$

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 15.1. *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

$$|G| = 2^n = 4 + \frac{1}{2}(2^n - 4),$$

se concluye que G tiene $2^{n-1} + 2$ clases de conjugación. \square

Ejemplo 15.2. Las fórmulas (15.1) dan una representación del grupo G del lema anterior. Escribamos a cada z_i como $z_i = \sum_{k=1}^4 a_{1k}(x_1, \dots, x_4)y_k$. 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 15.3 (Hurwitz). *Si existe una identidad*

$$(x_1^2 + \dots + x_n^2)(y_1^2 + \dots + y_n^2) = z_1^2 + \dots + z_n^2, \quad (15.2)$$

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 perder 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 (15.2) y comparamos coeficientes obtenemos

$$\sum_{i=1}^n a_{ik}(x_1, \dots, x_n) a_{il}(x_1, \dots, x_n) = \delta_{k,l}(x_1^2 + \dots + x_n^2), \quad (15.3)$$

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

$$AA^T = (x_1^2 + \dots + x_n^2)I, \quad (15.4)$$

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 (15.3). Como cada $a_{ij}(x_1, \dots, x_n)$ 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 (15.4) 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

$$A_i A_j^T + A_j A_i^T = 0 \quad i \neq j, \quad A_i A_i^T = I. \quad (15.5)$$

eq:condiciones

Queremos entonces encontrar n matrices complejas de $n \times n$ que cumplan las condiciones (15.5). Para cada $i \in \{1, \dots, n\}$ sea $B_i = A_n^T A_i$. Entonces (15.5) 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 15.2, 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 15.4. *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.

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. B. Fein, W. M. Kantor, and M. Schacher. Relative Brauer groups. II. *J. Reine Angew. Math.*, 328:39–57, 1981.
4. W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.
5. P. Flavell. Finite groups in which every two elements generate a soluble subgroup. *Invent. Math.*, 121(2):279–285, 1995.
6. 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.
7. 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.
8. 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.
9. R. M. Guralnick and G. R. Robinson. On the commuting probability in finite groups. *J. Algebra*, 300(2):509–528, 2006.
10. 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.
11. I. M. Isaacs. Characters of solvable and symplectic groups. *Amer. J. Math.*, 95:594–635, 1973.
12. I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.
13. I. M. Isaacs. *Characters of solvable groups*, volume 189 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2018.
14. I. M. Isaacs, G. Malle, and G. Navarro. A reduction theorem for the McKay conjecture. *Invent. Math.*, 170(1):33–101, 2007.
15. 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.
16. 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.
17. 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.
18. 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.

19. G. Malle and B. Späth. Characters of odd degree. *Ann. of Math. (2)*, 184(3):869–908, 2016.
20. P. M. Neumann. A lemma that is not Burnside’s. *Math. Sci.*, 4(2):133–141, 1979.
21. 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.
22. J.-P. Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440, 2003.
23. N. M. Stephens. On the Feit-Thompson conjecture. *Math. Comp.*, 25:625, 1971.
24. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, 74:383–437, 1968.
25. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. II. *Pacific J. Math.*, 33:451–536, 1970.
26. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. III. *Pacific J. Math.*, 39:483–534, 1971.
27. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. IV, V, VI. *Pacific J. Math.*, 48, 1973.

Índice alfabético

- Acción
 - 2-transitiva, 70
- Bimódulo, 80
- Burnside
 - Teorema de, 94
 - teorema de, 65
- Character
 - real, 93
- Character lineal, 28
- Caracteres
 - matriz de, 43
 - tabla de, 43
- Carácter
 - de una representación, 39
- Clase de conjugación
 - real, 93
- Conjetura
 - de Feit–Thompson, 97
 - de Isaacs–Navarro, 53
 - de McKay, 52
 - de Ore, 64
- Desarreglos, 71
- Dual
 - de una representación, 32
- Elemento
 - algebraico, 4
 - nil, 17
- Entero algebraico, 47
- Frobenius
 - complemento de, 88
 - grupo de, 88
 - núcleo de, 88, 90
- Teorema de, 88, 91
- teorema de, 49
- Función
 - de clases, 41
- Grado
 - de una representación, 25
- Ideal
 - de aumentación, 33
 - nilpotente, 14
- Identidad
 - de Euler, 99
 - de Fibonacci, 99
 - de Hamilton, 99
- Lema
 - de Nakayama, 14
 - de Schur, 4
- Maschke
 - teorema de, 34
- Morfismo
 - de álgebras, 3
- Módulo
 - inducido, 82
 - semisimple, 4
 - simple, 4
- Núcleo
 - de un caracter, 75
- Orbital, 69
- Parte irreducible
 - de un caracter, 79
- Producto tensorial

- de bimódulos, 81
- de espacios vectoriales, 29
- de representaciones, 31
- de transformaciones lineales, 30
- propiedad universal, 29
- Proyección, 34
- Radical
 - de Jacobson, 13
- Rango, 69
- Representaciones
 - equivalentes, 26
- Representación
 - completamente reducible, 28
 - de un grupo, 25
 - dual, 32
 - fiel, 26
 - regular de un álgebra, 4
 - trivial, 29
- Restricción, 78
- Schur
 - teorema de, 51
- Serie
 - derivada, 95
- Subespacio invariante, 27
- Subrepresentación, 27
- Tabla de caracteres, 55
- Teorema
 - 5/8, 67
 - de Artin–Wedderburn, 9
 - de Burnside, 61, 65, 96, 97
 - de Cameron–Cohen, 71
 - de Dixon, 68
 - de Erdős–Turan, 67
 - de Fein–Kantor–Schacher, 71
 - de Feit–Thompson, 97
 - de Frobenius, 88, 91
 - de Guralnick–Robinson, 69
 - de Guralnick–Wan, 72
 - de Guralnick–Wilson, 69
 - de Hurwitz, 101
 - de Itô, 52
 - de Jordan, 70
 - de Kegel–Wielandt, 97
 - de Kolchin, 20
 - de Liebeck–O’Brien–Shalev–Tiep, 64
 - de los conmutadores de Frobenius, 63
 - de Malle–Späth, 52
 - de Malle–Späth, 52
 - de Maschke, 34
 - de reciprocidad de Frobenius, 83
 - de Schur, 51
 - de Wedderburn, 11, 18
 - de Wildon, 71
 - primera ortogonalidad Schur, 43
 - segunda ortogonalidad Schur, 44
- Teorema de
 - Burnside, 94
 - Frobenius, 49
 - Solomon, 45
- Transversal, 82
- Álgebra, 3
 - algebraica, 4
 - asociativa, 3
 - conmutativa, 3
 - de grupo, 33
 - de matrices, 3
 - de polinomios, 3
 - de polinomios truncados, 4
 - dimensión, 3
 - ideal de un, 3
 - nil, 17
 - semisimple, 6
 - simple, 10