UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

Departamento de Álgebra, Geometría y Topología

TRABAJO DE FIN DE GRADO

El Teorema de Burnside

Guillermo García Sáez

Dirigido por Juan Ramón Delgado Pérez, José F. Fernando Galván y José Manuel Gamboa Mutuberria

Curso académico 2022-23

Madrid, a 20 de Junio de 2023

Resumen. El objetivo de este trabajo es dar una demostración del Teorema $p^a q^b$ de Burnside utilizando la Teoría de caracteres. Para ello es necesario desarrollar la Teoría de representación de grupos finitos, por lo que necesitaremos introducir los conceptos de módulo y el de álgebra o anillo de un grupo finito. Demostraremos resultados claves en la Teoría de representación como el Teorema de Maschke, el Lema de Schur y los teoremas de descomposición en representaciones irreducibles. Así mismo, realizaremos un sucinto repaso de resultados básicos de Teoría algebraica de números y estudiaremos su estrecha relación con los caracteres de las representaciones, clave en la demostración del Teorema de Burnside.

Abstract. The main goal of this work is to give a self-contained proof of the Burnside's $p^a q^b$ Theorem with Character Theory. To achive it we need to develop the Representation Theory of Finite Groups, which requires to rigorous define concepts as modules and ring groups. We will prove important results as Maschke's Theorem, Schur's Lemma and the decomposition theorems into irreducible representations. Additionally, we will make a succint review about Algebraic Number Theory and its relantionship with Character Theory, the key of the proof of Burnside's Theorem.

Contenido

Introducción

Así como los números primos son los ladrillos con los que se construyen los números naturales, de manera similar podemos considerar a los grupos simples como los ladrillos de los grupos finitos. Concretamente, todo grupo finito G admite una *serie de composición* o *torre* de subgrupos normales

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G,$$

tal que G_{i+1}/G_i es simple para $0 \leq i \leq m-1$, y el Teorema de Jordan-Hölder nos dice que todas las series de composición son equivalentes, es decir, tienen la misma longitud y factores isomorfos. A partir de este importante resultado demostrado a finales del siglo XIX surgieron dos importantes problemas en Teoría de grupos.

1. Clasificar todos los grupos simples.

2. Métodos de construcción de grupos a partir de los grupos simples.

Entre finales del siglo XIX y principios del XX, los esfuerzos de matemáticos como Otto Hölder, Frank Nelson Cole y William Burnside, lograron clasificar todos los grupos simples de orden menor o igual que 1092. Un resultado de Hölder que dice que un grupo cuyo orden es el producto de dos o tres primos distintos es resoluble, llevó a Burnside a preguntarse si existen grupos no abelianos simples de orden impar y si hay grupos no abelianos simples cuyo orden sea divisible por menos de tres primos distintos. En 1904, Burnside respondió ambas cuestiones cuando probó su célebre Teorema, que dice que todo grupo cuyo orden sea divisible por exactamente dos primos distintos es resoluble. La demostración de Burnside involucra la Teoría de la representación y la, hasta entonces desconocida, Teoría de caracteres, que Burnside desarrolla enormemente durante sus intentos por demostrar el resultado.
No sería hasta la década de 1970 que los matemáticos Goldschmidt, Bender y Matsuyama lograran una demostración del Teorema mediante técnicas puramente de Teoría de grupos.

CAPÍTULO I

Preliminares

I.1. Grupos finitos

En esta primera sección introducimos algunos de los conceptos básicos de la Teoría de Grupos, así como los conceptos de clases de conjugación y resolubilidad de grupos, muy importantes en la demostración del Teorema de Burnside.

Definiciones I.1.1. Un *grupo* es el par formado por un conjunto G y una operación $G \times G \to G; (a, b) \mapsto ab$, que cumple las siguientes condiciones:

1. $(ab)c = a(bc)$, para cualesquiera $a, b, c \in G$. (Propiedad *asociativa*).
2. Existe un elemento $e_G \in G$, denominado *elemento neutro* de G, tal que $ae_G = e_G a = a$ para todo $a \in G$. Si no existe ambigüedad acerca del grupo, este elemento se suele denotar por 0 si la operación es aditiva o por 1 si es multiplicativa. Es inmediato ver que dicho elemento es único.
3. Para cada $a \in G$ existe un elemento $a^{-1} \in G$ tal que $aa^{-1} = a^{-1}a = e_G$. Se dice que a^{-1} es el *inverso* de a. Es inmediato probar que el inverso de un elemento es único, y que si a^{-1} es el inverso de $a \in G$, entonces $(a^{-1})^{-1} = a$.

Se dice que dos elementos $g, h \in G$ *conmutan* si $gh = hg$. Si cada par de elementos de G conmutan se dice que G es un grupo *abeliano*. Si G es un conjunto finito se llama *orden* de G al número de elementos de G, al que se denota por $\mathrm{ord}(G)$. Si el orden de G es potencia de un número primo p se dice que G es un p-grupo.

Definición I.1.2. Un subconjunto H de un grupo G se dice *subgrupo* de G si, con la misma operación de G, es un grupo. Es inmediato ver que esto equivale a que $1_G \in H$ y $ab^{-1} \in H$ para cualesquiera $a, b \in H$. Para cada grupo G, él mismo y el conjunto $\{1_G\}$ son dos subgrupos de G, denominados triviales. Un subgrupo H de un grupo G se dice *normal* si dado $g \in G$ se tiene que $g^{-1}hg \in H$ para todo $h \in H$. Abusando de notación esto suele denotarse como $g^{-1}Hg = H$. Si H es un subgrupo normal de G se denotará como $H \trianglelefteq G$. Si los únicos subgrupos normales de G son $\{e_G\}$ y G, se dice que G es *simple.*

Definición I.1.3. Un grupo G se dice *cíclico* si existe un elemento $g \in G$ de modo que $G = \{g^k : k \in \mathbb{Z}\}$.

Definición I.1.4. Dado un subgrupo H de un grupo G se llama *centralizador* de H en G al subgrupo

$$C_G(H) := \{g \in G : gh = hg, \forall h \in H\}.$$

Si $g \in G$ se denomina centralizador de g, $C_G(g)$, al conjunto de elementos del grupo que conmutan con g. El centralizador de G, $Z(G) := C_G(G)$, se denomina *centro* de G.

Definición I.1.5**.** Sean G un grupo y H un subgrupo suyo. Se define en G la relación de equivalencia $\mathfrak{R}_H$ mediante: dados $a, b \in G$, decimos que a y b son *congruentes por la derecha* respecto de H, y escribimos $a\mathfrak{R}_H b$ si y solo si $ab^{-1} \in H$. De forma análoga se define la relación $\mathfrak{R}^H$ *ser congruente por la izquiera* respecto de H si dados $a, b \in G$ se tiene que $a^{-1}b \in H$. La aplicación $G/\mathfrak{R}_H \to G/\mathfrak{R}^H, Ha \mapsto a^{-1}H$, está bien definida y es inyectiva porque $Ha = Hb$ si y solo si $ab^{-1} = h \in H$, lo que equivale a que $b^{-1} = a^{-1}h$, o lo que es igual, $b^{-1}H = a^{-1}hH = a^{-1}H$. Además es evidente que es sobreyectiva, luego es una biyección. Por ello ambos conjuntos tienen el mismo cardinal, que se denomina *índice* de H en G y que se denota por $[G : H]$.

Definición I.1.6**.** Sea H un subgrupo normal de un grupo G. En tal caso las relaciones de equivalencia anteriores coinciden, denotaremos como G/H al conjunto cociente (común). Mediante la siguiente operación se puede probar que tiene estructura de grupo

$$G/H \times G/H \to G/H, (Ha, Hb) \mapsto Ha \cdot Hb = Hab.$$

La normalidad de H es imprescindible para ver que está bien definida. El orden del grupo cociente es el cardinal del conjunto cociente, que hemos definido como el índice, por lo tanto $\mathrm{ord}(G/H) = [G : H]$.

I.1.a. Clases de conjugación.

Definiciones I.1.7**.**

1. Se llama *acción de un grupo G sobre un conjunto no vacío X* a cualquier homomorfismo de grupos $G \to \mathrm{Biy}(X)$, $g \mapsto \hat{g}$. Conviene observar que este homomorfismo induce una aplicación $G \times X \to X, (g, x) \mapsto \hat{g}(x)$. Nótese que $\mathrm{id} = \hat{e}_G$ y $\hat{g}^{-1} = \hat{g^{-1}}$, por tratarse de un homomorfismo.

2. Se define en X la relación de equivalencia $x \sim y$ si existe $g \in G$ tal que $y = \hat{g}(x)$. En efecto es de equivalencia pues $x \sim x$ al ser $x = \widehat{e_G}(x)$, si $y = \hat{g}(x)$ entonces $x = \hat{g}^{-1}(y)$, y si dados $x, y, z \in X$ se tiene que $y = \hat{g}(x)$ y $z = \hat{h}(y)$, entonces $z = \hat{h} \circ \hat{g}(x)$.

La clase de equivalencia de $x \in X$ se llama *G-órbita* de x bajo la acción de G, que es el conjunto $O_{G,x} = \{\hat{g}(x) : g \in G\}$. Si no hay confusión respecto al grupo denotaremos $O_x := O_{G,x}$, y diremos que es la órbita de x. La familia $\{O_x : x \in X\}$ es una partición de X, y si $R \subset X$ es un conjunto de representantes de estas clases de equivalencia, se cumple $X = \bigsqcup_{x \in R} O_x$. En consecuencia $|X| = \sum_{x \in R} |O_x|$.

Definición I.1.8**.** Sean X un conjunto no vacío y G un grupo. Se denomina *estabilizador* del punto $x \in X$ bajo la acción de G al subgrupo

$$\mathrm{Stab}_G(x) := \{g \in G : \hat{g}(x) = x\}.$$

Es inmediato comprobar que es un subgrupo.

Proposición I.1.9 (Cardinal de una órbita)**.** *Si un grupo G actúa sobre un conjunto no vacío X y $x \in X$, entonces se cumple la igualdad $|O_x| = [G : \mathrm{Stab}_G(x)]$.*

Demostración. Denotemos $H := \mathrm{Stab}_G(x)$, y consideramos en G la relación de congruencia por la derecha $\mathfrak{R}_H$ y el correspondiente conjunto cociente $G/\mathfrak{R}_H$, cuyo cardinal es $[G : \mathrm{Stab}_G(x)|$. Todo se reduce a probar entonces que la aplicación $G/\mathfrak{R}_H \to O_x, Hg \mapsto \hat{g}(x)$, es biyectiva. Que está bien definida y es inyectiva se sigue de que $Hg_1 = Hg_2 \iff g_1 g_2^{-1} \in H$, lo que se traduce en que $(\hat{g_1}\hat{g_2}^{-1})(x) = x$; es decir, $\hat{g_2}^{-1}(\hat{g_1}(x)) = x$, o sea $\hat{g_1}(x) = \hat{g_2}(x)$. La sobreyectividad es inmediata. □

Corolario I.1.10 (Fórmula de las órbitas.)**.** *Sea R un conjunto de representantes de las órbitas de un conjunto finito X bajo la accción de un grupo G. Entonces*

$$|X| = \sum_{x \in R} [G : \mathrm{Stab}_G(x)].$$

El siguiente ejemplo será importante en la Teoría de Caracteres que más adelante desarrollaremos.

Ejemplo I.1.11**.** Sean G un grupo, $X := G$ como conjunto, y consideremos la acción $g \mapsto \hat{g}$ donde $\hat{g} : G \to G, x \to g^{-1}xg$. Esta acción se denomina *conjugación*, y la órbita $O_x = \{g^{-1}xg : g \in G\}$ se denomina *clase de conjugación* de x. Si suponemos que G es un grupo finito entonces la Fórmula de las órbitas nos dice que $\mathrm{ord}(G) = \sum_{x \in R}[G : \mathrm{Stab}_G(x)]$. Además $g \in \mathrm{Stab}_G(x)$ si y solo si $g^{-1}xg = x$, o sea, $gx = xg$, o lo que es lo mismo, $\mathrm{Stab}_G(x) = C_G(x)$. Por ello $[G : \mathrm{Stab}_G(x)] = 1$ si y solo si $G = C_G(x)$; es decir, $x \in Z(G)$. En consecuencia

$$\mathrm{ord}(G) = \mathrm{ord}(Z(G)) + \sum_{x \in R \setminus Z(G)} [G : \mathrm{Stab}_G(x)].$$

Esta fórmula se conoce como *ecuación de clases de conjugación* del grupo G.

Ejemplo I.1.12**.** Vamos a calcular las clases de conjugación del grupo de permutaciones de tres elementos $\mathfrak{S}_3 := \{\mathrm{id}, (12), (13), (23), (123), (132)\}$. Observemos primero que el centro de $\mathfrak{S}_3$ es trivial. Nótese que $(12)(13) = (132) \neq (123) = (13)(12)$ y que $(12)(23) = (123) \neq (132) = (23)(12)$, luego no hay trasposiciones en el centro. Por otro lado $(123)(12) = (13) \neq (23) = (12)(123)$, y $(132)(12) = (23) \neq (13) = (12)(132)$. Luego la única clase de conjugación trivial será $O_{\mathrm{id}} = \{\mathrm{id}\}$. Para el elemento (12) unos cálculos rutinarios nos dan que $O_{(12)} = \{(12), (13), (23)\}$. Como los elementos que quedan no tienen conjugaciones triviales por no estar en el centro necesariamente $O_{(123)} = \{(123), (132)\}$. Estas son las tres clases de conjugación de $\mathfrak{S}_3$.

Proposición I.1.13**.** *Sean G un grupo de orden p^n, donde p es un número primo y $n \geq 1$. Entonces si $\{1\} \neq H \trianglelefteq G$, entonces $H \cap Z(G) \neq \{1\}$. En particular $Z(G) \neq \{1\}$.*

Demostración. Consideremos la acción de G sobre $X := H \setminus \{e_G\}$ definida por

$$G \to \mathrm{Biy}(X), g \mapsto \hat{g},$$

donde $\hat{g} : X \to X$, $h \mapsto g^{-1}hg$, que está bien definida por ser H un subgrupo normal. Se trata de probar que existe $h \in X$ tal que $\mathrm{Stab}_G(h) = G$. En efecto, esto significa que

$g^{-1}hg = \hat{g}(h) = h$, o sea , $hg = gh$, para todo $g \in G$, es decir, $h \in H \cap Z(G) \setminus \{e_G\}$.

Supongamos, por reducción al absurdo, que ningún estabilizador coincide con G. Entonces, como G es un p-grupo, $[G : \mathrm{Stab}_G(h)] \in p\mathbb{Z}$ para cada $h \in R$, donde $R \subset X$ denota un conjunto de representantes de las órbitas de X bajo la acción de G. De la ecuación de clases de conjugación se desprende

$$|X| = \sum_{h \in R} [G : \mathrm{Stab}_G(h)] \in p\mathbb{Z},$$

y esto es absurdo, ya que al ser H un p-grupo, $1 + |X| = \mathrm{ord}(H) \in p\mathbb{Z}$. □

I.2. Introducción a los módulos

El objetivo de esta sección es el de introducir el concepto de módulo, una de las estructuras fundamentales del álgebra abstracta e íntimamente relacionado con la *teoría de representaciones de grupos*.

I.2.a. Módulos

Definición I.2.1. Sea $(R, +, \cdot)$ un anillo. Un *R-módulo* por la izquierda es un grupo abeliano $(H, +)$ equipado con una acción (una aplicación $R \times H \to H$) que cumple lo siguiente:

1. $(r + s)h = rh + sh, \forall r, s \in R\,, h \in H$,
2. $(rs)h = r(sh), \forall r, s \in R\,, h \in H$,
3. $r(h + h') = rh + rh', \forall r \in R\,, h, h' \in H$,
4. Si R tiene elemento unidad 1_R, entonces $1_R h = h$, $\forall h \in H$.

Un R-módulo por la derecha se define de manera análoga, pero en este caso las operaciones de los elementos del anillo actuarían por la derecha. Si R es un anillo conmutativo, entonces todo R-módulo por la izquierda será también un R-módulo por la derecha y viceversa. En este caso los denominaremos simplemente R-módulos. A partir de ahora y excepto que se diga lo contrario trabajaremos exclusivamente con R-módulos, y supondremos que R es unitario, es decir, que posee elemento unidad 1_R.

Definición I.2.2. Sean R un anillo conmutativo y M un R-módulo. Un *R-submódulo* de M es un subgrupo N de M que es cerrado respecto la acción del anillo R, es decir, $rn \in N, \forall r \in R, \forall n \in N$.

Observación I.2.3. Todo módulo tiene al total y al neutro de la suma como submódulos triviales. Un módulo que cuyos únicos submódulos son los triviales se denomina *irreducible* o *simple*.

Proposición I.2.4 (Criterio del Submódulo)**.** *Sean R un anillo conmutativo y M un R-módulo. Un subconjunto N de M es un submódulo si y solo si:*

1. $N \neq \varnothing$.
2. $x + ry \in N, \forall r \in R\,, \forall x, y \in N$.

Demostración. Si N es un submódulo, entonces $0 \in N$, luego $N \neq \varnothing$. Por otro lado N es cerrado respecto la suma y la acción del anillo R, luego tomando $x, y \in N$ y $r \in R$, $x + ry \in N$.
Recíprocamente tomando $r = -1$ vemos que $x - y \in N$, $\forall x, y \in N$, por lo que es un subgrupo. Ahora tomando $x = 0$, tenemos que $ry \in N, \forall r \in R\,, \forall y \in N$, luego la acción de R sobre N está bien definida y por lo tanto N es un submódulo. □

Definición I.2.5**.** Un R-módulo M se dice *libre* sobre un subconjunto $B \subset M$ si para todo elemento no nulo $x \in M$ existen un natural n, unos únicos elementos no nulos $r_1, \ldots, r_n \in R$ y unos únicos $a_1, \ldots, a_n \in B$, tales que $x = r_1 a_1 + \cdots + r_n a_n$.
El conjunto B se denomina *base* de M y su cardinal se denomina *rango* del módulo. Nótese que para cualquier conjunto no vacío A, existe un R-módulo libre sobre A, que se denotará $F(A)$, y que consiste en el conjunto de combinaciones R-lineales de elementos de A.

Observaciones I.2.6**.**

1. Cuando R es un cuerpo los axiomas de R-módulo son exactamente los mismos que los de R-espacio vectorial. Podemos pensar en los módulos como una generalización del concepto de espacio vectorial obtenido al reemplazar el cuerpo de escalares por los elementos de un anillo conmutativo unitario.

2. Los $\mathbb{Z}$-módulos son los grupos abelianos. En efecto, dado un grupo abeliano $(G, +)$, definimos la acción de $\mathbb{Z}$ sobre G que dota a G de estructura de $\mathbb{Z}$-módulo como:

$$\mathbb{Z} \times G \to G\,, (n, g) \to ng = \begin{cases} g + \overset{n)}{\cdots} + g & n > 0, \\ 0 & n = 0, \\ (-g) + \overset{-n)}{\cdots} + (-g) & n < 0. \end{cases}$$

3. Sea R un anillo. Entonces $M = R$ es un R-módulo donde la acción de un elemento del anillo sobre un elemento del módulo es la multiplicación habitual en R.

4. Sea R un anillo con elemento unidad. Entonces para todo n natural

$$R^n := \{(r_1, \ldots, r_n) \,|\, r_i \in R\}$$

es un R-módulo con la suma componente a componente usual de R, y la acción de un elemento de R sobre R^n definida por

$$a(b_1, \ldots, b_n) = (ab_1, \ldots, ab_n), \forall a \in R\,, \forall (b_1, \ldots, b_n) \in R^n$$

De hecho, R^n es un R-módulo libre de rango n con base $\{e_1, \ldots, e_n\}$, donde $e_i = (0, \ldots, 0, \overset{(i)}{1}, 0 \ldots, 0)$.

5. Un mismo grupo abeliano puede tener estructura de módulo para diferentes anillos. Más concretamente si M es un R-módulo y S es un subanillo de R tal que $1_S = 1_R$, entonces M es automáticamente un S-módulo. Por ejemplo $\mathbb{R}$ es un $\mathbb{R}$-módulo, un $\mathbb{Q}$-módulo y un $\mathbb{Z}$-módulo.

6. Si M es un R-módulo y para algún ideal $\mathfrak{a}$ de R se tiene que $am = 0$ para todo elemento a del ideal y todo elemento m de M, entonces se dice que M es *aniquilado* por $\mathfrak{a}$ o alternativamente que $\mathfrak{a}$ *aniquila* a M. En este caso M es un $R/\mathfrak{a}$-módulo con la acción del cociente $R/\mathfrak{a}$ sobre M siguiente: para cada $m \in M$ y para todo $r + \mathfrak{a} \in R/\mathfrak{a}$ definimos $(r + \mathfrak{a})m = rm$.
   Como $am = 0$ para cualquier $a \in \mathfrak{a}$ la operación está bien definida. Vamos a comprobar que dota a M de estructura de $R/\mathfrak{a}$-módulo.

   a) $((r+\mathfrak{a})+(s+\mathfrak{a}))m = ((r+s)+\mathfrak{a})m = (r+s)m = rm+sm = (r+\mathfrak{a})m+(s+\mathfrak{a})m$,
   b) $((r + \mathfrak{a})(s + \mathfrak{a}))m = ((rs) + \mathfrak{a})m = (rs)m = r(sm) = (r + \mathfrak{a})((s + \mathfrak{a})m)$,
   c) $(r + \mathfrak{a})(m + n) = r(m + n) = rm + rn = (r + \mathfrak{a})m + (r + \mathfrak{a})n$,
   d) $(1 + \mathfrak{a})m = 1 \cdot m = m$.

   para cualesquiera $r, s \in R$, $m, n \in M$.

Veamos ahora un importante resultado sobre los submódulos de un R-módulo libre cuando el anillo R es un dominio de ideales principales. Antes necesitamos introducir algunos conceptos sobre sucesiones exactas.

Definición I.2.7. Dado un anillo R, sean A, B, C tres R-módulos y $f : A \to B$, $g : B \to C$ dos R-homomorfismos. Decimos que el diagrama

$$A \xrightarrow{f} B \xrightarrow{g} C$$

es una *sucesión exacta* si el núcleo de g coincide con la imagen de f. Dado el siguiente diagrama de R-módulos y R-homomorfismos

$$\ldots \xrightarrow{f_{n-2}} E_{n-1} \xrightarrow{f_{n-1}} E_n \xrightarrow{f_n} E_{n+1} \xrightarrow{f_{n+1}} \ldots$$

decimos que es una sucesión exacta en E_n si el núcleo de f_n coincide con la imagen de f_{n-1}.

Proposición I.2.8. *Sean R un anillo, E un R-módulo y F un submódulo suyo. Si i es la inclusión natural y π es la proyección canónica, entonces el diagrama:*

$$0 \longrightarrow F \xrightarrow{i} E \xrightarrow{\pi} E/F \longrightarrow 0,$$

es una sucesión exacta.

Demostración. Que la sucesión es exacta se sigue de que $\pi^{-1}(0) = F = i(F)$. □

Proposición I.2.9. *Sea R un dominio de ideales principales. Todo submódulo no nulo de un R-módulo libre de rango finito es libre de rango finito. Además el rango del submódulo es menor o igual que el del módulo.*

Demostración. Lo probamos por inducción sobre el rango de R^n. Sea $M \subset R^n$. Si $n = 1$ entonces cualquier submódulo de R es un ideal, que será principal por la hipótesis de que R es DIP. Por lo tanto M será de la forma (a) para algún $a \in R$, y como M es no nulo, es libre de rango 1. Consideramos el siguiente diagrama:

$$0 \to R^{n-1} \xrightarrow{i} R^n \xrightarrow{\pi} R \to 0,$$

donde i es la inclusión natural $i(x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, 0)$, y π es la proyección sobre la última coordenada. Por la proposición anterior sabemos que es una sucesión exacta. Ahora, restringiéndonos a M tenemos lo siguiente:

$$0 \to M \cap R^{n-1} \xrightarrow{i} M \xrightarrow{\pi} \pi(M) \to 0.$$

Por hipótesis de inducción tenemos que $M \cap R^{n-1}$ es libre de rango $\leq n-1$ con base $\{m_1, \ldots, m_r\}$ con $r \leq n-1$. Distinguimos dos casos. Si $\pi(M) = 0$ entonces $M \cap R^{n-1} = i(M \cap R^{n-1}) = \operatorname{Ker} \pi = M$, luego M está contenido en R^{n-1}, es decir, M es submódulo de R^{n-1}, y por hipótesis de inducción es libre de rango $\leq n-1$. Si $\pi(M) \neq 0$ entonces es un submódulo no nulo de R, luego es un ideal no nulo de R. Por ser R un dominio de ideales principales $\pi(M) = (r)$ para algún $r \in R$ no nulo, luego dado $m \in M$, $\pi(m) = r \cdot x$ para algún $x \in R$. Por ser π sobreyectiva existe un $m_n \in M$ tal que $\pi(m_n) = r$, por lo que tomando $y := m - m_n x$ tenemos que $\pi(y) = 0$, es decir, $y \in \operatorname{Ker} \pi$. Esto último implica que $y \in \operatorname{Im} i$ por ser una sucesión exacta, luego existen $x_1, \ldots, x_r \in R$ tales que $y = m - m_n x = m_1 x_1 + \cdots + m_r x_r$, y por lo tanto m se escribe como una combinación R-lineal de elementos del conjunto $S := \{m_1, \ldots, m_r, m_n\} \subset M$. Por lo tanto S es un conjunto generador. Para ver que es una base, y por tanto concluir que M es libre de rango $\leq n$, consideramos una combinación R-lineal nula

$$m = \lambda_1 m_1 + \cdots + \lambda_r m_r + \lambda_n m_n = (0, \ldots, 0) = 0_M.$$

Cada $m_i := (x_{1,i}, \ldots, x_{n-1,i}, 0) \in R^{n-1}$ para $i = 1, \ldots, r$, mientras que $m_n := (y_1, \ldots, y_n) \in R^n$. Como S genera M y $\pi(M) \neq 0$ se tiene que $y_n \neq 0$. De la ecuación

$$\sum_{i=1}^{r} \lambda_i (x_{1,i}, \ldots, x_{n-1,i}, 0) + \lambda_n (y_1, \ldots, y_n) = (0, \ldots, 0),$$

igualando las últimas cordenadas de ambos miembros, se deduce que $\lambda_n y_n = 0$, y como R es un dominio e $y_n \neq 0$ necesariamente $\lambda_n = 0$. Sustituyendo resulta que

$$\sum_{i=1}^{r} \lambda_i m_i = 0_M,$$

pero por ser $\{m_1, \ldots, m_r\}$ base de $M \cap R^{n-1}$ se tiene que necesariamente $\lambda_1 = \cdots = \lambda_r = 0$, y por lo tanto todos los coeficientes son nulos, es decir, que el conjunto S es base de M, lo que concluye nuestra prueba. □

Definición I.2.10. Sea M un R-módulo, y sean $N_1, \ldots, N_k$ submódulos suyos.

1. La suma $N_1 + \cdots + N_k$ definida como el conjunto $\{a_1 + \cdots + a_k \mid a_i \in N_i \text{, para todo } i\}$ es un submódulo de M. De hecho es el menor submódulo de M que contiene a los submódulos $N_1, \ldots, N_k$.

2. Se dice que la suma $N_1 + \cdots + N_k$ es una *suma directa* de submódulos, y lo denotaremos por $N_1 \oplus \cdots \oplus N_k$, si

$$N_i \cap \sum_{i \neq j} N_j = 0$$

Es decir, que todo elemento de la suma se descompone de manera única como suma de elementos de los submódulos N_j.

3. Se dice que M es *indescomponible* si no se puede escribir como suma directa de dos submódulos suyos no nulos. En caso contrario se dice que es *descomponible.*

4. Se dice que M es *completamente reducible* si es suma directa de submódulos suyos irreducibles. A cada uno de sus sumandos se le denomina *constituyente* de M.

I.2.b. Producto tensorial de módulos

Definición I.2.11. Sea R un anillo. Sean M, N y P tres R-módulos. Una aplicación $f : M \times N \to P$ se dice *R-bilineal* si fijado $x \in M$ se tiene que la aplicación $y \to f(x, y)$ de N en P es R-lineal, y si fijado $y \in N$ la aplicación $x \to f(x, y)$ de M en P es R-lineal.

Nuestro objetivo es construir a partir de M y N un R-módulo T, llamado *producto tensorial* de M y N, que permita entender las aplicaciones R-bilineales entre $M \times N$ y P como aplicaciones R-lineales entre T y P, independientemente del R-módulo P escogido.

Proposición I.2.12. *Sean R un anillo, M y N dos R-módulos. Entonces existe un único par (salvo isomorfismo) (T, h) formado por un R-módulo T y una aplicación R-bilineal $h : M \times N \to T$, con la siguiente propiedad:*

Dado un R-módulo P y una aplicación R-bilineal $f : M \times N \to P$, existe una única aplicación R-lineal $f' : T \to P$ de forma que $f = f' \circ h$, es decir, toda aplicación R-bilineal desde $M \times N$ factoriza por T.

Demostración.

1. *Existencia.* Sea F el R-módulo libre generado por $M \times N$. Los elementos de F consisten en combinaciones lineales de elementos de $M \times N$ con coeficientes en el anillo R, es decir, de la forma

$$\sum_{i=1}^{n} a_i \cdot (x_i, y_i) \, , (x_i, y_i) \in M \times N \, , a_i \in R.$$

Sea E el submódulo de F generado por los elementos de F de las formas siguientes:

a) $(x_1 + x_2, y) - (x_1, y) - (x_2, y)$

b) $(x, y_1 + y_2) - (x, y_1) - (x, y_2)$

c) $(ax, y) - a \cdot (x, y)$

d) $(x, ay) - a \cdot (x, y)$

para $x, x_1, x_2 \in M$, $y, y_1, y_2 \in N$ y $a \in R$. Sea $T := F/E$. Para cada elemento (x, y) de F denotamos a su clase en T como $x \otimes y$. Por lo tanto T está generado por los elementos de la forma $x \otimes y$, y de nuestra definición se desprenden las siguientes propiedades:

a) $(x_1 + x_2) \otimes y = x_1 \otimes y + x_2 \otimes y$

b) $x \otimes (y_1 + y_2) = x \otimes y_1 + x \otimes y_2$

c) $(ax) \otimes y = x \otimes (ay) = a(x \otimes y)$

para cualesquiera $x, x_1, x_2 \in M$, $y, y_1, y_2 \in N$ y $a \in R$. Es decir, que la aplicación $h : M \times N \to T$ definida como $h(x, y) = x \otimes y$ es R-bilineal. Sea ahora $f : M \times N \to P$ una aplicación R-bilineal, donde P es un R-módulo. Por ser f bilineal se anula en todos los generadores de E, en consecuencia en todo E, luego induce un homomorfismo entre R-módulos $f' : T \to P$ bien definido, de forma que $(f' \circ h)(x, y) = f'(x \otimes y) = f(x, y)$. La aplicación f' queda unívocamente determinada por esta condición, y por lo tanto el par (T, h) satisface las condiciones de la proposición.

2. *Unicidad.* Sea otro par (T', h') que cumple también estas propiedades. Reemplazando (P, f) por (T', h') obtenemos que existe una única aplicación R-lineal $i : T \to T'$ tal que $h' = i \circ h$. Intercambiando T por T' obtenemos que existe una única aplicación R-lineal $i' : T' \to T$ tal que $h = i' \circ h'$. Sustituyendo obtenemos que

$$h = i' \circ (i \circ h) = (i' \circ i) \circ h.$$

Recíprocamente obtenemos que

$$h' = (i \circ i') \circ h'.$$

Como los pares (T, id_T), $(T', \mathrm{id}_{T'})$ verifican que $h = \mathrm{id}_T \circ h$ y $h' = \mathrm{id}_{T'} \circ h'$, respectivamente, por lo probado en el apartado anterior concluimos que $i' \circ i = \mathrm{id}_T$, $i \circ i' = \mathrm{id}_{T'}$. Por lo tanto ambas composiciones son la identidad, lo que implica que i es un isomorfismo.

□

Observación I.2.13. El R-módulo T construido a partir de M y N se suele denotar por $M \otimes_R N$, o simplemente $M \otimes N$ si no hay ambigüedad sobre el anillo R en el que se trabaja. Se puede ver como un R-módulo libre generado por los elementos $x \otimes y$, denominados *tensores descomponibles*. Si $(x_i)_{i \in I}$, $(y_j)_{j \in J}$ son dos familias que generan M y N respectivamente, entonces los elementos $x_i \otimes y_j$ generan $M \otimes N$. En particular, si M y N son finitamente generados, entonces también lo es $M \otimes N$.

Ejemplo I.2.14. Sean $m, n \in \mathbb{N}$ y $d = \gcd(m, n)$. Veamos que

$$\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \cong \mathbb{Z}_d.$$

Sea la aplicación $f : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_d$ definida como:

$$f(x + m\mathbb{Z}, y + n\mathbb{Z}) = xy + d\mathbb{Z}.$$

Está bien definida y es bilineal, luego por la proposición anterior existe una única aplicación lineal $g : \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \to \mathbb{Z}_d$ tal que

$$g((x + m\mathbb{Z}) \otimes (y + n\mathbb{Z})) = xy + d\mathbb{Z}.$$

Sea ahora la aplicación $h : \mathbb{Z}_d \to \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$ definida como:

$$h(l + d\mathbb{Z}) = (l + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}).$$

Veamos que está bien definida. Sean $l, l' \in \mathbb{Z}$ tales que $l - l' \in d\mathbb{Z}$, luego existe $k \in \mathbb{Z}$ tal que $l = l' + kd$. Por la identidad de Bézout existen $a, b \in \mathbb{Z}$ tales que $d = am + bn$. Sustituyendo en la expresión anterior obtenemos que $l = l' + akm + bkn$. Por lo tanto:

$$\begin{aligned} h(l + d\mathbb{Z}) &= h(l' + akm + bkn + d\mathbb{Z}) = (l' + akm + bkn + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \\ &= (l' + bkn + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) = (1 + m\mathbb{Z}) \otimes (l' + bkn + n\mathbb{Z}) \\ &= (1 + m\mathbb{Z}) \otimes (l' + n\mathbb{Z}) = (l' + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) = h(l' + d\mathbb{Z}). \end{aligned}$$

La aplicacion h cumple que

$$(h \circ g)((x + m\mathbb{Z}) \otimes (y + n\mathbb{Z})) = h(xy + d\mathbb{Z}) = (xy + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) = (x + m\mathbb{Z}) \otimes (y + n\mathbb{Z}).$$

Además,

$$(g \circ h)(l + d\mathbb{Z}) = g((l + m\mathbb{Z}) \otimes (1 + n\mathbb{Z})) = l + d\mathbb{Z}.$$

Hemos comprobado que $h = g^{-1}$ y por lo tanto g es un isomorfismo entre $\mathbb{Z}$-módulos.

Ejemplo I.2.15. Sean V y W dos espacios vectoriales. Definimos una aplicación $\phi : V^* \otimes W \to \mathrm{Hom}(V, W)$ que sobre los elementos descomponibles del producto tensorial actúa como

$$\phi(v^* \otimes w) = f_{v^*,w},$$

donde $f_{v^*,w}$ es la aplicación lineal $V \to W$ definida por $f_{v^*,w}(u) = v^*(u)w$. Como cada elemento de $V \otimes W$ puede escribirse como suma de tensores descomponibles esta asignación se extiende a un homomorfismo, que denotamos ϕ. Supongamos que $v^* \otimes w \in \ker(\phi)$. Entonces $f_{v^*,w}(u) = v^*(u)w = 0$ para cualquier $u \in V$. Si v^* es la función 0, entonces $v^* \otimes w = 0 \otimes w = 0$. Supongamos que v^* es no nulo, luego existe $u \in V$ tal que $v^*(u) \neq 0$, luego necesitamos que $w = 0$ para que $v^* \otimes w = 0$. Por lo tanto $\ker(\phi) = \{0\}$ y ϕ es inyectiva. Concluimos así que $\dim(\mathrm{Hom}(V, W)) = \dim(V^* \otimes W)$, y por lo tanto

$$\mathrm{Hom}(V, W) \cong V^* \otimes W.$$

I.2.c. Anillos de grupos

El siguiente concepto será importante a la hora de entender las representaciones de grupos. Se trata de dotar a un grupo (que asumiremos finito) de estructura de anillo a través de un anillo dado. Así, un anillo de grupos es por un lado un anillo y por otro un módulo libre cuyo anillo de escalares es el anillo a través el cual ha sido construido, y una de cuyas bases es el conjunto de elementos del grupo de partida.

Definición I.2.16. Sea R un anillo conmutativo con elemento unidad $1_R \neq 0$, y sea $G = \{g_1, \ldots, g_n\}$ un grupo finito. Definimos el *anillo del grupo G con coeficientes en R*, que se denotará por RG, como el conjunto de las sumas formales

$$a_1 g_1 + a_2 g_2 + \cdots + a_n g_n \ \ , a_i \in R \, , 1 \leq i \leq n$$

La suma en RG se define componente a componente

$$(a_1g_1+\cdots+a_ng_n)+(b_1g_1+\cdots+b_ng_n)=(a_1+b_1)g_1+\cdots+(a_n+b_n)g_n \;\; a_i,b_i\in R\,, 1\leq i\leq n$$

donde a_i+b_i es la suma en el anillo R. La multiplicación se define primero para las tuplas $(ag_i)(bg_j)$ como $(ag_i)(bg_j)=(ab)g_k$, donde ab es el producto en el anillo R, y $g_k=g_ig_j$ es la operación definida en el grupo. Esta definición se extiende a todas las sumas formales mediante la propiedad distributiva de manera que el coeficiente de g_k en el producto $(a_1g_1+\cdots+a_ng_n)(b_1g_1+\cdots+b_ng_n)$ es

$$\sum_{g_ig_j=g_k} a_ib_j$$

Con estas operaciones RG es un anillo unitario cuyo elemento unidad es $1_R\cdot e$, donde e es el neutro para la operación en el grupo G. RG será conmutativo si y solo si G es abeliano.

Ejemplo I.2.17**.** Sea $\mathbb{H}=\{e,\bar{e},\mathtt{i},\bar{\mathtt{i}},\mathtt{j},\bar{\mathtt{j}},\mathtt{k},\bar{\mathtt{k}}\}$ el grupo cuaternión, y consideramos el anillo de grupo $\mathbb{RH}$. Un elemento cualquiera del anillo vendrá dado por la siguiente suma formal

$$x_1e+x_2\bar{e}+x_3\mathtt{i}+x_4\bar{\mathtt{i}}+x_5\mathtt{j}+x_6\bar{\mathtt{j}}+x_7\mathtt{k}+x_8\bar{\mathtt{k}}$$

donde los x_i son números reales. Veamos un ejemplo de operación en el anillo del grupo:

$$(3+\pi\cdot\mathtt{i})\cdot(7\cdot\mathtt{k})=(3\cdot1)(7\cdot\mathtt{k})+(\pi\cdot\mathtt{i})\cdot(7\cdot\mathtt{k})=(3\cdot7)\cdot(1\cdot\mathtt{k})+(\pi\cdot7)\cdot(\mathtt{i}\cdot\mathtt{k})=21\cdot\mathtt{k}+(7\pi)\cdot(\bar{\mathtt{j}})$$

Definimos el *anillo de Hamilton* como el conjunto

$$\mathbf{Q}=\{a\cdot e+b\cdot\mathtt{i}+c\cdot\mathtt{j}+d\cdot\mathtt{k}:a,b,c,d\in\mathbb{R}\},$$

donde $\mathtt{i}^2=\mathtt{j}^2=\mathtt{k}^2=\mathtt{ijk}=\bar{e}$, y la adición se define componente a componente. Nótese que $\mathbb{RH}$ no es isomorfo al anillo de Hamilton. Esto se debe a que en el anillo se cumplen relaciones adicionales entre los elementos que no se cumplen en $\mathbb{RH}$. Por ejemplo en el anillo de Hamilton $\bar{\mathtt{i}}=1\cdot\bar{\mathtt{i}}=1\cdot(-\mathtt{i})=-\mathtt{i}$, mientras que en el anillo de grupo $\bar{\mathtt{i}}\neq(-1)\cdot\mathtt{i}$ pues representan sumas formales distintas.

A la hora de estudiar las representaciones de grupos nos interesará en concreto el caso de un anillo de grupo en el que el anillo R es a su vez un cuerpo F. En este caso el anillo FG, que también será un FG-módulo libre, es un espacio vectorial sobre F cuya base es G, y por lo tanto su dimensión será el orden del grupo G.

Definición I.2.18**.** Sea G un grupo finito. Se define el *centro* del anillo del grupo G, $\mathbb{C}G$, que se denotará como $Z(\mathbb{C}G)$, como el conjunto

$$Z(\mathbb{C}G):=\{z\in\mathbb{C}G:zr=rz,\forall r\in\mathbb{C}G\}.$$

Definición I.2.19**.** Sean $C_1,\ldots,C_r$ las clases de conjugación de un grupo G. Para cada $1\leq i\leq r$, definimos

$$\overline{C_i}:=\sum_{g\in C_i} g\in\mathbb{C}G.$$

Los elementos $\overline{C}_1,\ldots,\overline{C}_r$ de $\mathbb{C}G$ se denominan *sumas de clase* de G.

Proposición I.2.20. *Las sumas de clase de un grupo finito G pertenecen al centro de $\mathbb{C}G$. De hecho, forman una base de $\mathbb{C}G$.*

Demostración. Sean C una clase de conjugación de G, y $g \in G$ un representante de C. Entonces los elementos de C son $x_1^{-1}gx_1, \ldots, x_r^{-1}gx_r$, para ciertos $x_1, \ldots, x_r \in G$. Por lo tanto

$$\overline{C} = \sum_{i=1}^{r} x_i^{-1}gx_i.$$

Para cualquier $h \in G$, $h^{-1}\overline{C}h = \sum_{i=1}^{r} h^{-1}x_i^{-1}gx_ih$. Si i varía entre 1 y r, los elementos $h^{-1}x_i^{-1}gx_ih$ varían en todo C puesto que

$$h^{-1}x_i^{-1}gx_ih = h^{-1}x_k^{-1}gx_kh \iff x_i^{-1}gx_i = x_k^{-1}gx_k.$$

Por lo tanto $\sum_{i=1}^{r} h^{-1}x_i^{-1}gx_ih = \overline{C}$, y por lo tanto $h^{-1}\overline{C}h = \overline{C}$; es decir, $h\overline{C} = \overline{C}h$. Tenemos que $\overline{C}$ conmuta con todo $h \in G$, y por lo tanto también conmuta con todo $\sum_{h\in G} a_h h \in \mathbb{C}G$, luego $\overline{C} \in Z(\mathbb{C}G)$.
Para la segunda parte observemos primero que $\overline{C_1}, \ldots, \overline{C_r}$, son linealmente independientes puesto que las clases $C_1, \ldots, C_r$ forman una partición disjunta de G. Veamos ahora que generan todo $Z(\mathbb{C}G)$. Sea $r = \sum g \in Ga_g g \in Z(\mathbb{C}G)$. Para $h \in G$ (que en particular es un elemento de $\mathbb{C}G$), tenemos que $rh = hr$, luego $h^{-1}rh = r$. Esto implica que $\sum_{g\in G} a_g h^{-1}gh = \sum_{g\in G} a_g g$. Por lo tanto para cada $g \in G$ el coeficiente a_g de g es igual al coeficiente $a_{h^{-1}gh}$ de $h^{-1}gh$. En particular esto implica que la asignación $g \mapsto a_g$ es constante en O_g, luego $r = \sum_{i=1}^{r} a_i\overline{C_i}$, donde a_i es el coeficiente de un representante de la clase de conjugación C_i. □

CAPÍTULO II

Teoría de representación

En este capítulo vamos a introducir los conceptos básicos de la teoría de representación de grupos, necesaria para entender la noción de caracteres de grupos, pues estos últimos están intimamente ligados a las representaciones. Una representación de grupos asocia a cada elemento del grupo una matriz invertible, luego la operación interna del grupo se podrá ver como una multiplicación de matrices usual. Veremos también que una representación de un grupo G es equivalente a un FG-módulo sobre un cuerpo F.

II.1. Representación de grupos.

Definición II.1.1. Sean G un grupo finito, F un cuerpo y V un F-espacio vectorial. Denotaremos por $\mathrm{GL}(V)$ al grupo formado por los F-automorfismos del F-espacio vectorial V, con la operación composición.

1. Una *representación lineal* de G en V es un homomorfismo de grupos $\rho : G \to \mathrm{GL}(V)$. El *grado* de la representación es la dimensión de V como F-espacio vectorial.

2. Sea n un entero positivo. Una *representación matricial* de G es un homomorfismo de grupos $\rho : G \to \mathrm{GL}_n(F)$, donde $\mathrm{GL}_n(F)$ es el grupo de las matrices $n \times n$ invertibles con coeficientes en F.

3. Una representación lineal o matricial se dice *fiel* si es inyectiva.

Observación II.1.2. A partir de ahora el término representación denotará indistintamente representación lineal o matricial, pues en nuestro contexto ambas son equivalentes. En efecto, si V es un F-espacio vectorial de dimensión finita n, fijada una base de nuestro espacio obtenemos que $\mathrm{GL}(V) \cong \mathrm{GL}_n(F)$. De esta forma toda representación lineal induce una representación matricial y viceversa.

Ejemplo II.1.3. Sea $\mathfrak{D}_4 = \{r, s \mid r^4 = s^2 = (sr)^2 = 1\}$ el grupo diédrico de orden 8, que no es más que el grupo de simetrías del cuadrado que tienes por vértices los puntos del plano $(1,1), (-1,1), (-1,-1), (1,-1)$, donde r denota la rotación en sentido antihorario de 90 grados y s denota la reflexión respecto del eje horizontal $\{y = 0\}$. Sean las matrices

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

definimos la aplicación $\rho : \mathfrak{D}_4 \to \mathrm{GL}_2(\mathbb{C}), r^i s^j \mapsto R^i S^j$, para $0 \leq i \leq 3$ y $0 \leq j \leq 2$. Que es un homomorfismo es inmediato, luego ρ es una representación de $\mathfrak{D}_4$ de grado 2.

Más generalmente si tenemos $\mathfrak{D}_n = \{r, s \mid r^n = s^2 = (sr)^2 = 1\}$, las matrices

$$R = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \; S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

y la aplicación $\rho : \mathfrak{D}_n \to \mathrm{GL}_2(\mathbb{C}), r^i s^j \mapsto R^i S^j$, para $0 \leq i \leq n-1$ y $0 \leq j \leq 2$, nos dan una representación de grado 2 del grupo diédrico de orden $2n$.

Vamos a ver ahora la relación entre FG-módulos y representaciones de grupos. Sea ρ una representación de $G := \{g_1, \ldots, g_n\}$ en un F-espacio vectorial V. Para cada $1 \leq i \leq n$, $\rho(g_i)$ es un endomorfismo de V. Podemos dotar a V de estructura de FG-módulo si definimos la acción del anillo de grupo FG sobre un elemento de V de la siguiente manera:

$$\left(\sum_{i=1}^{n} \lambda_i g_i\right) \cdot v = \sum_{i=1}^{n} \lambda_i \cdot \rho(g_i)(v),$$

para cualesquiera $\sum_{i=1}^n \lambda_i g_i \in FG$ y $v \in V$. Vamos a verificar que esto es en efecto un FG-módulo.

1. $((\sum_{i=1}^n \lambda_i g_i) + (\sum_{i=1}^n \beta_i g_i)) \cdot v = (\sum_{i=1}^n (\lambda_i + \beta_i)\, g_i) \cdot v = \sum_{i=1}^n (\lambda_i + \beta_i) \cdot \rho(g_i)(v) = \sum_{i=1}^n (\lambda_i \rho(g_i)(v) + \beta_i \rho(g_i)(v)) = \sum_{i=1}^n \lambda_i \rho(g_i)(v) + \sum_{i=1}^n \beta_i \rho(g_i)(v) = (\sum_{i=1}^n \lambda_i g_i) \cdot v + (\sum_{i=1}^n \beta_i g_i) \cdot v$.

2. Para probar el segundo axioma y para evitar lo engorroso de la notación lo probaremos para la suma formal de un único elemento $g_i \cdot v = \rho(g_i)(v)$, y el resultado para la acción de FG se extenderá de forma lineal. Para esto es fundamental el hecho de que ρ es un homomorfismo de grupos.
$(g_i g_j) \cdot v = \rho(g_i g_j)(v) = (\rho(g_i) \circ \rho(g_j))(v) = \rho(g_i)(\rho(g_j)(v)) = g_i \cdot (g_j \cdot v)$.

3. Aquí es clave el hecho de que $\rho(g_i)$ sea un endomorfismo de V.
$(\sum_{i=1}^n \lambda_i g_i) \cdot (v + w) = \sum_{i=1}^n \lambda_i \rho(g_i)(v + w) = \sum_{i=1}^n \lambda_i (\rho(g_i)(v) + \rho(g_i)(w)) = \sum_{i=1}^n \lambda_i \rho(g_i)(v) + \sum_{i=1}^n \lambda_i \rho(g_i)(w) = (\sum_{i=1}^n \lambda_i g_i) \cdot v + (\sum_{i=1}^n \lambda_i g_i) \cdot w$.

4. $(1_F \cdot e) \cdot v = 1_F \rho(e)(v) = 1_F \cdot v = v$.

Recíprocamente supongamos que tenemos un FG-módulo V. Por ser un FG-módulo en particular será un F-módulo, lo que sabemos que es equivalente a ser un espacio vectorial. Para cada $g \in G$ definimos la aplicación ϕ_g de V en V como $\phi_g(v) = g \cdot v$, donde $g \cdot v$ viene dado por la acción del elemento del anillo FG sobre V. Como los elementos de F conmutan con cada uno de los $g \in G$ se sigue de los axiomas de módulo que para todos $v, w \in V$ y para todos $a, b \in F$, se tiene que

$$\phi_g(av + bw) = g \cdot (av + bw) = g \cdot (av) + g \cdot (bw) = a(g \cdot v) + b(g \cdot w) = a\phi_g(v) + b\phi_g(w).$$

Es decir, para cualquier $g \in G$, ϕ_g es una aplicación lineal. Si ahora definimos $\phi : G \to \mathrm{End}(V); g \mapsto \phi_g$, tenemos que de los axiomas de módulo se desprende que

$$\phi(g_i g_j)(v) = \phi_{g_i g_j}(v) = (g_i g_j)(v) = g_i(g_j(v)) = \phi_{g_i}(\phi_{g_j}(v)) = (\phi(g_i) \circ \phi(g_j)(v).$$

Luego ϕ es un homomorfismo de grupos que manda cada elemento del grupo G en un endomorfismo de V que, fijando una base en V, vendrá dado por una matriz. Además $\phi(g^{-1}) = \phi(g)^{-1}$, luego las matrices son necesariamente invertibles y por lo tanto podemos ver ϕ como un homomorfismo de G en $\mathrm{GL}(V)$. Así hemos probado que un FG-módulo induce una representación de grupos. El siguiente resultado recoge la información que hemos probado.

Proposición II.1.4. *Sean F un cuerpo, G un grupo finito y V un conjunto. Entonces V es un FG-módulo si y solo si V es un F-espacio vectorial y $\phi : G \to \mathrm{GL}(V)$ (como la hemos definido antes) es una representación de G.*

Definición II.1.5. Sean G un grupo finito, V un espacio vectorial y $U \subset V$ un subespacio suyo. Diremos que U es *G-estable* si $g \cdot u \in U$ para todo $g \in G, u \in U$.

Si vemos V como un FG-módulo, entonces se sigue de las definiciones que sus submódulos son sus subespacios G-estables.

Definición II.1.6. Dos representaciones de un grupo finito G se dirán *equivalentes* si los FG-módulos que inducen son isomorfos.

Supongamos que tenemos $\phi : G \to \mathrm{GL}(V)$ y $\psi : G \to \mathrm{GL}(W)$ dos representaciones de un grupo finito G, donde V y W son dos F-espacios vectoriales, y sea $f : V \to W$ un isomorfismo entre FG-módulos. En particular será un isomorfismo entre F-módulos; es decir, un isomorfismo entre espacios vectoriales, luego $\dim V = \dim W$. Por lo tanto ambas representaciones tienen el mismo grado. Además, dados $g \in G, v \in V$ tenemos que $f(g \cdot v) = g \cdot (f(v))$ por ser un isomorfismo de FG-módulos. En el lenguaje de la acción del anillo de grupo esto significa que $f(\phi(g)(v)) = \psi(g)(f(v))$, lo que implica que $f \circ \phi(g) = \psi(g) \circ f$, para todo $g \in G$. En particular dos representaciones ϕ, ψ de G sobre el mismo espacio vectorial V son equivalentes si y solo si existe $f \in \mathrm{GL}(V)$ tal que $f \circ \phi(g) \circ f^{-1} = \psi(g)$, para todo $g \in G$. En términos matriciales esto se traduce en que existe una matriz invertible P tal que $P\phi(g)P^{-1} = \psi(g)$ para todo $g \in G$. Este hecho no es más que la existencia de bases B_1 y B_2 en V tales que la matriz de $\phi(g)$ respecto de B_1 coincide con la matriz de $\psi(g)$ respecto de B_2 para todo $g \in G$.

Definición II.1.7. Sean $\phi : G \to \mathrm{GL}(V)$ y $\psi : G \to \mathrm{GL}(W)$ dos representaciones de un grupo finito G sobre un cuerpo F. La suma directa $V \oplus W$ tiene estructura de FG-módulo, y por tanto de espacio vectorial. Sea $\rho : \mathrm{GL}(V) \times \mathrm{GL}(W) \to \mathrm{GL}(V \oplus W); (\phi(g), \psi(g)) \mapsto \phi(g) + \psi(g)$. Entonces el homomorfismo de G a $\mathrm{GL}(V \oplus W)$ viene dado por $\rho \circ (\phi \times \psi)$. En términos matriciales esto se puede ver como la aplicación

$$g \mapsto \begin{pmatrix} \phi(g) & 0 \\ 0 & \psi(g) \end{pmatrix}.$$

Definición II.1.8. Sean $\phi : G \to \mathrm{GL}(V)$ y $\psi : G \to \mathrm{GL}(W)$ dos representaciones de un grupo finito G sobre un cuerpo F. Definimos la representación del producto tensorial como sigue

$$\rho : G \to \mathrm{GL}(V \otimes W); g \mapsto \phi(g) \otimes \psi(g).$$

Recíprocamente dados dos FG-módulos V y W, definimos la acción de G sobre el producto tensorial como $g \cdot (v \otimes w) = (g \cdot v) \otimes (g \cdot w)$, para cualesquiera $g \in G$, $v \in V$, $w \in W$.

En términos matriciales la representación viene dada por el *producto de Kronecker* de las matrices de las representaciones ϕ y ψ. Denotemos $A := \phi(g) = \{a_{ij}\}$ y $B := \psi(g)$ para cierto $g \in G$, entonces el producto de Kronecker se define como

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{bmatrix}.$$

Definición II.1.9. Sean F un cuerpo, V y W dos F-espacios vectoriales y $f : V \to W$ una aplicación lineal entre ellos. Se define la aplicación *traspuesta* de f como la aplicación lineal $f^t : W^* \to V^*; \phi \mapsto \phi \circ f$.

Proposición II.1.10. *Sea F un cuerpo. Sean V, W dos F-espacios vectoriales de dimensión finita y $f : V \to W$ una aplicación lineal entre ellos. Consideramos bases B_V, B_W en V y W, respectivamente, y denotamos por $A = (a_{ij})$ a la matriz de f respecto dichas bases. Entonces la matriz de f^t respecto de las bases duales B_V^*, B_W^* es A^t.*

Demostración. Si $B_V := \{v_1, \dots, v_n\}$ y $B_W := \{w_1, \dots, w_n\}$, entonces $B_V^* := \{v_1^*, \dots, v_n^*\}$ y $B_W^* := \{w_1^*, \dots, w_n^*\}$ son bases de V^* y W^*, respectivamente. Si $B = (b_{ij})$ es la matriz de f^t respecto dichas bases se cumple que

$$b_{ji} = (f^t(w_i^*))(v_j) = (w_i^* \circ f)(v_j) = w_i^*(f(v_j)) = w_i^*\left(\sum_{k=1}^{m} a_{kj} w_k\right) = \sum_{k=1}^{m} a_{kj} w_i^*(w_k) = a_{ij}.$$

□

Definición II.1.11. Sea $\rho : G \to \mathrm{GL}(V)$ una representación de un grupo finito G sobre un F-espacio vectorial V. Definimos la *representación dual* de ρ como el homomorfismo $\rho^* : G \to \mathrm{GL}(V^*); g \mapsto (\rho(g^{-1}))^t$.

Observación II.1.12. Sean G un grupo finito, F un cuerpo y V y W dos FG-módulos. Entonces por las definiciones anteriores y el Ejemplo I.4.15, tenemos que $\mathrm{Hom}(V, W)$ con la acción $g \cdot f(v) = gf(g^{-1}v)$ para cualesquiera $g \in G$, $f \in \mathrm{Hom}(V, W)$ y $v \in V$, es un FG-módulo y por lo tanto induce una representación.

II.2. Representaciones irreducibles.

Definición II.2.1. Sean G un grupo finito, F un cuerpo y V un FG-módulo. Sea $\rho : G \to \mathrm{GL}(V)$ la representación de G en V asociada. Se dice que ρ es *reducible*, *irreducible*, *descomponible*, *indescomponible*, o *completamente reducible* si V como FG-módulo lo es.

Ejemplo II.2.2. Sea $U = \mathbb{C}$ y sea G un grupo finito. Consideremos la acción trivial de G sobre U; es decir, $g \cdot u = u$ para cualesquiera $g \in G$, $u \in U$. Está claro que, como $\mathbb{C}G$-módulo, U es irreducible, y la representación de G que induce se denomina *representación trivial.* Claramente en la base canónica la matriz de la representación es la identidad.

Teorema II.2.3 (Teorema de Maschke)**.** *Sean G un grupo finito y F un cuerpo cuya característica no divide al orden de G. Si V es un FG-módulo y U es un submódulo propio suyo, entonces existe un submódulo W de V tal que $V = U \oplus W$.*

Demostración. La clave de la demostración está en encontrar un FG-homomorfismo

$$\pi : V \to U,$$

que sea una proyección sobre U; es decir, que cumpla que $\pi(u) = u$, para todo $u \in U$. Supongamos que existe dicho FG-homomorfismo, y sea $W := \ker \pi$. Como π es un homomorfismo de FG-módulos, W es un FG-submódulo, y de hecho es el suplementario de U que buscamos. En efecto, si $v \in U \cap W$, entonces a su vez se cumple que $\pi(v) = v$ y que $\pi(v) = 0$, luego necesariamente $U \cap W = \{0\}$. Por otro lado dado $v \in V$ arbitrario, podemos escribir $v = \pi(v) + (v - \pi(v))$. Por definición de π, $\pi(v) \in U$, y $\pi(v - \pi(v)) = \pi(v) - \pi^2(v) = \pi(v) - \pi(v) = 0$, luego $v - \pi(v) \in W$. Se concluye así que $V = U \oplus W$.

Para finalizar la demostración necesitamos probar que existe dicho FG-homomorfismo. Como U es un subespacio de V podemos tomar una base B_U de U y completarla hasta obtener una base B de V. Si tomamos U' el subespacio generado por el conjunto $B \setminus B_U$, tenemos entonces que $V = U \oplus U'$. Sin embargo, U' podría no ser un submódulo (un subespacio G-estable), como queremos. Sea $\pi_0 : V \to U$ la proyección sobre U respecto a la descomposición anterior; es decir, π_0 verifica que $\pi_0(u + u') = u$ para cualesquiera $u \in U$, $u' \in U'$. La idea será obtener nuestra proyección π promediando π_0 sobre G. Para cada $g \in G$ definimos la aplicación $g\pi_0 g^{-1}$ como $g\pi_0 g^{-1}(v) = g \cdot \pi_0(g^{-1} \cdot v)$, para cada $v \in V$. Aquí $(\cdot)$ denota la acción de los elementos del anillo FG. Como U es un submódulo, y por tanto es G-estable, entonces la imagen de la aplicación está contenida en U. Por otro lado, como g y g^{-1} actúan como aplicaciones F-lineales entonces $g\pi_0 g^{-1}$ es una aplicación F-lineal. Finalmente, como U es G-estable, y por definición de π_0, $\pi_0(g^{-1} \cdot u) = g^{-1} \cdot u$, concluimos que $g\pi_0 g^{-1}(u) = u$, para todo $u \in U$, y por lo tanto es una proyección de V sobre U como espacio vectoriales.

Sea ahora $n := \mathrm{ord}(G)$, podemos ver n como un elemento de F puesto que $n = e_F + \overset{n)}{\cdots} + e_F$, donde e_F denota al elemento neutro respecto del producto en F. Por hipótesis n es nulo no en F, luego existe $m \in F$ tal que $nm = e_F = mn$. Definimos

$$\pi := m \sum_{g \in G} g\pi_0 g^{-1},$$

que es de nuevo una aplicación F-lineal de V en U por ser una combinación lineal de aplicaciones F-lineales de V en U. Como dado $u \in U$ y $g \in G$ arbitrarios tenemos que $g\pi_0 g^{-1}(u) = u$, entonces $\pi(u) = m(nu) = e_F u = u$. Luego π es una proyección de V sobre U. Resta probar que es un FG-homomorfismo, y por ser una aplicación F-lineal basta probar que también respeta la acción de G; es decir, que $\pi(h \cdot v) = h \cdot \pi(v)$, para cualesquiera $h \in G$, $v \in V$. En efecto,

$$\begin{aligned} \pi(h \cdot v) &= m \sum_{g \in G} g\pi_0 g^{-1}(h \cdot v) = m \sum_{g \in G} g\pi_0(g^{-1} \cdot (h \cdot v)) \\ &= m \sum_{g \in G} h(h^{-1}g)\pi_0((g^{-1}h) \cdot v) = m \sum_{k \in G} h \cdot k\pi_0 k^{-1}(v) = h \cdot \pi(v), \end{aligned}$$

donde $k := h^{-1}g$ para todo $g \in G$ también recorre todo G. □

Corolario II.2.4. *Sean G un grupo finito, V y W dos $\mathbb{C}G$-módulos, y $g : V \to W$ un $\mathbb{C}G$-homomorfismo. Entonces existe un submódulo U de V tal que $V = U \oplus \ker g$ verificando que $U \cong \operatorname{im} g$.*

Demostración. Por ser $\ker g$ un submódulo de V y por el Teorema de Maschke, existe un submódulo U de V tal que $V = U \oplus \ker g$. Definimos ahora una aplicación $\hat{g} : U \to \operatorname{im} g, u \mapsto g(u)$, que será un $\mathbb{C}G$-homomorfismo por serlo g. Si $u \in \ker \hat{g}$, entonces $u \in \ker g \cap U = \{0\}$, luego $\ker \hat{g} = \{0\}$. Sea ahora $w \in\in g$, luego $w = g(v)$ para cierto $v \in V$. Escribimos $v = u_0 + u$, con $u_0 \in \ker g$ y $u \in U$. Entonces

$$w = g(v) = g(u_0 + u) = g(u_0) + g(u) = g(u) = \hat{g}(u),$$

y por lo tanto $\operatorname{im} \hat{g} = \operatorname{im} g$. Tenemos así que $\hat{g}$ es un $\mathbb{C}G$-isomorfismo; es decir, $U \cong \operatorname{im} g$. □

Lema II.2.5 (Lema de Schur)**.** *Sean G un grupo finito, F un cuerpo, y V y W dos FG-módulos irreducibles. Sea $f : V \to W$ un FG-homomorfismo. Entonces:*

- *$V \cong W$ o $\ker f = V$.*
- *Si $V = W$, entonces para todo $v \in V$, $f(v) = zv$ para algún $z \in \mathbb{C}$.*

Demostración. Para la primera parte, sean $g \in G$ y $v \in \ker f$. Entonces $g \cdot v \in \ker f$ ya que $f(g \cdot v) = g \cdot f(v) = 0$. Por lo tanto $\ker f$ es un subespacio G-estable de V, luego es un submódulo suyo. Como V es irreducible entonces o bien $\ker f = \{0\}$ o bien $\ker f = V$. Por otro lado $\operatorname{im} f$ es un submódulo de W, y como W es irreducible entonces o bien $\operatorname{im} f = \{0\}$ o bien $\operatorname{im} f = W$. Esto implica que o los dos FG-módulos son isomorfos o que la aplicación f es nula.
Para la segunda parte veamos f como una aplicación F-lineal entre los espacios vectoriales V y W, y fijando bases B_V y B_W en V y W, respectivamente, denotamos por A a la matriz de f respecto dichas bases. Sea $g(\mathtt{t}) = \det(A - \mathtt{t}I)$ su polinomio característico. Por ser $\mathbb{C}$ algebraicamente cerrado el polinomio g tendrá al menos una raíz en $\mathbb{C}$; es decir, existe $z \in \mathbb{C}$ tal que $\det(A - zI) = 0$ y por lo tanto $\ker(f - z \cdot \mathrm{id}_V) \neq 0$. Por el apartado anterior tenemos que $\ker(f - z \cdot \mathrm{id}_V) = V$, luego $f = z \cdot \mathrm{id}_V$. □

Corolario II.2.6. *Sean G un grupo finito, V un $\mathbb{C}G$-módulo irreducible y $z \in Z(\mathbb{C}G)$. Entonces existe $\lambda \in \mathbb{C}$ tal que $z \cdot v = \lambda v$, para cualquier $v \in V$.*

Demostración. Sean $r \in \mathbb{C}G$ y $v \in V$. Entonces $(rz) \cdot v = (zr) \cdot v$, luego la función $v \mapsto z \cdot v$ es un $\mathbb{C}G$-automorfismo de V. Por el Lema de Schur este automorfismo es de la forma $\lambda \,\mathrm{id}_V$ para algún $\lambda \in \mathbb{C}$. □

Teorema II.2.7 (Teorema de descomposición)**.** *Sean G un grupo finito, F un cuerpo cuya característica no divide al orden de G, y V un FG-módulo libre de rango finito. Entonces V es completamente reducible.*

Demostración. Que V sea un FG-módulo libre de rango finito es equivalente a que V tenga dimensión finita como F-espacio vectorial. Si la dimensión de V es 1 entonces es irreducible y por lo tanto es completamente reducible pues $V = V \oplus 0$. Supongamos que

el resultado es cierto para dimensiones menores que cierto natural n. Sea ahora V de dimensión n. Si V es irreducible entonces es completamente irreducible. En caso contario existirá un submódulo propio suyo U, y por el Teorema de Maschke existe un submódulo W de V tal que $V = U \oplus W$, donde las dimensiones de U y W han de ser estrictamente menores que n. Por la hipótesis de inducción, tanto U como W son completamente reducibles, luego V lo es. □

Corolario II.2.8. *Sean G un grupo finito, F un cuerpo cuya característica no divide al orden de G, V un F-espacio vectorial, y $\rho : G \to \mathrm{GL}(V)$ una representación de grado finito. Entonces existe una base de V tal que para cada $g \in G$ la matriz de $\rho(g)$ con respecto a esta base es diagonal por bloques*

$$\begin{pmatrix} \rho_1(g) & & \\ & \ddots & \\ & & \rho_m(g) \end{pmatrix},$$

donde cada $\rho_i(g)$ es la matriz de una representación irreducible de G.

Demostración. Por el teorema anterior existe una familia $\{U_i\}_{i=1}^m$ de FG-submódulos irreducibles de V, tales que $V = U_1 \oplus \cdots \oplus U_m$. Tomamos $B = \bigcup_{i=1}^m B_i$, que base de V, donde cada B_i es una base de U_i. Entonces, para cada $g \in G$, la matriz de $\rho(g)$ respecto de la base V será de la forma del enunciado, donde cada $\rho_i(g)$ es la matriz de $\rho(g)|_{U_i}$ respecto de la base B_i. □

Proposición II.2.9. *Sean G un grupo finito, F un cuerpo y V un FG-módulo. Escribimos*

$$V = U_1 \oplus \cdots \oplus U_r,$$

donde cada U_i es un FG-submódulo irreducible de V. Si U es un FG-submódulo irreducible de V, entonces $U \cong U_i$ para algún $1 \leq i \leq r$.

Demostración. Dado $u \in U \subset V$ no nulo, tenemos que $u = u_1 + \cdots + u_r$, con $u_i \in U_i$ para todo $1 \leq i \leq r$, y algún i tal que $u_i \neq 0$. Definimos el FG-homomorfismo $\pi_i : U \to U_i, u \mapsto u_i$. Como U y U_i son ambos irreducibles y $\pi_i \neq 0$ entonces por el Lema de Schur (Lema II.2.4), tenemos que $U \cong U_i$. □

El resultado anterior es de suma importancia, pues nos garantiza que para todo FG-módulo existen una cantidad finita de submódulos suyos irreducibles. De hecho dado un FG-módulo V, deben existir $V_1, \ldots, V_k$, FG-módulos irreducibles no isomorfos y enteros no negativos $a_1, \ldots, a_k$, tal que $V \cong \bigoplus_{i=1}^k V_i^{\oplus a_i}$. A esta descomposición la denominaremos *descomposición canónica*. Nótese que los coeficientes a_i dependen de V, pero la familia $\{V_i\}_{i=1}^k$ no, así que lo que diferencia las representaciones canónicas de dos FG-módulos son los coeficientes a_i de cada una.

Ejemplo II.2.10. Sea $\mathfrak{S}_3$ el grupo de permutaciones de 3 elementos. Sabemos que la representación trivial U en $\mathbb{C}$ es irreducible de dimensión 1. La *representación alternante* es la inducida por el $\mathbb{C}$-espacio vectorial de dimensión 1 $U' = \mathbb{C}$ con la acción del grupo

$g \cdot u :=\text{sgn}(g)u$ para cualesquiera $g \in \mathfrak{S}_3$, $u \in U'$, donde $\text{sgn}(g)$ es 1 si g es una permutación par y -1 si es impar. Por tener dimensión 1 también es trivialmente irreducible.

Consideramos el $\mathbb{C}$-espacio vectorial $\mathbb{C}^3$, que será de dimensión 3, y la acción del grupo $\mathfrak{S}_3$ siguiente:

$$\sigma \cdot (z_1, z_2, z_3) := (z_{\sigma^{-1}(1)}, z_{\sigma^{-1}(2)}, z_{\sigma^{-1}(3)}).$$

Esta acción sobre $\mathbb{C}^3$ induce la denominada *representación por permutaciones* de $\mathfrak{S}_3$, que no es irreducible pues el subespacio $W := L[(1,1,1)]$ es $\mathfrak{S}_3$-estable, y por lo tanto es un $\mathbb{C}\mathfrak{S}_3$-submódulo. Sea V el subespacio de $\mathbb{C}^3$ de dimensión 2 siguiente:

$$V := \{(z_1, z_2, z_3) \in \mathbb{C}^3 : z_1 + z_2 + z_3 = 0\},$$

que es claramente $\mathfrak{S}_3$-estable, y por lo tanto un $\mathbb{C}\mathfrak{S}_3$-submódulo. Además, nótese que $V \cap W = \{0\}$, y que $\dim \mathbb{C}^3 = \dim V + \dim W$, luego $\mathbb{C}^3 = V \oplus W$. De hecho, por el Lema de Schur, W y U son isomorfos. Más adelante veremos que las únicas representaciones irreducibles de $\mathfrak{S}_3$ son las inducidas por los $\mathbb{C}\mathfrak{S}_3$-módulos U, U', V.

Definición II.2.11. Sean G un grupo finito y F el cuerpo $\mathbb{R}$ ó $\mathbb{C}$. El espacio vectorial FG, con la acción natural multiplicativa $g \cdot v = gv$ para $v \in FG$ y $g \in G$, se denomina FG-módulo *regular*.

Observación II.2.12. La representación que induce el FG-módulo regular se denomina *representación regular*. Es inmediato ver que dicha representación es fiel y su grado coincide con el orden del grupo G.

Teorema II.2.13. *Sea G un grupo finito, y denotemos por $\mathbb{C}G$ al $\mathbb{C}G$-módulo regular, y escribamos*

$$\mathbb{C}G = U_1 \oplus \cdots \oplus U_r,$$

donde cada U_i es un submódulo irreducible de $\mathbb{C}G$. Entonces todo $\mathbb{C}G$-módulo irreducible es isomorfo a alguno de los U_i.

Demostración. Sea W un $\mathbb{C}G$-módulo irreducible, y tomamos $w \in W$ no nulo. El conjunto $\{rw : r \in \mathbb{C}G\}$ es un submódulo de W, y por ser W irreducible, $W = \{rw : r \in \mathbb{C}G\}$. Sea $f : \mathbb{C}G \to W, r \to rw$, que será un $\mathbb{C}G$-homomorfismo sobreyectivo. Por el Corolario II.2.4, $\mathbb{C}G$ se puede descomponer como suma directa de un $\mathbb{C}G$-módulo U con $\ker f$, donde $U \cong W$. Como W es irreducible, entonces U lo es, y por la Proposición II.2.8, $U \cong U_i$ para cierto $1 \leq i \leq r$. □

Definición II.2.14. Sean G un grupo finito y V y W dos $\mathbb{C}G$-módulos. Denotamos por $\text{Hom}_{\mathbb{C}G}(V, W)$ al conjunto de $\mathbb{C}G$-homomorfismos de V en W, que no es más que el espacio vectorial de aplicaciones lineales de V en W como $\mathbb{C}$-espacios vectoriales que, además, son G-lineales.

Como consecuencia del Lema de Schur tenemos el siguiente resultado.

Lema II.2.15. *Sean V y W dos $\mathbb{C}G$-módulos irreducibles. Entonces* $\dim(\text{Hom}_{\mathbb{C}G}(V, W))$ *es* 1 *si $V \cong W$, y* 0 *en caso contrario.*

Demostración. Si $V \ncong W$ el único $\mathbb{C}G$-homomorfismo entre ambos espacios es el nulo, luego se tiene que $\dim(\mathrm{Hom}_{\mathbb{C}G}(V,W)) = 0$. Supongamos ahora $V \cong W$, y tomamos $f \in \mathrm{Hom}_{\mathbb{C}G}(V,W)$ que sea isomorfismo. Si $g \in \mathrm{Hom}_{\mathbb{C}G}(V,W)$, entonces $f^{-1} \circ g$ es un $\mathbb{C}G$-isomorfismo de V en V, luego por el Lema de Schur, existe $z \in \mathbb{C}$ tal que $f^{-1} \circ g = z\,\mathrm{id}_V$, y por lo tanto $g = zf$, y $\mathrm{Hom}_{\mathbb{C}G}(V,W) = \{zf : z \in \mathbb{C}\}$ es un $\mathbb{C}$-espacio vectorial de dimensión 1. □

Por el Teorema II.2.13, sabemos que todo $\mathbb{C}G$-módulo irreducible es isomorfo a uno de los submódulos irreducibles del $\mathbb{C}G$-módulo regular, que forman una familia finita salvo isomorfismo. Nuestro objetivo será saber, dado un $\mathbb{C}G$-módulo irreducible U, cuántos de los constituyentes de $\mathbb{C}G$ son isomorfos a U. La clave es la siguiente proposición.

Proposición II.2.16. *Sea G un grupo finito, y sean V, V_1, V_2, W, W_1 y W_2 $\mathbb{C}G$-módulos. Entonces*

- $\dim(\mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2)) = \dim(\mathrm{Hom}_{\mathbb{C}G}(V, W_1)) + \dim(\mathrm{Hom}_{\mathbb{C}G}(V, W_2))$,
- $\dim(\mathrm{Hom}_{\mathbb{C}G}(V_1 \oplus V_2, W)) = \dim(\mathrm{Hom}_{\mathbb{C}G}(V_1, W)) + \dim(\mathrm{Hom}_{\mathbb{C}G}(V_2, W))$.

Demostración.

1. Sean $\pi_i : W_1 \oplus W_2 \to W_i$ para $i = 1, 2$ donde $\pi_1(w_1 + w_2) = w_1$ y $\pi_2(w_1 + w_2) = w_2$, para todo $w_1 \in W_1$, $w_2 \in W_2$. Definimos $f : \mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2) \to \mathrm{Hom}_{\mathbb{C}G}(V, W_1) \oplus \mathrm{Hom}_{\mathbb{C}G}(V, W_2), g \mapsto (\pi_1 \circ g, \pi_2 \circ g)$. Claramente f es una aplicación lineal, resta ver que es isomorfismo. Dado $h_i \in \mathrm{Hom}_{\mathbb{C}G}(V, W_i)$ para $i = 1, 2$, entonces la función $g(v) = h_1(v) + h_2(v)$ para $v \in V$, es un elemento de $\mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2)$, y su imagen por f es (h_1, h_2), luego f es sobreyectiva. Si $g \in \ker f$, entonces $\pi_i(g(v)) = 0$ para todo $v \in V$, $i = 1, 2$, luego $g(v) = (\pi_1 + \pi_2)(g(v)) = 0$ para todo $v \in V$ y por lo tanto $g = 0$; es decir, f es inyectiva y por lo tanto un isomorfismo.

2. Dado $f \in \mathrm{Hom}_{\mathbb{C}G}(V_1 \oplus V_2, W)$, definimos $f_i : V_i \to W$ como la restricción de f a V_i, $i = 1, 2$. Como todo $v \in V_1 \oplus V_2$ se escribe de forma única como $v_1 + v_2$ con $v_1 \in V_1, v_2 \in V_2$, entonces $f_i(v_i) = f(v_i)$, luego $f_i \in \mathrm{Hom}_{\mathbb{C}G}(V_i, W)$ para $i = 1, 2$. Sea la función $g : \mathrm{Hom}_{\mathbb{C}G}(V_1 \oplus V_2, W) \to \mathrm{Hom}_{\mathbb{C}G}(V_1, W) \oplus \mathrm{Hom}_{\mathbb{C}G}(V_2, W), h \mapsto (h_1, h_2)$. Claramente g es una aplicación lineal inyectiva. Dadas $h_i \in \mathrm{Hom}_{\mathbb{C}G}(V_i, W)$ para $i = 1, 2$, entonces la función $h(v_1 + v_2) = h_1(v_1) + h_2(v_2)$ para $v_i \in V_i$, $i = 1, 2$, es un elemento de $\mathrm{Hom}_{\mathbb{C}G}(V_1 \oplus V_2, W)$, y su imagen por g es (h_1, h_2); es decir, g es sobreyectiva y por lo tanto isomorfismo. □

Observación II.2.17. Mediante inducció, el resultado anterior se extiende a sumas directas finitas de $\mathbb{C}G$-módulos.

Corolario II.2.18. *Sean G un grupo finito y V un $\mathbb{C}G$-módulo con*

$$V = U_1 \oplus \cdots \oplus U_r,$$

donde cada U_i es un $\mathbb{C}G$-submódulo irreducible de V. Sea W un $\mathbb{C}G$-módulo irreducible. Entonces las dimensiones de $\mathrm{Hom}_{\mathbb{C}G}(V, W)$ y $\mathrm{Hom}_{\mathbb{C}G}(W, V)$ son ambas iguales al número de $\mathbb{C}G$-submódulos U_i tales que $U_i \cong W$.

Demostración. Por la Proposición II.2.16,

1. $\dim(\mathrm{Hom}_{\mathbb{C}G}(V,W)) = \sum_{i=1}^{r} \mathrm{Hom}_{\mathbb{C}G}(U_i,W)$ y
2. $\dim(\mathrm{Hom}_{\mathbb{C}G}(W,V)) = \sum_{i=1}^{r} \mathrm{Hom}_{\mathbb{C}G}(W,U_i)$,

y por el Lema II.2.15, $\dim(\mathrm{Hom}_{\mathbb{C}G}(U_i,W) = \dim(\mathrm{Hom}_{\mathbb{C}G}(W,U_i)) = 1$ si $U_i \cong W$, y $\dim(\mathrm{Hom}_{\mathbb{C}G}(U_i,W) = \dim(\mathrm{Hom}_{\mathbb{C}G}(W,U_i)) = 0$ en caso contrario. □

Proposición II.2.19. *Sea G un grupo finito. Si U es un $\mathbb{C}G$-módulo irreducible, entonces* $\dim(\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G,U)) = \dim U$.

Demostración. Sean $d := \dim U$ y 1 la identidad de $\mathbb{C}G$. Sea $\{u_1,\dots,u_d\}$ una base de U. Para $1 \le i \le d$, definimos $f_i : \mathbb{C}G \to U, r \mapsto r \cdot u$. Entonces $f_i \in \mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G,U)$. Vamos a probar que $\{f_1,\dots,f_d\}$ forman una base de $\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G,U)$. Sea $g \in \mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G,U)$. Entonces $g(1) = c_1u_1 + \cdots + c_du_d$, para ciertos $c_i \in \mathbb{C}$. Como g es un $\mathbb{C}G$-homomorfismo, tenemos que para todo $r \in \mathbb{C}G$,

$$g(r) = g(r\cdot 1) = rg(1) = rc_1u_1 + \cdots + rc_du_d = c_1(r\cdot u_1) + \cdots + c_d(r\cdot u_d) = \sum_{i=1}^{d} c_if_i(r).$$

Por lo tanto $g = \sum_{i=1}^{d} c_if_i$, y tenemos que $\{f_1,\dots,f_d\}$ es un conjutno generador de $\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G,U)$. Supongamos ahora que $c_1f_1+\cdots+c_df_d = 0$ para ciertos $c_i \in \mathbb{C}$. Evaluando en 1 tenemos que $c_1u_1+\cdots+c_du_d = 0$, lo que implica que todos los $c_i = 0$. Así $\{f_1,\dots,f_d\}$ es base de $\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G,U)$. □

Corolario II.2.20. *Sea G un grupo finito. Supongamos que $\mathbb{C}G = U_1 \oplus \cdots \oplus U_r$, donde cada U_i es un $\mathbb{C}G$-submódulo de $\mathbb{C}G$ irreducible. Si U es un $\mathbb{C}G$-módulo irreducible, entonces el número de los U_i isomorfos a U es igual a la dimensión de U.*

Demostración. Se sigue inmediantamente del Corolario II.2.18 y la Proposición II.2.19. □

CAPÍTULO III

Teoría de caracteres

Desarrollamos a continuación los conceptos básicos de la teoría de caracteres, que es la clave de la demostración del Teorema de Burnside. El caracter será un concepto que recogerá de forma muy condensada la información clave de la representación de un grupo. De hecho, en los inicios de la teoría de representación de grupos finitos, esta se basó enteramente en la teoría de caracteres, sin una representación matricial explícita de la representación. Esto es posible, como veremos, debido a que la representación compleja de un grupo finito queda determinada salvo isomorfismo por su caracter.

III.1. Caracteres

Definición III.1.1. Sean G un grupo finito y F un cuerpo. Una función $f : G \to F$ se dice que es una *función de clase* si es constante en las clases de conjugación de G; es decir, $f(ghg^{-1}) = f(h)$ para cualesquiera $g, h \in G$.

Definición III.1.2. Sean G un grupo finito y $\rho : G \to \mathrm{GL}(V)$ una representación de G sobre un F-espacio vectorial V. El *caracter* de ρ, que denotaremos por χ_ρ, es la función $\chi_\rho : G \to \mathbb{C}, g \mapsto \chi_\rho(g) = \mathrm{tr}(\rho(g))$. Diremos que el caracter es *irreducible* si es el caracter de una representación irreducible.

Observaciones III.1.3.

1. Nuestra definición de caracter parece algo ambigua en el sentido de que aparentemente su valor dependerá de la base escogida en V al dar la representación (o equivalentemente que depende de la representación escogida). Vamos a comprobar que nuestra definición es en efecto adecuada. Un resultado clásico de álgebra lineal es que dadas dos matrices cuadradas del mismo orden A, B, entonces $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. De aquí se deduce que si A es invertible entonces

$$\mathrm{tr}(A^{-1}BA) = \mathrm{tr}(A^{-1}AB) = \mathrm{tr}\, B.$$

   Por tanto, dadas dos representaciones ϕ, ψ y su matriz de cambio de base P, tenemos que

$$\mathrm{tr}(\psi(g)) = \mathrm{tr}(P\phi(g)P^{-1}) = \mathrm{tr}(\phi(g)),$$

   para todo $g \in G$, luego representaciones equivalentes tienen el mismo caracter. De hecho, por el mismo motivo, son funciones de clase.

2. Como la traza de la matriz identidad $n \times n$ es n y el elemento neutro e de G, actúa trivialmente sobre los elementos de V, tenemos que $\chi_\rho(e) = \dim V$.

3. Si consideramos la descomposición canónica de un FG-módulo V, $\bigoplus_{i=1}^{k} V_i^{\oplus a_i}$, y denotamos por χ_i al caracter de la representación inducida por V_i, tenemos que el caracter χ de la representación inducida por V se escribe de forma única como $\chi = \sum_{i=1}^{k} a_i \chi_i$. Si $V = \mathbb{C}G$, entonces a los $\chi_1, \ldots, \chi_k$ se les denomina *caracteres irreducibles* de G. Así, toda representación viene determinada de forma unívoca por su caracter.

El siguiente resultado será crucial en la demostración del Teorema de Burnside.

Proposición III.1.4. *Sea ρ una representación de un grupo finito G en V.*

- *Para todo $g \in G$, $\chi_\rho(g)$ es suma de $\chi_\rho(e)$ raíces k-ésimas de la unidad, donde $k :=$ ord(g) y e es el elemento neutro de G.*
- *$|\chi_\rho(g)| \leq \chi_\rho(e)$, para todo $g \in G$.*
- *$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.*

Demostración.

1. Como $g^k = e$ y ρ es un homomorfismo de grupos, entonces si $M := \rho(g)$ tenemos que $M^k = \rho(g)^k = \rho(g^k) = \rho(e) = I$. De esto deducimos que el polinomio mínimo de M divide a $\mathtt{t}^k - 1$, luego los autovalores de M son raíces k-ésimas de la unidad. Tomando una base de V respecto de la que la matriz de $\rho(g)$ sea su forma de Jordan J, los elementos en la diagonal principal de J son los autovalores de $\rho(g)$; esto es, raíces k-ésimas de la unidad, y tenemos el resultado.

2. Por el apartado anterior tenemos que dado $g \in G$ existen $\zeta_1, \ldots, \zeta_{\chi_\rho(e)}$ raíces ord(g)-ésimas de la unidad tales que

$$\chi_\rho(g) = \zeta_1 + \cdots + \zeta_{\chi_\rho(e)}.$$

   Tomando módulos tenemos que, por la desigualdad triangular,

$$|\chi_\rho(g)| \leq |\zeta_1| + \cdots + |\zeta_{\chi_\rho(e)}| = \chi_\rho(e).$$

3. Sabemos que si A es una matriz invertible con autovalores $\{\lambda_i\}$, entonces los autovalores de A^{-1} son $\{\lambda_i^{-1}\}$. Por lo tanto si los autovalores son las raíces de la unidad $\{\zeta_i\}$, entonces los autovalores de su inversa son $\{\zeta_i^{-1}\}$, y por ser raíces de la unidad sus inversos coinciden con sus conjugados. Por tanto tenemos que

$$\chi_\rho(g^{-1}) = \overline{\zeta_1} + \cdots + \overline{\zeta_{\chi_\rho(e)}} = \overline{\zeta_1 + \cdots + \zeta_{\chi_\rho(e)}} = \overline{\chi_\rho(g)}.$$

Teorema III.1.5. *Sean G un grupo finito con elemento neutro e_G y $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ una representación matricial de G. Sea χ el caracter de ρ. Entonces:*

- *Para todo $g \in G$, $|\chi(g)| = \chi(e_G) \iff \rho(g) = zI_n$, para algún $z \in \mathbb{C}$.*
- *$\ker \rho = \{g \in G : \chi(g) = \chi(e_G)\}$.*

Demostración.

- Sea $g \in G$ tal que $\mathrm{ord}(g) = m$. Si $\rho(g) = zI_n$ con $z \in \mathbb{C}$, entonces como $I_n = \rho(e_G) = \rho(g^m) = \rho(g)^m = z^m I_n$, entonces z es una raíz m-ésima de la unidad. Como $\chi(g) = \mathrm{tr}(zI) = nz$, entonces $|\chi(g)| = n = \chi(e_G)$. Recíprocamente supongamos que $|\chi(g)| = \chi(e_G)$. Por la Proposición III.1.4 $\chi(g) = \zeta_1 + \cdots + \zeta_n$, donde cada ζ_i es una raíz m-ésima de la unidad. Entonces $|\chi(g)| = |\zeta_1 + \cdots + \zeta_n| = \chi(e_G) = n$. Recordemos que para cualesquiera $z_1, \ldots, z_n \in \mathbb{C}$ se tiene que $|z_1 + \cdots + z_n| \leq |z_1| + \cdots + |z_n|$, dándose la igualdad únicamente si todos los z_i son iguales. Como $|\zeta_i| = 1$ para todo $1 \leq i \leq n$, se deduce que $\zeta_i = \zeta_j$ para cualesquiera $1 \leq i, j \leq n$. Tomando $z := \zeta_1$ se tiene el resultado.
- Si $g \in \ker \rho$, entonces $\rho(g) = I_n$, luego $\chi(g) = n = \chi(e_G)$. Recíprocamente si $\chi(g) = \chi(e_G)$, entonces por lo anterior $\rho(g) = zI_n$ para algún $z \in \mathbb{C}$. Esto implica que $\chi(g) = z\chi(e_G)$, luego $z = 1$. Por lo tanto $\rho(g) = I_n$, lo que implica que $g \in \ker \rho$.

□

Lema III.1.6. *Sean G un grupo finito con elemento neutro e_G, $g \in G$ y O_g la clase de conjugación de g. Sea U un $\mathbb{C}G$-módulo irreducible, y sea χ el caracter de su representación asociada. Entonces $\overline{O_g} \cdot u = \lambda u$ para todo $u \in U$, donde*

$$\lambda = \frac{|G|\chi(g)}{|C_G(g)|\chi(e_G)}.$$

Demostración. Como $\overline{O_g}$ pertenece al centro de $\mathbb{C}G$, entonces por el Corolario II.2.6, existe $\lambda \in \mathbb{C}$ tal que $\overline{O_g} \cdot u = \lambda u$ para cualquier $u \in U$; es decir,

$$\left(\sum_{x \in O_g} x \right) \cdot u = \lambda u.$$

Sea ρ la representación de G asociada a U. Si fijamos una base B de U, para cada $g \in G$, podemos ver $\rho(g)$ como una matriz con coeficientes complejos. Se sigue de lo anterior que $\sum_{x \in O_g} \rho(x) = \lambda I$. Tomando trazas tenemos que $\sum_{x \in O_g} \chi(x) = \lambda\chi(e_G)$, y como χ es constante en cada clase de conjugación de G obtenemos que $|O_g|\chi(g) = \lambda\chi(e_G)$. Como $|O_g| = |G : C_G(g)|$, despejando λ se obtiene el resultado buscado. □

Proposición III.1.7. *Sean ϕ, ψ dos representaciones de G en V y W, respectivamente, y $g \in G$. Entonces:*

- $\chi_{\phi \bigoplus \psi}(g) = \chi_\phi(g) + \chi_\psi(g)$,
- $\chi_{\phi \bigotimes \psi}(g) = \chi_\phi(g)\chi_\psi(g)$,
- $\chi_{\phi^*}(g) = \overline{\chi_\phi(g)}$,

donde $V \oplus W$ y $V \otimes W$ denotan la suma directa y producto tensorial como FG-módulos, respectivamente.

Demostración.

1. Como ya vimos la representación de la suma directa de representaciones viene dada matricialmente por la matriz por bloques diagonal con entradas $\phi(g)$ y $\psi(g)$ para todo $g \in G$. Por lo tanto su caracter vendrá dado por la traza de esta matriz, que no es más que la suma de las trazas de las representaciones ϕ y ψ; es decir, la suma de $\chi_\phi(g)$ y $\chi_\psi(g)$.

2. Como ya vimos la representación matricial del producto tensorial viene dado por el producto de Kronecker de las representaciones de ϕ y ψ. Fijado $g \in G$, entonces la traza de $\phi(g) \otimes \psi(g)$ será

$$\mathrm{tr}(\phi(g) \otimes \psi(g)) = \sum_{i=1}^{n} \phi(g)_{ii} \cdot \mathrm{tr}(\psi(g)) = \mathrm{tr}(\phi(g)) \cdot \mathrm{tr}(\psi(g)).$$

   Por tanto el caracter del producto tensorial de representaciones es el producto de los caracteres de dichas representaciones.

3. $\chi_{\phi^*}(g) = \mathrm{tr}(\phi^*(g)) = \mathrm{tr}(\phi(g^{-1})^t) = \mathrm{tr}(\phi(g^{-1})) = \chi_\phi(g^{-1}) = \overline{\chi_\phi(g)}$ □

Definición III.1.8 (Tabla de caracteres)**.** Sean $\chi_1, \ldots, \chi_k$ los caracteres irreducibles de G, y sean $g_1, \ldots, g_r$ unos representantes de las clases de conjugación de G. La matriz de orden $k \times r$ cuya ij-ésima entrada es $\chi_i(g_j)$, para todo i, j con $1 \leq i \leq k$, $1 \leq j \leq r$, se llama *tabla de caracteres* de G. Encima de la matriz se dispone una fila con las clases de conjugación de G y el número de elementos que hay en cada una.

Ejemplo III.1.9**.** Retomamos el ejemplo II.2.6 con las mismas notaciones, y trabajaremos durante el ejemplo con la bases canónicas $\{1\}$ en el caso de $\mathbb{C}$ y $\{(1,0,0),(0,1,0),(0,0,1)\}$ en el caso de $\mathbb{C}^3$. La representación trivial asocia cada elemento del grupo con la matriz identidad de orden 1×1, luego el caracter de dicha representación es igual a 1 constantemente en cada elemento del grupo. Sean I la representación trivial, A la representación alternante, inducida por el espacio U', P la representación alternante inducida por $\mathbb{C}^3 = U \oplus V$, y P' la representación inducida por el espacio V. Como $\dim U' = 1$ y $\dim V = 2$, entonces si identificamos al elemento neutro de $\mathfrak{S}_3$ con la permutación id, tenemos que $\chi_A(\mathrm{id}) = 1$ y $\chi_{P'}(\mathrm{id}) = 2$. Como (12) y (123) son permutaciones impar y par, respectivamente, tenemos que $\chi_A((12)) = -1$ y $\chi_A((123)) = 1$. La matriz de $P((12))$ es de la forma

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

luego $\chi_P((12)) = 1$. De manera similar la matriz de $P(123)$ será

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

y por lo tanto $\chi_P((123)) = 0$. Como $\mathbb{C}^3 = U \oplus V$, tenemos que $\chi_{P'}((12)) = \chi_P((12)) - \chi_I((12)) = 1 - 1 = 0$, y que $\chi_{P'}((123)) = \chi_P((123)) - \chi_I((123)) = 0 - 1 = -1$. Luego la

tabla de caracteres de $\mathfrak{S}_3$ queda como

$\mathfrak{S}_3$	id[1]	(12)[3]	(123)[2]
I	1	1	1
A	1	-1	1
P'	2	0	-1

III.2. Relaciones de ortogonalidad.

El conjunto de funciones de clase entre un grupo finito G y un cuerpo F forma un F-espacio vectorial. Vamos a ver qué lo podemos dotar de un producto interno, que en el caso de que el cuerpo F sea $\mathbb{C}$ será hermítico.

Definición III.2.1. Sea V un $\mathbb{C}$-espacio vectorial. Un *producto interno hermítico* es una aplicación $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$, que cumple lo siguiente para cualesquiera $x, y, z \in V$, $a, b \in \mathbb{C}$:

1. $\langle x, y \rangle = \overline{\langle y, x \rangle}$,
2. $\langle ax + by, z \rangle = a\langle x, z \rangle + b\langle y, z \rangle$,
3. $\langle x, ay + bz \rangle = \overline{a}\langle x, y \rangle + \overline{b}\langle x, z \rangle$,
4. Si $x \neq 0$, entonces $\langle x, x \rangle > 0$.

Definición III.2.2. Sea G un grupo finito. Denotamos por $C_{\mathbb{C}}(G)$ al conjunto de funciones de clase de un grupo finito G a valores en $\mathbb{C}$. El conjunto $C_{\mathbb{C}}(G)$ es un subespacio del espacio vectorial de funciones de G en $\mathbb{C}$, y una base vendrá dada por aquellas funciones que toman el valor 1 en una clase de conjugación y cero en el resto de clases de conjugación de G. Luego si G tiene r clases de conjugación, $\dim C_{\mathbb{C}}(G) = r$.

Definición III.2.3. Dados $f, g \in C_{\mathbb{C}}(G)$ definimos el producto

$$\langle f, g \rangle := \frac{1}{\mathrm{ord}(G)} \sum_{h \in G} f(h)\overline{g(h)}.$$

Es rutinario comprobar que se trata de un producto interno hermítico.

Como sabemos que el caracter de una representación es una función de clase tenemos un producto interno de caracteres asociados a representaciones de un grupo finito G. Por la Proposición III.1.4 la expresión del producto interno queda como

$$\langle \chi_\rho, \chi_\psi \rangle = \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} \chi_\rho(g)\chi_\psi(g^{-1}),$$

donde ρ y ψ son dos representaciones de G. De la Proposición III.1.4, usando el hecho de que $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$, y que $G = \{g^{-1} : g \in G\}$, se deduce que $\langle \chi_\rho, \chi_\psi \rangle = \langle \chi_\psi, \chi_\rho \rangle$, luego en particular es un número real. A partir de ahora denotaremos caracteres asociados a representaciones de G sin especificar la representación para no recargar la notación.

Proposición III.2.4. *Sea G un grupo finito con r clases de conjugación, y sea $R = \{g_1, \dots, g_r\}$ un conjunto de representantes. Sean χ y ψ dos caracteres asociados a dos representaciones de G. Entonces se cumple que*

$$\langle \chi, \psi \rangle = \sum_{i=1}^{r} \frac{\chi(g_i)\psi(g_i^{-1})}{\mathrm{ord}(C_G(g_i))}.$$

Demostración. Sea O_{g_i} la clase de conjugación de g_i. Por ser los caracteres funciones de clase son constantes en las clases de conjugación, luego

$$\sum_{g \in O_{g_i}} \chi(g)\psi(g^{-1}) = |O_{g_i}|\chi(g_i)\psi(g_i^{-1}).$$

Ahora como G es la unión disjunta de las clases de conjugación de los elementos de R, y $|O_{g_i}| = \frac{|G|}{|C_G(g_i)|}$, tenemos que

$$\begin{aligned}\langle \chi, \psi \rangle &= \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} \chi(g)\psi(g^{-1}) = \frac{1}{\mathrm{ord}(G)} \sum_{i=1}^{r} \sum_{g \in O_{g_i}} \chi(g)\psi(g^{-1}) \\ &= \sum_{i=1}^{r} \frac{|O_{g_i}|}{|G|} \chi(g_i)\psi(g_i^{-1}) = \sum_{i=1}^{r} \frac{\chi(g_i)\psi(g_i^{-1})}{\mathrm{ord}(C_G(g_i))}.\end{aligned}$$

□

Definición III.2.5. Sean G un grupo finito, F un cuerpo y V un FG-módulo. Definimos el conjunto $V^G := \{v \in V : g \cdot v = v, \forall g \in G\}$.

Lema III.2.6. *Sean G un grupo finito y V y W dos $\mathbb{C}G$-módulos. Entonces* $\mathrm{Hom}_{\mathbb{C}G}(V, W) = \mathrm{Hom}(V, W)^G$.

Demostración. Sean $f \in \mathrm{Hom}_{\mathbb{C}G}(V, W)$ y $g \in G$. Por ser f G-lineal, se tiene que para todo $v \in V$, $g \cdot f(v) = gf(g^{-1}v) = f((gg^{-1})v) = f(v)$, luego $f \in \mathrm{Hom}(V, W)^G$. Recíprocamente, sean $f \in \mathrm{Hom}(V, W)^G$ y $g \in G$. Como f queda fijo por la acción de g, se tiene que dado $v \in V$, $gf(v) = gf((g^{-1}g)v) = gf(g^{-1}(gv)) = g \cdot f(gv) = f(gv)$, luego $f \in \mathrm{Hom}_{\mathbb{C}G}(V, W)$. □

Teorema III.2.7 (Ortonormalidad de caracteres)**.** *Sean G un grupo finito, V y W dos $\mathbb{C}G$-módulos irreducibles y χ y ψ los caracteres de sus representaciones asociadas. Entonces $\langle \chi, \psi \rangle = 1$ si $V \cong W$ y $\langle \chi, \psi \rangle = 0$ en caso contrario.*

Demostración. Definimos $p : V \to V^G, v \mapsto \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} g \cdot v$. Por las propiedades de los módulos, p es lineal. De hecho dado $h \in G$,

$$p(h \cdot v) = \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} g \cdot (h \cdot v) = \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} (hgh^{-1}) \cdot (h \cdot v) = h \cdot \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} g \cdot v = h \cdot p(v),$$

pues si g recorre G, entonces hgh^{-1} también lo hace. Luego p es G-lineal. Ahora, dado $w \in p(V)$, existe un $v \in V$ tal que $w = p(v)$. Dado ahora $h \in G$, se tiene que

$$h \cdot w = \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} h \cdot (g \cdot v) = \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} (hg) \cdot v = \frac{1}{\mathrm{ord}(G)} \sum_{k \in G} k \cdot v = w,$$

donde $k = hg$ también recorre G si g lo hace. Así $p(V) \subset V^G$. Por otro lado, dado $v \in V^G$, $p(v) = \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} g \cdot v = \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} v = v$, luego $p(V) = V^G$. Además,

$$\begin{aligned} p^2(v) = p(p(v)) &= \frac{1}{\mathrm{ord}(G)} \sum_{h\in G} h \cdot \left(\frac{1}{\mathrm{ord}(G)} \sum_{g\in G} g \cdot v \right) \\ &= \frac{1}{\mathrm{ord}(G)} \sum_{h\in G} \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} g \cdot v = \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} g \cdot v = p(v). \end{aligned}$$

Por lo tanto p es una proyección sobreyectiva, y tenemos la siguiente descomposición

$$V = \ker p \oplus V^G,$$

luego de aquí se deduce que $\mathrm{tr}\, p = \dim V^G$.
Por otro lado p se descompone como $p = \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} \phi_g$, donde cada $\phi_g : V \to V, v \mapsto g\cdot v$. En consecuencia, $\mathrm{tr}\, p = \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} \mathrm{tr}\, \phi_g$. Recordemos que la representación inducida por un $\mathbb{C}G$-módulo es el homomorfismo de grupos $\rho : G \to \mathrm{GL}(V), g \mapsto \phi_g$, luego $\mathrm{tr}\, \rho(g) = \chi(g) = \mathrm{tr}\, \phi_g$, y por lo tanto tenemos que

$$\dim V^G = \mathrm{tr}\, p = \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} \mathrm{tr}\, \phi_g = \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} \chi(g).$$

Así,

$$\begin{aligned} \dim(\mathrm{Hom}_{\mathbb{C}G})(V, W)) = \dim(\mathrm{Hom}(V, W)^G) &= \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} \chi_{\mathrm{Hom}(V,W)}(g) \\ &= \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} \chi_{V^*\oplus W}(g) = \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} \chi_{V^*}(g)\chi_W(g) \\ &= \frac{1}{\mathrm{ord}(G)} \sum_{g\in G} \overline{\chi(g)}\psi(g) = \langle \psi, \chi \rangle = \langle \chi, \psi \rangle. \end{aligned}$$

El resultado se sigue del Lema II.2.15. □

Proposición III.2.8. *Sean G un grupo finito y V un $\mathbb{C}G$-módulo. Denotemos por χ al caracter de la representación inducida por V. Entonces V es irreducible si y solo si $\langle \chi, \chi \rangle = 1$.*

Demostración. Si V es irreducible se sigue del resultado anterior. Recíprocamente, supongamos que $\langle \chi, \chi \rangle = 1$. Considerando la descomposición canónica $V = \bigoplus_{i=1}^k V_i^{\oplus a_i}$, tenemos que $\chi = a_1\chi_1 + \cdots + a_k\chi_k$, para ciertos caracteres χ_i y enteros no negativos a_i. Por lo tanto, $1 = \langle \chi, \chi \rangle = \langle a_1\chi_1 + \cdots + a_k\chi_k, a_1\chi_1 + \cdots + a_k\chi_k \rangle = a_1^2 + \cdots + a_k^2$. Necesariamente existe un único $1 \leq i \leq k$ tal que $a_i \neq 0$ y $a_i = 1$; es decir, $V \cong V_i$, luego V es irreducible. □

Proposición III.2.9. *Sean G un grupo finito, y $\chi_1, \ldots, \chi_k$ los caracteres irreducibles de G. Entonces los $\chi_1, \ldots, \chi_k$ son vectores linealmente independientes en el espacio $C_{\mathbb{C}}(G)$.*

Demostración. Supongamos que existen $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ tales que $\lambda_1\chi_1 + \cdots + \lambda_k\chi_k = 0$. Por la relación de ortogonalidad tenemos que $0 = \langle 0, \chi_i \rangle = \langle \lambda_1\chi_1 + \cdots + \lambda_k\chi_k, \chi_i \rangle = \lambda_i$, luego son linealmente independientes. □

Teorema III.2.10. *El número de caracteres irreducibles de un grupo finito G es igual al número de clases de conjugación que tiene G.*

Demostración. Sean $\chi_1, \dots, \chi_k$ los caracteres irreducibles de G, y sea r el número de clases de conjugación de G. Por el resultado anterior $\chi_1, \dots, \chi_k$ es un conjunto linealmente independiente de $C_{\mathbb{C}}(G)$, luego $k \leq r$. Consideramos la descomposición canónica de $\mathbb{C}G$ en la forma $\mathbb{C}G = W_1 \oplus \cdots \oplus W_k$, donde cada $W_i = V_i^{\oplus a_i}$ para una familia $\{V_i\}_{i=1}^k$ de $\mathbb{C}G$-submódulos irreducibles no isomorfos dos a dos. Escribimos $1 = w_1 + \cdots + w_k$, con cada $w_i \in W_i$. Sea ahora $z \in Z(\mathbb{C}G)$. Por el Corolario II.2.6, para cada i existe un $\lambda_i \in \mathbb{C}$ tal que para todo $v \in V_i$ se tiene que $z \cdot v = \lambda_i v$, y por lo tanto $z \cdot w_i = \lambda_i w_i$. De esto se sigue que

$$z = z \cdot 1 = z \cdot (w_1 + \cdots + w_k) = \lambda_1 w_1 + \cdots + \lambda_k w_k.$$

Esto implica que $Z(\mathbb{C}G)$ está contenido en el subespacio de $\mathbb{C}G$ generado por $\{w_1, \dots, w_k\}$. Como $\dim(Z(\mathbb{C}G)) = r$, se tiene que $r \leq k$, y por lo tanto $r = k$. □

Como corolarios directos obtenemos lo siguiente.

Corolario III.2.11. *Los caracteres irreducibles $\chi_1, \dots, \chi_k$ de un grupo finito G forman una base de $C_{\mathbb{C}}(G)$.*

Corolario III.2.12. *La tabla de caracteres de un grupo finito G es cuadrada.*

Retomando el Ejemplo III.1.9 manteniendo las notaciones, ya podemos demostrar que U, U' y V son los únicos $\mathbb{C}\mathfrak{S}_3$-módulos irreducibles de $\mathfrak{S}_3$. En efecto, $\mathfrak{S}_3$ tiene tres clases de conjugación, y se tiene que

1. $\langle \chi_I, \chi_I \rangle = \frac{1}{6}(1 \cdot 1^2 + 3 \cdot 1^2 + 2 \cdot 1^2) = 1$,
2. $\langle \chi_A, \chi_A \rangle = \frac{1}{6}(1 \cdot 1^2 + 3 \cdot (-1)^2 + 2 \cdot 1^2) = 1$,
3. $\langle \chi_{P'}, \chi_{P'} \rangle = \frac{1}{6}(1 \cdot 2^2 + 3 \cdot 0^2 + 2 \cdot (-1)^2) = 1$,
4. $\langle \chi_I, \chi_A \rangle = \frac{1}{6}(1 \cdot 1 \cdot 1 + 3 \cdot 1 \cdot (-1) + 2 \cdot 1 \cdot 1) = 0$,
5. $\langle \chi_I, \chi_{P'} \rangle = \frac{1}{6}(1 \cdot 1 \cdot 2 + 3 \cdot 1 \cdot 0 + 2 \cdot 1 \cdot (-1)) = 0$,
6. $\langle \chi_A, \chi_{P'} \rangle = \frac{1}{6}(1 \cdot 1 \cdot 2 + 3 \cdot (-1) \cdot 0 + 2 \cdot 1 \cdot (-1)) = 0$.

Teorema III.2.13 (Relaciones de ortogonalidad en las columnas de la tabla de caracteres)**.** *Sean $\chi_1, \dots, \chi_k$ los caracteres irreducibles de un grupo finito G, y sean $g_1, \dots, g_k$ representantes de las clases de conjugación de G. Entonces para cualesquiera $r, s \in \{1, \dots, k\}$, se tiene que*

$$\sum_{i=1}^{k} \chi_i(g_r)\overline{\chi_i(g_s)} = \delta_{rs}|C_G(g_r)|,$$

donde δ_{rs} es la Delta de Kronecker.

Demostración. Para $1 \leq s \leq k$, definimos ψ_s como la función de clase que satisface que $\psi_s(g_r) = \delta_{rs}$ para $1 \leq r \leq k$. Por el Corolario III.2.10, existen $z_1, \dots, z_k \in \mathbb{C}$ tales que $\psi_s = z_1\chi_1 + \cdots + z_k\chi_k$. Como $\langle \chi_i, \chi_j \rangle = \delta_{ij}$, $z_i = \langle \psi_s, \chi_i \rangle = \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} \psi_s(g)\overline{\chi_i(g)}$.

Como dado $g \in G$, $\psi_s(g) = 1$ si y solo si g es conjugado de g_s, y hay $\mathrm{ord}(G)/\mathrm{ord}(C_G(g_s))$ elementos de G conjugados con g_s, tenemos que

$$z_i = \frac{1}{\mathrm{ord}(G)} \sum_{g \in O_{g_s}} \psi_s(g)\overline{\chi_i(g)} = \frac{\overline{\chi_i(g_s)}}{|C_G(g_s)|}.$$

Por lo tanto

$$\delta_{rs} = \psi_s(g_r) = \sum_{i=1}^{k} z_i \chi_i(g_r) = \sum_{i=1}^{k} \frac{\chi_i(g_r)\overline{\chi_i(g_s)}}{|C_G(g_s)|}.$$

□

Este resultado se conoce como las *Relaciones de ortogonalidad en las columnas de la tabla de caracteres.*

CAPÍTULO IV

El Teorema de Burnside

En esta última sección demostraremos el Teorema de Burnside, el objetivo principal de este trabajo, y discutiremos brevemente su importancia en la clasificación de los grupos finitos. Previamente necesitamos unos resultados básicos sobre números algebraicos y su relación con los caracteres.

IV.1. Números algebraicos y caracteres

Definición IV.1.1. Un *número algebraico* α es un número complejo que es raíz de un polinomio con coeficientes en $\mathbb{Q}$. El polinomio mónico con coeficientes en $\mathbb{Q}$ de menor grado entre los que tienen a α como raíz se denomina *polinomio mínimo*.

Definición IV.1.2. Decimos que un número complejo α es un *entero algebraico* si es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$. Denotaremos al conjunto de todos ellos como $\mathbb{A}$.

Parece natural pensar que dado un entero algebraico, su polinomio mínimo tendrá coeficientes en $\mathbb{Z}$. Antes de probar este hecho, que será fundamental para la Proposición IV1,4, necesitamos algunos resultados previos.

Definición IV.1.3. Sea $f(\mathtt{t}) := a_n\mathtt{t}^n + \cdots + a_0 \in \mathbb{Z}[\mathtt{t}]$. Decimos que f es *primitivo* si $\gcd(a_0, \ldots, a_n) = 1$.

Lema IV.1.4. *El producto de dos polinomios primitivos es primitivo.*

Demostración. Sean $f, g \in \mathbb{Z}[\mathtt{t}]$, y supongamos que existe un primo p que divide a todos los coeficientes de fg. Sea $\phi : \mathbb{Z}[\mathtt{t}] \to \mathbb{Z}_p[\mathtt{t}]$; $f \mapsto f \bmod p$, que es un homomorfismo de anillos. Tenemos que $0 = \phi(fg) = \phi(f)\phi(g)$, y como $\mathbb{Z}_p[\mathtt{t}]$ es un dominio $\phi(f) = 0$, ó $\phi(g) = 0$, luego uno de los dos no es primitivo. □.

Teorema IV.1.5. *Sean $f, g \in \mathbb{Q}[\mathtt{t}]$ dos polinomios mónicos tales que $fg \in \mathbb{Z}[\mathtt{t}]$. Entonces $f, g \in \mathbb{Z}[\mathtt{t}]$.*

Demostración. Sea n (respectivamente m) el menor entero positivo para el que $nf \in \mathbb{Z}[\mathtt{t}]$ (respectivamente $mg \in \mathbb{Z}[\mathtt{t}]$). Si d es el máximo común divisor de los coeficientes de nf, en particular d divide al coeficiente director de nf, que es n por ser f mónico. Por lo tanto $\frac{n}{d}f \in \mathbb{Z}[\mathtt{t}]$, lo que contradice la minimalidad de n. Tenenemos entonces que $d = 1$ y nf es primitivo. Un razonamiento totalmente análogo nos da que mg es primitivo.
Por el Lema anterior tenemos que $h := (nf)(mg) = (nm)fg$ es también primitivo. Como

$fg \in \mathbb{Z}[\mathtt{t}]$ por hipótesis, nm divide a todos los coeficientes de h, luego $nm = 1$, lo que implica que $n = m = 1$, es decir, $f, g \in \mathbb{Z}[\mathtt{t}]$. □.

Proposición IV.1.6. *Sea $\alpha \in \mathbb{A}$. Entonces el polinomio mínimo f de α sobre $\mathbb{Q}$ cumple que $f \in \mathbb{Z}[\mathtt{t}]$*

Demostración. Como $\alpha \in \mathbb{A}$ existe un polinomio mónico $g \in \mathbb{Z}[\mathtt{t}]$ tal que $g(\alpha) = 0$. Dividiendo g entre f en $\mathbb{Q}[\mathtt{t}]$ existen $c(\mathtt{t}), r(\mathtt{t}) \in \mathbb{Q}[\mathtt{t}]$ con $0 \leq \deg r < \deg f$, tales que $g = c \cdot f + r$. Como $g(\alpha) = f(\alpha) = 0$ necesariamente $r(\alpha) = 0$. Si $r(\mathtt{t}) \neq 0$ existe $l \in \mathbb{Z}$ tal que $r(\mathtt{t})/l \in \mathbb{Q}[\mathtt{t}]$ es mónico de grado menor que f y con α como raíz, lo que contradice la minimalidad de f. Por lo tanto $g = c \cdot f$, con c mónico por serlo f y g. En virtud del teorema anterior $c, f \in \mathbb{Z}[\mathtt{t}]$. □

Proposición IV.1.7. *$\alpha \in \mathbb{A}$ si y solo si $\mathbb{Z}[\alpha]$ es un $\mathbb{Z}$-módulo libre de rango finito.*

Demostración. Sea $f(\mathtt{t}) := \mathtt{t}^n + a_{n-1}\mathtt{t}^{n-1} + \cdots + a_0$ el polinomio mínimo de $\alpha \in \mathbb{A}$. Por la proposición anterior $f \in \mathbb{Z}[\mathtt{t}]$. Los elementos $\{1, \alpha, \ldots, \alpha^{n-1}\}$ son $\mathbb{Z}$-linealmente independientes, pues de lo contario existirían $b_0, \ldots, b_{n-1} \in \mathbb{Z}$ no todos nulos tales que

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0.$$

Sin pérdida de generalidad asumimos que $b_{n-1} \neq 0$, por lo que dividiendo por dicho término tenemos que α es raíz del polinomio mónico con coeficientes en $\mathbb{Q}$

$$g(\mathtt{t}) := t^{n-1} + (b_{n-2}/b_{n-1})\mathtt{t}^{n-2} + \cdots + (b_0/b_{n-1}),$$

lo que contradice la minimalidad de f.
Como $f(\alpha) = 0$ despejando obtenemos que

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_0).$$

Así, para cualquier $m \geq n$ tenemos que

$$\alpha^m = -(a_{n-1}\alpha^{m-1} + \cdots + a_0\alpha^{m-n}).$$

Esto implica que α^m está en el $\mathbb{Z}$-módulo generado por $\{1, \alpha, \ldots, \alpha^{m-1}\}$. Por inducción sobre m tenemos entonces que α^m está en el $\mathbb{Z}$-módulo generado por $\{1, \alpha, \ldots, \alpha^{n-1}\}$, y como el conjunto es $\mathbb{Z}$-linealmente independiente, $\mathbb{Z}[\alpha]$ es libre con base $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Recíprocamente, supongamos que $\mathbb{Z}[\alpha]$ está finitamente generado por el conjunto

$$\{f_1(\alpha), \ldots, f_r(\alpha)\}, f_i \in \mathbb{Z}[\mathtt{t}].$$

Sea n el máximo de los grados de los f_i más uno. Como $\alpha^n \in \mathbb{Z}[\alpha]$ entonces existen $a_1, \ldots, a_r \in \mathbb{Z}$ tales que

$$\alpha^n = a_1 f_1(\alpha) + \cdots + a_r f_r(\alpha).$$

Por tanto α es raíz de un polinomio mónico con coeficientes enteros, es decir, es un entero algebraico. □

Proposición IV.1.8. *$\mathbb{A}$ es un subanillo de $\mathbb{C}$. Además se cumple que $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.*

Demostración. Para la primera parte es suficiente con comprobar que si $\alpha, \beta \in \mathbb{A}$, entonces $\alpha + \beta, \alpha\beta \in A$. Por el resultado anterior tenemos que tanto $\mathbb{Z}[\alpha]$ como $\mathbb{Z}[\beta]$ son $\mathbb{Z}$-módulos libres de rango finito. Por lo tanto $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\alpha][\beta]$ es libre de rango finito. Como $\mathbb{Z}[\alpha + \beta]$ y $\mathbb{Z}[\alpha\beta]$ son submódulos de $\mathbb{Z}[\alpha, \beta]$, por la Proposición I.3.9 ambos son $\mathbb{Z}$-módulos libres de rango finito. En consecuencia, el resultado se sigue de la Proposición IV.1.4.
Para la segunda parte, sea $\alpha \in \mathbb{A} \cap \mathbb{Q}$. Entonces existen $p, q \in \mathbb{Z}$ con $s \neq 0$ y $\gcd(p, q) = 1$ tales que $\alpha = p/q$. Por ser un entero algebraico existe un polinomio mónico $f(\mathtt{t}) = \mathtt{t}^n + a_{n-1}\mathtt{t}^{n-1} + \cdots + a_0$ con coeficientes en $\mathbb{Z}$, tal que $f(\alpha) = 0$. Por lo tanto

$$(p^n/q^n) + a_{n-1}(p^{n-1}/q^{n-1}) + \cdots + a_0 = 0.$$

Multiplicando a ambos lados por q^n y despejando p^n llegamos a que

$$p^n = -q(a_{n-1}p^{n-1} + a_0 q^{n-1}),$$

lo que implica que q divide a p^n, y como son coprimos necesariamente $q = \pm 1$, es decir, $\alpha \in \mathbb{Z}$. □

Corolario IV.1.9. *Sean G un grupo finito, V un espacio vectorial sobre un cuerpo F y ρ una representación de G en V. Entonces para todo $g \in G$, $\chi_V(g) \in \mathbb{A}$.*

Demostración. Sea $g \in G$, y denotemos $k := \mathrm{ord}(g)$. Por la Proposición III.1.4 sabemos que $\chi_V(g) = \zeta_1 + \cdots + \zeta_{\chi_V(e)}$, donde $\zeta_i^k = 1$ para $0 \leq i \leq \chi_V(e)$. Como cada ζ_i es un entero algebraico y estos forman un anillo, entonces $\chi_V(g) \in A$. □

Lema IV.1.10. *Sea G un grupo finito y tomamos $r := \sum_{g \in G} a_g g \in \mathbb{C}G$, tal que $a_g \in \mathbb{Z}$ para todo $g \in G$. Sea $u \in \mathbb{C}G$ no nulo tal que $ru = \lambda u$ para algún $\lambda \in \mathbb{C}$. Entonces $\lambda \in \mathbb{A}$.*

Demostración. Sean $g_1, \ldots, g_n$ los elementos de G. Entonces para cualquier $1 \leq i \leq n$, tenemos que $g_i r = \sum_{j=1}^n a_{ij} g_j$ para ciertos enteros a_{ij}. De hecho $a_{ij} = a_g$ donde $g = g_i^{-1} g_j$. Que $ru = \lambda u$ implica que λ es un autovalor de la matriz con coeficientes enteros $A = (a_{ij})$; es decir, es raíz de un polinomio mónico con coeficientes enteros. Por lo tanto $\lambda \in \mathbb{A}$. □

Corolario IV.1.11. *Sean χ un caracter irreducible de un grupo finito G con elemento neutro e_G, y $g \in G$. Entonces*

$$\lambda = \frac{|G|\chi(g)}{|C_G(g)|\chi(e_G)} \in \mathbb{A}.$$

Demostración. Sea U un $\mathbb{C}G$-módulo irreducible tal que el caracter de su representación asociada es χ. Sea $\overline{C}$ la suma de clase de la clase de conjugación de G que contiene a g. Entonces, por el Lema III.1.6, sabemos que $\overline{C} \cdot u = \lambda u$, para todo $u \in U$, y por el lema anterior $\lambda \in \mathbb{A}$. □

Definición IV.1.12. Sean $\alpha \in \mathbb{C}$ un número algebraico y $f \in \mathbb{Q}[\mathtt{t}]$ su polinomio mínimo. Llamaremos *conjugados* de α a las raíces de f.

Proposición IV.1.13. *Sean $\alpha, \beta \in \mathbb{C}$ números algebraicos, y sean $p, q \in \mathbb{Q}[\mathtt{t}]$ sus respectivos polinomios mínimos. Sea $r \in \mathbb{Q}[\mathtt{t}]$ el polinomio mínimo de $\alpha + \beta$. Si c es una raíz de r, entonces existen raíces a, b de p, q, respectivamente, tales que $c = a + b$. Además, dado $r \in \mathbb{Q}$, los conjugados de $r\alpha$ serán de la forma $r\alpha'$, donde α' es raíz de p.*

Demostración. Sea K el cuerpo de descomposición de r sobre $\mathbb{Q}$. Sea $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ tal que $\sigma(\alpha+\beta) = c$. Por ser σ un automorfismo tenemos que $c = \sigma(\alpha) + \sigma(\beta)$. Recordemos que dado $\gamma \in K$ los $\mathbb{Q}$-automorfismos de K mandan γ a raíces de su polinomio mínimo, por lo tanto $\sigma(\alpha)$ y $\sigma(\beta)$ serán raíces de los polinomios p y q, respectivamente.
Para la segunda parte basta ver que los $\mathbb{Q}$-automorfismos de K fijan los elementos de $\mathbb{Q}$. □

Proposición IV.1.14. *Sea ζ una raíz n-ésima de la unidad. Entonces todos los conjugados de ζ son raíces n-ésimas de la unidad.*

Demostración. Por ser ζ raíz n-ésima de la unidad será raíz del polinomio $\mathtt{t}^n - 1$. Como el polinomio mínimo de ζ divide a $\mathtt{t}^n - 1$, entonces todos los conjugados de ζ son también raíces de $\mathtt{t}^n - 1$; es decir, son raíces n-ésimas de la unidad. □

Lema IV.1.15. *Sean χ el caracter de un grupo finito G con elemento neutro e_G, y $g \in G$. Si $0 < |\chi(g)/\chi(e_G)| < 1$, entonces $\chi(g)/\chi(e_G)$ no es un entero algebraico.*

Demostración. Sea $d := \chi(e_G)$. Supongamos que $\chi(g)/d \in \mathbb{A}$ y que $|\chi(g)/d| < 1$. Vamos a probar que $\chi(g) = 0$. Sean $\gamma := \chi(g)/d$ y $p(\mathtt{t})$ el polinomio mínimo de γ. Entonces

$$p(\mathtt{t}) = \mathtt{t}^n + a_{n-1}\mathtt{t}^{n-1} + \cdots + a_0,$$

donde cada $a_i \in \mathbb{Z}$. Por la Proposición IV.1.13 y la Proposición IV.1.14, los conjugados de γ son de la forma

$$\frac{\zeta_1' + \cdots + \zeta_d'}{d},$$

donde cada ζ_i' es una raíz k-ésima de la unidad, siendo $k = \mathrm{ord}(g)$. Como $|\zeta_i'| < 1$ para todo $1 \leq i \leq d$, tenemos que el módulo de cualquier conjugado de γ es a lo sumo 1. Sea ω el producto de todos los conjugados de γ (incluyendo γ). Como $|\gamma| < 1$, entonces $|\omega| < 1$. Por otro lado, el producto de las raíces de un polinomio es igual en valor absoluto al término independiente de dicho polinomio, luego $\omega = \pm a_0$. Como $a_0 \in \mathbb{Z}$ y $|a_0| < 1$, tenemos que $a_0 = 0$. Por la irreducibilidad p, $p(\mathtt{t}) = \mathtt{t}$, luego $\gamma = 0$ y por lo tanto $\chi(g) = 0$. □

IV.2. Demostración del Teorema

Teorema IV.2.1. *Sean p un número primo y r un entero mayor que 0. Supongamos que G es un grupo finito que tiene una clase de conjugacion con p^r elementos. Entonces G no es simple.*

Demostración. Denotemos por simplicidad 1 el elemento neutro de G. Sea $g \in G$ tal que $|O_g| = p^r$. Sean $\chi_1, \ldots, \chi_r$ los caracteres irreducibles de G, donde χ_1 es el asociado a la representación trivial. Por las relaciones de ortogonalidad en la columna de la tabla de caracteres de G, aplicadas a las columnas de 1 y g, tenemos que

$$0 = \sum_{i=1}^{k} \chi_i(g)\chi_i(1) = 1 + \sum_{i=2}^{k} \chi_i(g)\chi_i(1).$$

Dividiendo ambos lados entre p obtenemos que

$$\sum_{i=2}^{k} \chi_i(g)\frac{\chi_i(1)}{p} = \frac{-1}{p}.$$

Por la Proposición IV.1.8, $-1/p$ no es un entero algebraico, y por lo tanto para algún $k \geq i \geq 2$, $\chi_i(g)\chi_i(1)/p$ no es un entero algebraico. Por ser $\chi_i(g)$ un entero algebraico, y ser $\mathbb{A}$ un anillo, se sigue que $\frac{\chi_i(1)}{p}$ no es un entero algebraico. De aquí se deduce que $\chi_i(g)$ es no nulo y que p no divide a $\chi_i(1)$. Como $|O_g| = p^r$, $|O_g|$ y $\chi_i(1)$ son coprimos, y por la identidad de Bézout existen enteros a, b tales que

$$a[G : C_G(g)] + b\chi_i(1) = 1.$$

Multiplicando ambos lados por el cociente $\frac{\chi_i(g)}{\chi_i(1)}$ llegamos a que

$$a\frac{|G|\chi_i(g)}{|C_G(g)|\chi_i(1)} + b\chi_i(g) = \frac{\chi_i(g)}{\chi_i(1)}.$$

Por el Corolario IV.1.11 y la Proposición IV.1.8, el lado izquierdo de la igualdad es un entero algebraico no nulo, y el Lema IV.1.15, implica que $\frac{|\chi_i(g)|}{|\chi_i(1)|} = 1$. Sea ρ la representación matricial de G cuyo caracter es χ_i. Por el Teorema III.1.5, existe $\lambda \in \mathbb{C}$ tal que $\rho(g) = \lambda I$. Sea $K := \ker \rho$, que es subgrupo normal de G. Como χ_i no es el caracter trivial, $K \neq G$. Si $K \neq \{1\}$, entonces G no es simple y hemos terminado. Si $K = \{1\}$ entonces ρ es una representación fiel. Como $\rho(g)$ es un múltiplo complejo de la identidad, conmuta con $\rho(h)$ para todo $h \in G$; es decir,

$$\rho(gh) = \rho(g)\rho(h) = \rho(h)\rho(g) = \rho(hg),$$

y por ser fiel tenemos que $gh = hg$ para todo $h \in G$, luego $g \in Z(G)$. Por lo tanto, $Z(G) \neq \{1\}$ y $Z(G) \neq G$, y como $Z(G)$ es un subgrupo normal de G, G no es simple. □

Ya estamos preparados para demostrar el Teorema.

Teorema IV.2.2 (Teorema de Burnside, 1904)**.** *Sean p y q números primos, y sean a, b dos enteros no negativos tales que $a + b \geq 2$. Si G es un grupo de orden $p^a q^b$, entonces G no es simple.*

Demostración. Supongamos primero que o bien a o bien b es cero. Entonces el orden de G es potencia de un primo, y por la Proposición I.1.13, tenemos que $Z(G) \neq \{1\}$. Sea $g \in Z(G)$ un elemento de orden primo, cuya existencia garantiza el Teorema de Cauchy. Entonces $\langle g \rangle \trianglelefteq G$, y $\langle g \rangle$ no es ni $\{1\}$ ni G, por lo tanto G no es simple.
Supongamos ahora que $a > 0$ y $b > 0$. Por el segundo teorema de Sylow, G tiene un subgrupo H de orden q^b, y de nuevo por la Proposición I.1.13, $Z(H) \neq \{1\}$. Sea $h \in Z(H)$, con $h \neq 1$. Por estar h en el centro del subgrupo H se tiene que H es a su vez un subgrupo de $C_G(h)$, luego $|O_h| = [G : C_G(h)] = p^r$, para algún $0 \leq r \leq a$. Si $r = 0$, entonces $h \in Z(G)$, luego $Z(G) \neq \{1\}$ y por el mismo argumento que antes G no es simple. Si $r > 0$, entonces por el Teorema IV.2.1, G no es simple. □

Como Corolario obtenemos el resultado fundamental de la memoria, la resolubilidad de los grupos de orden $p^a q^b$.

Corolario IV.2.3. *Sean p y q dos números primos, a y b dos enteros no negativos, y sea G un grupo de orden $p^a q^b$. Entonces G es resoluble.*

Demostración. Procedemos por inducción sobre la suma $a+b$. Si $a+b \leq 1$, entonces la única posibilidad es que G tenga orden primo y por lo tanto que sea cíclico, por lo que es abeliano, lo que implica que es resoluble. Ahora si $a+b > 1$, por el Teorema de Burnside, G no es simple; es decir, existe H subgrupo normal de G no trivial. Por lo tanto el orden de H es estrictamente menor que el de G y estrictamente mayor que 1, y los órdenes de H y G/H son de la forma $p^{a'}q^{b'}$, donde $a'+b' < a+b$. Por hipótesis de inducción tanto H como G/H son resolubles, y por la Proposición I.1.16 concluimos que G es resoluble. □

Corolario IV.2.4. *El grupo alternado de grado cinco $\mathfrak{A}_5$ es el grupo no resoluble de menor orden.*

Demostración. En primer lugar veamos que si G es un grupo de orden menor que 60 entonces es resoluble. Por el Teorema de Burnside el orden de G ha de ser divisible al menos por tres primos distintos. Como $3 \cdot 5 \cdot 7 > 60$, entonces el orden de G ha de ser par, luego las únicas posibilidades para el orden de G son $2 \cdot 3 \cdot 5 = 30$ y $2 \cdot 3 \cdot 7 = 42$.

Si $|G| = 30$, el número n_3 de 3-subgrupos de Sylow de G, cumple que $n_3 \in \{1, 10\}$, mientras el número n_5 de 5-subgrupos de Sylow de G, cumple que $n_5 \in \{1, 6\}$. Supongamos que $n_3 = 10$ y $n_5 = 6$, y sean $\{H_i : 1 \leq i \leq 10\}$ y $\{K_j : 1 \leq j \leq 6\}$ las familias de subgrupos de G de órdenes 3 y 5, respectivamente. Por el Teorema de Lagrange la intersección de cualesquiera par de miembros de ambas familias es únicamente el neutro del grupo, luego contando elementos llegamos a una contradicción:

$$30 = \mathrm{ord}(G) \geq 1 + 10 \cdot (3-1) + 6 \cdot (5-1) = 45$$

Así, bien G posee un único subgrupo de orden 3, que será normal por ser único, o bien G posee un único subgrupo de orden 5, que también será normal. Sea H el único subgrupo de orden 3 o 5. Por el Teorema de Burnside tanto H como G/H son resolubles, luego por el criterio de resolubilidad G es resoluble.

El caso $|G| = 42$ es más sencillo pues por el Tercer Teorema de Sylow la única posibilidad para el número de 7-subgrupos de G es $n_7 = 1$, luego G posee un único subgrupo de orden 7 que será por lo tanto normal. De nuevo el Teorema de Burnside y el criterio de resolubilidad nos dan que G es resoluble.

Que $\mathfrak{A}_5$ es no resoluble se desprende del hecho de que es no abeliano y simple (por el Teorema de Abel). Vamos a demostrar que si G es un grupo simple de orden 60 entonces necesariamente $G \cong \mathfrak{A}_5$.
Supongamos, por reducción al absurdo, que existe un grupo simple G de orden 60 que no es isomorfo al grupo alternado $\mathfrak{A}_5$. Por ser G simple no puede poseer ningún subgrupo cuyo índice sea 2. Tampoco puede poseer ningún subgrupo de índice 3 ó 4, pues de lo contrario sería isomorfo a algún subgrupo de $\mathfrak{A}_3$ ó $\mathfrak{A}_4$, respectivamente. Por el mismo motivo tampoco puede tener un subgrupo de índice 5, pues entonces el grupo sería isomorfo a $\mathfrak{A}_5$. Por lo tanto el índice de cualquier subgrupo de G debe ser mayor o igual que 6. En concreto

para cada divisor primo del orden del grupo el número de p-subgrupos de Sylow cumple que $n_p = [G : N_G(H)] \geq 6$, donde H es un p-subgrupo de Sylow de G.
Por el Tercer Teorema de Sylow necesariamente $n_2 = 15$, $n_3 = 10$ y $n_5 = 6$. Sean H_1 y H_2 dos 2-subgrupos de Sylow, y supongamos que su intersección tiene orden 2. Tanto H_1 como H_2 contienen a $H := H_1 \cap H_2$ como subgrupo de índice 2, por lo que H es un subgrupo normal de ambos y por lo tanto $H_i \subset N = N_G(H)$ para $i = 1, 2$. En particular:

$$8 = \frac{\text{ord}(H_1) \cdot \text{ord}(H_2)}{\text{ord}(H_1 \cap H_2)} = \#H_1H_2 \leq \text{ord}(N)$$

De aquí se deduce que $\text{ord}(N) \in \{12, 20, 60\}$. Los dos primeros casos son descartados pues ya hemos visto que G no posee subgrupos de índice menor que 6, y el último caso implica que $N = G$, así H sería un subgrupo normal de G contradiciendo que sea simple.
Por tanto, podemos suponer que la intersección de dos 2-subgrupos de Sylow cualesquiera es trivial, luego la intersección entre dos p y q subgrupos cualesquiera es trivial, y contando elementos llegamos a una contradicción:

$$60 = \text{ord}(G) \geq 1 + 15(4 - 1) + 10(3 - 1) + 6(5 - 1) = 90 \qquad \square$$

IV.3. Conclusiones

Más allá de la importancia que el Teorema de Burnside tuvo en el desarrollo de la Teoría de Representación de grupos finitos y en la Teoría de caracteres, el Teorema de Burnside y lo que implica jugaron un importante papel en el Teorema de Clasificación de grupos simples finitos, en cuya demostración participaron algunos de los algebristas más importantes del siglo XX, y que no fue completado completamente hasta 2004, cuando Michael Aschbacher publicó una prueba de 1221 páginas con el caso que faltaba. El enunciado del teorema es el siguiente.

Teorema IV.3.1 (Clasificación de grupos finitos simples)**.** *Todo grupo simple de orden finito es isomorfo a uno solo y solo uno de los siguientes:*

- *Un grupo cíclico de orden finito.*
- *Un grupo alternado de grado mayor o igual que* 5*.*
- *Uno grupo de tipo Lie (no confundir con los grupos de Lie).*
- *Uno de los* 26 *grupos esporádicos o el Grupo de Tits.*

La importancia del Teorema de Burnside radica en el siguiente resultado que se obtiene como corolario directo.

Corolario IV.3.2**.** *Sea G un grupo no abeliano simple de orden finito. Entonces* $\text{ord}(G)$ *es divisible por al menos tres primos distintos.*

El estudio que varios matemáticos habían hecho de casos concretos y los resultados de Burnside llevaron al propio Burnside a conjeturar lo siguiente[1]:

[1] *The contrast that these results show between groups of odd and even order suggests inevitably that simple groups of odd order do not exist.*

Conjetura IV.3.3. *Sea G un grupo no abeliano simple de orden finito. Entonces* $\mathrm{ord}(G)$ *es un número par.*

Cerca de 50 años después, esta conjetura fue probada por los matemáticos Walter Feit y John Griggs Thompson en la demostración de su célebre teorema.

Teorema IV.3.4 (Teorema de Feit-Thompson)**.** *Sea G un grupo finito de orden impar. Entonces G es resoluble.*

La demostración inicial ocupaba cerca de 255 páginas y era de una gran complejidad técnica. Hasta ese momento las demostraciones en Teoría de grupos no se extendían más allá de unas cuantas páginas, y habitualmente no involucraban argumentos muy técnicos. La demostración de este Teorema fue pionera matemática y filosóficamente, pues abrió el camino a demostraciones complejas y largas en Teoría de grupos.

A modo de curiosidad, Feit y Thompson conjeturaron en 1962 lo siguiente:

Conjetura IV.3.5**.** *No existen dos primos p y q distintos tales que $\frac{p^q-1}{p-1}$ y $\frac{q^p-1}{q-1}$ tienen un factor en común.*

De ser cierta esta conjetura, el capítulo final de su demostración del Teorema IV.3.4 se simplificaría enormemente.

Bibliografía

[AM] M.F. Atiyah, I.G. Macdonald. Introduction to Commutative Algebra. *Addison-Wesley* (1969).

[B] W. Burnside. Theory of Groups of Finite Order. *Cambridge University Press*. Segunda edición (1911).

[DF] D.S. Dummit, R.M. Foote. Abstract Algebra. *John Wiley and Sons, Inc.* Tercera edición (2004).

[FG1] J.F. Fernando, J.M. Gamboa: Estructuras Algebraicas: Teoría elemental de grupos. *Editorial Sanz y Torres*. Segunda edición (revisada) (2017).

[FG2] J.F. Fernando, J.M. Gamboa: Estructuras Algebraicas: Divisibilidad en anillos conmutativos. *Editorial Sanz y Torres*. Segunda edición (revisada) (2017).

[FG3] J.F. Fernando, J.M. Gamboa: Ecuaciones Algebraicas: Extensiones de cuerpos y Teoría de Galois. *Editorial Sanz y Torres*. Segunda edición (revisada) (2017).

[FH] W. Fulton, J. Harris. Representation Theory: A First Course. *Springer New York, NY* (2004).

[FT] W. Feit, J.G. Thompson. Solvablity of groups of odd order. *Pacific Journal of Mathematics*, **13** (1963), 775-1029.

[I] I.M. Isaacs. Character Theory of Finite Groups. *Dover publications* (2013).

[JL] G. James, M. Liebeck. Representation and Characters of Groups. *Cambridge University Press*. Segunda edición (2003).

[Z] L. Zeng. A note on finitely generated $\mathbb{Z}$-modules and algebraic integers. *International Conference on Education Reform and Modern Management* (April 19, 2015, Hong Kong).