UNIVERSIDAD NACIONAL DE CÓRDOBA

FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA

SERIE "B"

TRABAJOS DE MATEMATICA

Nº 58/2011

XV ELAM
Escuela Latinoamericana de Matemática
Álgebra no conmutativa y Teoría de Lie
CIMPA Research School
16-27 de mayo, 2011
Córdoba, Argentina

Cursos para estudiantes

Editores: Jorge R. Lauret–Jorge G. Adrover

CIUDAD UNIVERSITARIA – 5000 CÓRDOBA

REPÚBLICA ARGENTINA

XV ELAM
Escuela Latinoamericana de Matemática
Álgebra no conmutativa y Teoría de Lie

CIMPA Research School

16 – 27 de mayo, 2011

Córdoba, Argentina

Cursos para estudiantes

XV Escuela Latinoamericana de Matemática
Álgebra no conmutativa y Teoría de Lie

Cursos para estudiantes

El presente volumen contiene las notas de tres cursos para estudiantes que se dictaron en la XV Escuela Latinoamericana de Matemática, XV ELAM, sobre Álgebra no conmutativa y Teoría de Lie. La misma se llevó a cabo en la ciudad de Córdoba, Argentina, del 16 al 27 de mayo de 2011.

Durante la escuela hubo conferencias invitadas a cargo de especialistas, tanto locales como extranjeros, y hubo dos clases de cursos: avanzados y básicos. Los primeros estaban orientados a estudiantes de doctorado y jóvenes investigadores, y los últimos a estudiantes de grado y de maestría. Para que los cursos básicos fueran aprovechados de la mejor manera posible, además de estas notas, tuvieron clases prácticas en las cuales los alumnos trabajaron intensamente.

Gracias al invalorable esfuerzo de los profesores, que con gran antelación prepararon sus clases y notas, el presente volumen fue posible.

Gastón Andrés García Paulo Tirao

Contenido

REPRESENTACIONES DE GRUPOS FINITOS

MARIANO SUÁREZ-ALVAREZ

Índice

1. Representaciones

Groups, as men, will be known by their actions.
G. Moreno

1.1. Definiciones

Sea G un grupo finito y notemos $e \in G$ a su elemento neutro.

Definición 1.1.1. Una *representación (lineal)* de G es un par (V, ρ) en el que V es un espacio vectorial complejo y $\rho : G \to \mathrm{GL}(V)$ es un homomorfismo de grupos con codominio en el grupo $\mathrm{GL}(V)$ de los automorfismos lineales de V.

El espacio V es el *espacio de representación* de la representación (V, ρ) o, también, su *espacio subyacente*, y, si aquél tiene dimensión finita, el número $\dim V \in \mathbb{N}_0$ es el *grado* de la representación. Muchas veces, cuando este abuso de lenguaje no cause confusión, diremos que el espacio V mismo es una representación de G, dejando a la segunda

Date: 25 de abril, 2011.

componente del par (V, ρ) implícita. Cuando en esa situación queramos referirnos a ρ, escribiremos ρ_V.

Si V es un espacio vectorial, una función $\alpha : G \times V \to V$ es una *acción lineal* de G sobre V si se tiene, para cada v, $w \in V$, cada g, $h \in G$ y cada $\lambda \in \mathbb{C}$, que

$$\alpha(g, \lambda v) = \lambda\alpha(g, v), \qquad \alpha(g, v + w) = \alpha(g, v) + \alpha(g, w),$$
$$\alpha(e, v) = v, \qquad \alpha(g, \alpha(h, v)) = \alpha(gh, v).$$

Escribiremos generalmente $g \rightharpoonup v$ en lugar de $\alpha(g, v)$.

Los conceptos de representación y de acción lineal son esencialmente equivalentes. Por un lado, una representación (V, ρ) determina una función

$$\alpha : (g, v) \in G \times V \mapsto \rho(g)(v) \in V,$$

que es una acción lineal de G sobre V, como es inmediato verificar. Por otro, si $\alpha : G \times V \to V$ es una acción lineal de G sobre un espacio vectorial complejo V, podemos definir una función $\rho : G \to \mathrm{GL}(V)$ de manera que sea $\rho(g)(v) = \alpha(g, v)$ para cada $g \in G$ y cada $v \in V$, y obtener una representación (V, ρ) de G sobre V. Más aún, es fácil verificar que estas dos construcciones son mutuamente inversas.

Una *representación matricial* de G de *grado* n es un homomorfismo $r : G \to \mathrm{GL}(n, \mathbb{C})$ con valores en el grupo $\mathrm{GL}(n, \mathbb{C}) \subset M_n(\mathbb{C})$ de matrices complejas $n \times n$ inversibles.

Una representación lineal da origen a muchas representaciones matriciales. En efecto, sea (V, ρ) una representación de grado n, sea $\mathscr{B}$ una base ordenada de V y para cada $f \in \mathrm{End}(V)$ escribamos $\|f\|_B \in M_n(\mathbb{C})$ a la matriz de f con respecto a $\mathscr{B}$. Si $g \in G$, entonces la aplicación lineal $\rho(g) : V \to V$ es un automorfismo y, en consecuencia, la matriz $\|\rho(g)\|_{\mathscr{B}}$ es inversible, esto es, es un elemento de $\mathrm{GL}(n, \mathbb{C})$. Así, ρ y $\mathscr{B}$ determinan una función $\rho_{\mathscr{B}} : G \to \mathrm{GL}(n, \mathbb{C})$ tal que $\rho_{\mathscr{B}}(g) = \|\rho(g)\|_{\mathscr{B}}$ para todo $g \in G$, que es claramente un homomorfismo de grupos. Decimos que $\rho_{\mathscr{B}}$ es la representación matricial de G correspondiente a (V, ρ) y a la base $\mathscr{B}$.

Recíprocamente, una representación matricial $r : G \to \mathrm{GL}(n, \mathbb{C})$ determina una representación $(\mathbb{C}^n, \rho)$ de G sobre el espacio $\mathbb{C}^n$ en la que $\rho : G \to \mathrm{GL}(\mathbb{C}^n)$ está dada por $\rho(g)(v) = r(g) \cdot v$ para cada $g \in G$ y cada $v \in \mathbb{C}^n$; el producto $\cdot$ que aparece aquí es el producto usual de matrices y vectores. Es inmediato verificar que si $\mathscr{B}$ es la base ordenada canónica de $\mathbb{C}^n$, entonces la representación matricial $\rho_{\mathscr{B}}$ de G correspondiente a $(\mathbb{C}^n, \rho)$ y a $\mathscr{B}$ es precisamente el homomorfismo r.

Ejemplo 1.1.2. Si V es un espacio cualquiera, hay una representación $(V, \rho_{\mathsf{triv}})$ de G en la que $\rho_{\mathsf{triv}} : G \to \mathrm{GL}(V)$ es el homomorfismo trivial, de manera que $\rho_{\mathsf{triv}}(g) = \mathsf{id}_V$ para todo $g \in G$. Decimos en este caso que G *actúa trivialmente* sobre V y que $(V, \rho_{\mathsf{triv}})$ es la *representación trivial* de G sobre V. En particular, llamamos a la representación $(\mathbb{C}, \rho_{\mathsf{triv}})$ sobre $V = \mathbb{C}$ simplemente *la* representación trivial. □

Ejemplo 1.1.3. Si $V = 0$ es el espacio nulo, entonces el grupo $\mathrm{GL}(V)$ es trivial, su único elemento es id_V y hay entonces exactamente un homomorfismo de grupos $\rho : G \to \mathrm{GL}(V)$. Decimos que la representación correspondiente (V, ρ) es la *representación nula*. □

Ejemplo 1.1.4. Si V es un espacio vectorial y $G \subseteq \mathrm{GL}(V)$ es un subgrupo finito, entonces la inclusión $\rho : G \to \mathrm{GL}(V)$ es un homomorfismo de grupos. Tenemos entonces una representación (V, ρ) de G sobre V. □

Ejemplo 1.1.5. Dupongamos que X es un conjunto finito y que $\alpha : G \times X \to X$ es una acción de G sobre X. Recordemos que esto significa, si escribimos $g \cdot x$ en lugar

de $\alpha(g,x)$, que se tiene

$$e \cdot x = x, \qquad g \cdot (h \cdot x) = gh \cdot x \tag{1}$$

para cada $x \in X$ y cada g, $h \in G$. Sea $\mathbb{C}X$ el espacio vectorial que tiene como base al conjunto X, cuyos elementos son las combinaciones lineales formales $\sum_{x\in X} a_x x$ de elementos de X con coeficientes a_x en $\mathbb{C}$. Para cada $g \in G$ hay una única aplicación lineal $m_g : \mathbb{C}X \to \mathbb{C}X$ tal que $m_g(x) = g \cdot x$ si $x \in X$, ya que X es una base de $\mathbb{C}X$, y, como la imagen por m_g de X es el conjunto X mismo, es claro que m_g es un automorfismo de $\mathbb{C}X$. Podemos entonces definir una función $\rho_\alpha : G \to \mathrm{GL}(\mathbb{C}X)$ de manera que sea $\rho_\alpha(g) = m_g$ para cada $g \in G$. Es fácil verificar que las condiciones (1) satisfechas por la acción α de G sobre el conjunto X implican que ρ_α es un homomorfismo de grupos. Obtenemos así una representación $(\mathbb{C}X, \rho_\alpha)$ de G sobre $\mathbb{C}X$, a la que llamamos la *representación por permutación* correspondiente a X y la acción α. El grado de $\mathbb{C}X$ es el cardinal $|X|$ de X.

Si $X = G$ y si la acción $\alpha : G \times X \to X$ está dada por $\alpha(g,x) = gx$, entonces llamamos a la representación $(\mathbb{C}G, \rho_\alpha)$ la *representación regular* de G. □

1.2. Morfismos

Definición 1.2.1. Si (V, ρ_V) y (W, ρ_W) son representaciones de G, un *morfismo de representaciones* $\phi : (V, \rho_V) \to (W, \rho_W)$ es una aplicación lineal $\phi : V \to W$ entre los espacios vectoriales subyacentes tales que para cada $g \in G$ es

$$\phi \circ \rho_V(g) = \rho_W(g) \circ \phi.$$

Si, más aún, ϕ es biyectiva, decimos que ϕ es un *isomorfismo* de representaciones. Escribimos $\hom_G((V, \rho_V), (W, \rho_W))$, o simplemente $\hom_G(V, W)$, al subconjunto de $\hom(V, W)$ de los morfismos de representaciones.

En la situación de la definición, denotemos $\rightharpoonup_V$ y $\rightharpoonup_W$ a las acciones lineales de G sobre V y sobre W correspondientes a las representaciones (V, ρ_V) y (W, ρ_W), respectivamente. Entonces una aplicación lineal $\phi : V \to W$ es un morfismo de representaciones sii para cada $g \in V$ y cada $v \in V$ se tiene que

$$\phi(g \rightharpoonup_V v) = g \rightharpoonup_W \phi(v).$$

De manera similar, podemos expresar la condición de que ϕ sea un morfismo de representaciones en términos de representaciones matriciales. Sean $n = \dim V$ y $m = \dim W$, sean $\mathscr{B}$ y $\mathscr{B}'$ bases ordenadas de V y de W, y sean $(\rho_V)_{\mathscr{B}} : G \to \mathrm{GL}(n, \mathbb{C})$ y $(\rho_W)_{\mathscr{B}'} : G \to \mathrm{GL}(m, \mathbb{C})$ las representaciones matricales correspondientes a (V, ρ_V) y $\mathscr{B}$, y a (W, ρ_W) y $\mathscr{B}'$, respectivamente. Escribamos además $\|\phi\|_{\mathscr{B},\mathscr{B}'}$ a la matriz de ϕ con respecto a $\mathscr{B}$ y $\mathscr{B}'$. Entonces ϕ es un morfismo de representaciones si y solo si

$$\|\phi\|_{\mathscr{B},\mathscr{B}'} \cdot (\rho_V)_{\mathscr{B}}(g) = (\rho_W)_{\mathscr{B}'}(g) \cdot \|\phi\|_{\mathscr{B},\mathscr{B}'}$$

para cada $g \in G$; aquí $\cdot$ es el producto de matrices.

Proposición 1.2.2. *Sean (V, ρ_V), (W, ρ_W), (U, ρ_U) representaciones de G.*

(*i*) *La función identidad $\mathsf{id}_V : V \to V$ es un morfismo de representaciones.*

(*ii*) *Si $\phi : V \to W$ y $\psi : W \to U$ son morfismos de representaciones, entonces la composición $\psi \circ \psi : V \to U$ es un morfismo de representaciones.*

(*iii*) *El subconjunto $\hom_G(V, W)$ de $\hom(V, W)$ es un subespacio vectorial.*

(*iv*) *Si $f : V \to W$ es un isomorfismo de representaciones, entonces la función inversa $f^{-1} : W \to V$ también lo es.*

Demostración. □

Ejemplo 1.2.3. Consideremos la representación trivial $(\mathbb{C}, \rho_{\mathsf{triv}})$ y la representación regular $(\mathbb{C}G, \rho_{\mathsf{reg}})$. Sea $t = \sum_{h\in G} h \in \mathbb{C}G$ y sea $\phi_0 : \lambda \in \mathbb{C} \mapsto \lambda t \in \mathbb{C}G$. Si $g \in G$ y $\lambda \in \mathbb{C}$, entonces $\phi_0(g \rightharpoonup \lambda) = \phi_0(\lambda) = \lambda t = g \rightharpoonup \lambda t$: esto muestra que ϕ_0 es un morfismo de representaciones, de manera que $\phi_0 \in \hom_G(\mathbb{C}, \mathbb{C}G)$.

De hecho, en esta situación podemos ver que $\hom_G(\mathbb{C}, \mathbb{C}G)$ es un subespacio de $\hom(\mathbb{C}, \mathbb{C}G)$ generado por ϕ_0, de manera que en particular tiene dimensión 1. En efecto, supongamos que $\phi : \mathbb{C} \to \mathbb{C}G$ es un morfismo de representaciones, y sea $s = \phi(1) \in \mathbb{C}G$. Como G es una base de $\mathbb{C}G$, existen escalares a_h, $h \in G$, tales que $s = \sum_{h\in G} a_h h$. Si $g \in G$, entonces, como ϕ es un morfismo,

$$\sum_{h\in G} a_h h = \phi(1) = \phi(g \rightharpoonup 1) = g \rightharpoonup \phi(1) = g \rightharpoonup \sum_{h\in G} a_h h = \sum_{h\in G} a_{g^{-1}h} h.$$

El conjunto G es una base de $\mathbb{C}G$, asi que esto implica que $a_h = a_{g^{-1}h}$ para todo $h \in G$; en particular, tomando $h = g$ vemos que $a_g = a_e$. Esto es cierto para cada $g \in G$, así que en definitiva tenemos que $s = a_e t$ y, entonces, $\phi = a_e \phi_0$. Esto muestra que $\hom_G(\mathbb{C}, \mathbb{C}G)$ está generado por ϕ_0, como afirmamos. □

1.3. Subrepresentaciones

Proposición 1.3.1. *Sea (V, ρ) una representación de G, sea $W \subseteq V$ un subespacio vectorial y supongamos que*

$$\text{para cada } g \in G \text{ se tiene que } \rho(g)(W) \subseteq W. \tag{2}$$

Hay entonces una función $\rho_W : G \to \mathrm{GL}(W)$ tal que $\rho_W(g) = \rho(g)|_W$ para cada $g \in G$, el par (W, ρ_W) es una representación de G en W y la inclusión $\iota : W \to V$ es un morfismo de representaciones.

De hecho, es fácil verificar que en esta sitación el subespacio W puede dotarse de una *única* estructura de representación de G tal que la inclusión ι resulte un morfismo de representaciones.

Demostración. □

Definición 1.3.2. Si (V, ρ) es una representación de G y $W \subseteq V$ es un subespacio vectorial. Si W satisface la condición (2) de la proposición anterior, decimos que W es una *subrepresentación* de V o, también, que W es *G-invariante*.

Si W es una subrepresentación de (V, ρ), entonces W es el espacio subyacente a una representación (W, ρ_W), con ρ_W determinada por ρ como en la proposición. En todo lo que sigue, siempre que tengamos una subrepresentación de una representación, la considereraremos implicitamente a ella misma como una representación de esta manera.

Sea (V, ρ) una representación y sea $W \subseteq V$ un subespacio G-invariante. Sean $n = \dim V$ y $m = \dim W$, y sea $\rho_W : G \to \mathrm{GL}(W)$ la representación de G sobre W. Podemos elegir una base $\mathscr{B} = \{v_1, \dots, v_n\}$ de V de manera que el subconjunto $\mathscr{B}' = \{v_1, \dots, v_m\}$ sea una base de W. Si $\rho_{\mathscr{B}} : G \to \mathrm{GL}(n, \mathbb{C})$ es la representación matricial correspondiente a V y a $\mathscr{B}$, y $(\rho_W)_{\mathscr{B}'} : G \to \mathrm{GL}(m, \mathbb{C})$ es la representación

matricial correspondiente a W y a $\mathscr{B}'$, entonces como W es invariante, para cada $g \in G$ la matriz $\rho_{\mathscr{B}}(g)$ es una matriz de bloques de la forma

$$\left(\begin{array}{c:c} (\rho_W)_{\mathscr{B}'}(g) & * \\ \hdashline 0 & * \end{array}\right)$$

Definición 1.3.3. Sea V una representación. Si $W \subseteq V$ es una subrepresentación, decimos que W es *propia* si $W \subsetneq V$ y que es *nula* si $W = 0$. Por otro lado, V es *simple* si $V \neq 0$ y no posee subrepresentaciones propias y no nulas.

Ejemplo 1.3.4. Si V es una representación, el subespacio nulo $0 \subseteq V$ y el espacio total V mismo son subrepresentaciones de V. Esto implica inmediatamente que V es simple si tiene *exactamente* dos subrepresentaciones distintas. □

Ejemplo 1.3.5. Una representación de grado 1 es siempre simple. Por otro lado, una representación trivial V es simple si y solo si $\dim V = 1$: en efecto, si $\dim V > 1$, existe un subespacio $W \subset V$ tal que $0 \subsetneq W \subsetneq V$ y es inmediato que W es G-invariante. □

Ejemplo 1.3.6. Si (V, ρ) es una representación, escribimos

$$V^G = \{v \in V : \text{para todo } g \in G \text{ es } g \rightharpoonup v = v\}.$$

Es fácil ver que V^G es una subrepresentación de V y que es, de hecho, la subrepresentación más grande de V sobre la que G actúa trivialmente. □

Ejemplo 1.3.7. Supongamos que G actúa sobre un conjunto finito X, como en el ejemplo 1.1.5, y sea $\mathbb{C}X$ la correspondiente representación de G. Afirmamos que $\mathbb{C}X$ es simple sii $|X| = 1$. La condición es suficiente, ya que cuando $|X| = 1$ es $\dim \mathbb{C}X = 1$. Por otro lado, si $|X| = 1$, entonces el subespacio $T \subset \mathbb{C}X$ generado por el elemento $t = \sum_{x \in X} x$ es una subrepresentación y, como $\dim T = 1 < \dim \mathbb{C}X$, se trata de una subrepresentación propia. □

Proposición 1.3.8. *Sean V y W representaciones y sea $f : V \to W$ un morfismo de representaciones. Entonces el núcleo* $\ker f$ *es una subrepresentación de V y la imagen* $\operatorname{im} f$ *es una subrepresentación de W.*

Demostración. □

Una aplicación inmediata de esta proposición es el llamado Lema de Schur, una de las herramientas fundamentales de toda la teoría:

Teorema 1.3.9 (Lema de Schur)**.** *Sean (V, ρ_V) y (W, ρ_W) dos representaciones simples.*

(*i*) *Un morfismo no nulo $\phi : V \to W$ de representaciones es un isomorfismo.*

(*ii*) *Si $\phi : V \to V$ es un endomorfismo de representaciones, entonces existe $\lambda \in \mathbb{C}$ tal que $\phi = \lambda \operatorname{id}_V$.*

Demostración. (*i*) Como ϕ no es nulo, es $\ker \phi \subsetneq V$: como V es simple y $\ker \phi$ es una subrepresentación de V, esto implica que necesariamente $\ker \phi = 0$. Por otro lado, $\operatorname{im} \phi \neq 0$ porque, otra vez, ϕ no es nulo, y como $\operatorname{im} \phi$ es una subrepresentación de la representación simple W, debe ser $\operatorname{im} \phi = W$. Vemos así que ϕ es un isomorfismo.

(*ii*) Como $\mathbb{C}$ es algebraicamente cerrado, existen $\lambda \in \mathbb{C}$ y $v_0 \in V$ tales que $\phi(v_0) = \lambda v_0$. En consecuencia, la aplicación lineal $\phi - \lambda \operatorname{id}_V : V \to V$ no es biyectiva. Si $g \in G$ y

$v \in V$, entonces

$$\begin{aligned}(\phi - \lambda \operatorname{id}_V)(g \rightharpoonup v) &= \phi(g \rightharpoonup v) - \lambda(g \rightharpoonup v)\\ &= g \rightharpoonup \phi(v) - g \rightharpoonup (\lambda v)\\ &= g \rightharpoonup (\phi - \lambda \operatorname{id}_V)(v).\end{aligned}$$

Vemos así que $\phi - \lambda \operatorname{id}_V$ es un morfismo de representaciones y la parte (i) del teorema implica entonces que $\phi - \lambda \operatorname{id}_V = 0$: esto prueba la parte (ii). □

Ejemplo 1.3.10. Supongamos que G actúa sobre el conjunto finito X. Supongamos además que $Y \subseteq X$ es un subconjunto G-invariante, esto es, tal que

$$g \in G,\, y \in Y \implies g \cdot y \in Y.$$

El subespacio $\mathbb{C}Y = \langle y : y \in X\rangle$ de $\mathbb{C}X$ generado por los elementos de Y es entonces una subrepresentación. □

Ejemplo 1.3.11. Sea X un conjunto finito sobre el que G actúa y sea $f : \mathbb{C}X \to \mathbb{C}$ la aplicación lineal tal que $f(x) = 1$ para todo $x \in X$. Es fácil verificar que f es un morfismo de representaciones, así que $W = \ker f$ es una subrepresentación de $\mathbb{C}X$; explícitamente, es

$$W = \Big\{\sum_{x\in X} \lambda_x x \in \mathbb{C}X : \sum_{x\in X} \lambda_x = 0\Big\}.$$

El grado de W es claramente $\dim \ker f = \dim \mathbb{C}X - \dim \mathbb{C} = |X| - 1$. En particular, W es no nula exactamente cuando $|X| > 1$. □

Proposición 1.3.12. *Toda representación no nula de G contiene subrepresentaciones simples.*

Demostración. Sea V una representación. Probemos que V posee al menos una subrepresentación simple $U \subseteq V$ haciendo inducción sobre el grado $n = \dim V$. Cuando $n = 1$, podemos tomar $U = V$. Supongamos entonces que $n > 1$.

Si V es simple, podemos elegir otra vez $U = V$. Si en cambio V no es simple, entonces posee una subrepresentación $V' \subseteq V$ propia y no nula. En particular, $\dim V' < \dim V$, así que la hipótesis inductiva implica que V' posee una subrepresentación simple $U \subseteq V'$. Pero entonces U es una subrepresentación simple de V, que es lo que buscábamos. □

1.4. Completa reducibilidad

Definición 1.4.1. Decimos que una representación V es *descomponible* si existen subrepresentaciones no nulas W y U tales que $V = W \oplus U$, y que es *indescomponible* en caso contrario.

Ejemplo 1.4.2. Sea X un conjunto finito sobre el que G actúa, y consideremos la relación $\sim$ en X tal que si x, $y \in X$ es

$$x \sim y \iff \text{existe } g \in G \text{ tal que } g \cdot x = y.$$

Se trata de una relación de equivalencia, así que determina una partición Π de X. Más aún, es claro que para cada parte $Y \in \Pi$ se tiene que

$$g \in G,\, y \in Y \implies g \cdot y \in Y,$$

de manera que, como en el ejemplo 1.3.10, el subespacio $\mathbb{C}Y = \langle y \in Y \rangle$ de $\mathbb{C}X$ es G-invariante. Puede verse fácilmente que $\mathbb{C}X$ es la suma directa de los subespacios $\mathbb{C}Y$ con $Y \in \Pi$. □

Ejemplo 1.4.3. Sea otra vez X un conjunto finito sobre el que G actúa, y supongamos que $|X| > 1$. En el ejemplo 1.3.7 construimos una subrepresentación T de $\mathbb{C}X$ de grado 1, generada en tanto espacio vectorial por el elemento $t = \sum_{x \in X} x$, y en el ejemplo 1.3.7 construimos una subrepresentación

$$W = \Big\{ \sum_{x \in X} \lambda_x x \in \mathbb{C}X : \sum_{x \in X} \lambda_x = 0 \Big\}.$$

de grado $|X| - 1$. Es inmediato verificar que $T \cap W = 0$, y que $T + W = \mathbb{C}X$, de manera que $\mathbb{C}X = T \oplus W$. Así, como T y W son subrepresentación propias, $\mathbb{C}X$ es descomponible. □

Se sigue inmediatamente de las definiciones que una representación simple es indescomponible. Un resultado fundamental de la teoría es que la afirmación recíproca tambien es cierta. Para obtener este resultado, que enunciamos en el Corolario 1.4.7 más abajo, necesitamos establecer antes algunos resultados preliminares.

Lema 1.4.4. *Sean (V, ρ_V) y (W, ρ_W) dos representaciones, y sea $f : V \to W$ una aplicación lineal. Entonces la función lineal $\hat{f} : V \to W$ dada por*

$$\hat{f} = \frac{1}{|G|} \sum_{g \in G} \rho_W(g) \circ f \circ \rho_V(g^{-1})$$

es un morfismo de representaciones. Más aún, si $(W, \rho_W) = (V, \rho_V)$, entonces

$$\operatorname{tr} \hat{f} = \operatorname{tr} f.$$

Demostración. Denotemos $\rightharpoonup_V$ y $\rightharpoonup_W$ a las acciones lineales de G sobre V y sobre W correspondientes a las representaciones (V, ρ_V) y (W, ρ_W).

Si $h \in G$ y $v \in V$, entonces

$$\begin{aligned} \hat{f}(h \rightharpoonup_V v) &= \frac{1}{|G|} \sum_{g \in G} g \rightharpoonup_W f(g^{-1} \rightharpoonup_V (h \rightharpoonup_V v)) \\ &= \frac{1}{|G|} \sum_{g \in G} g \rightharpoonup_W f(g^{-1}h \rightharpoonup_V v) \end{aligned}$$

y, poniendo $k = h^{-1}g$, esto es

$$\begin{aligned} &= \frac{1}{|G|} \sum_{k \in G} hk \rightharpoonup_W f(k^{-1} \rightharpoonup_V v) \\ &= h \rightharpoonup_W \frac{1}{|G|} \sum_{k \in G} k \rightharpoonup_W f(k^{-1} \rightharpoonup_V v) \\ &= h \rightharpoonup_W \hat{f}(v). \end{aligned}$$

Vemos de esta forma que $\hat{f}$ es un morfismo.

Para terminar, supongamos que $(W, \rho_W) = (V, \rho_V)$. Si $g \in G$, tenemos que

$$\operatorname{tr}\big(\rho_V(g) \circ f \circ \rho_V(g^{-1})\big) = \operatorname{tr}\big(\rho_V(g^{-1}) \circ \rho_V(g) \circ f\big) = \operatorname{tr} f,$$

de manera que

$$\operatorname{tr} \hat{f} = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}\big(\rho_V(g) \circ f \circ \rho_V(g^{-1})\big) = \operatorname{tr} f. \qquad \square$$

Proposición 1.4.5. *Sea V una representación de G y sea $W \subseteq V$ un subespacio G-invariante. Entonces existe otro subespacio G-invariante $U \subseteq V$ tal que $V = W \oplus U$.*

Demostración. Fijemos una aplicación lineal $p : V \to V$ tal que $p \circ p = p$ y cuya imagen es el subespacio W; en particular, se tendrá que $p(w) = w$ para todo $w \in W$. Por ejemplo, si $\dim V = n$ y $\dim W = r$, existe una base $\{v_1, \dots, v_n\}$ de V tal que $\{v_1, \dots, v_r\}$ es una base de W, y podemos considerar la aplicación lineal $p : V \to V$ tal que $p(v_i) = v_i$ para cada $i \in \{1, \dots, r\}$ y tal que $p(v_i) = 0$ si $i \in \{r+1, \dots, n\}$.

Consideremos además la función lineal $\hat{p} : V \to V$ tal que

$$\hat{p}(v) = \frac{1}{|G|} \sum_{g \in G} g \rightharpoonup p(g^{-1} \rightharpoonup v)$$

para todo $v \in V$. Mostremos que $U = \ker \hat{p}$ es una subrepresentación de V y que $V = W \oplus U$: esto probará la proposición.

- Para ver que U es una subrepresentación, es suficiente —de acuerdo a la Proposicion 1.3.8— con observar que $\hat{p}$ es un morfismo de representaciones, y esto es consecuencia del Lema 1.4.4.
- La aplicación $\hat{p}$ tiene imagen W y es $\hat{p} \circ \hat{p} = \hat{p}$. En efecto, como la imagen de p es W y W es G-invariante, es claro que para todo $v \in V$ es $\hat{p}(v) \in W$. Por otro lado, si $w \in W$ y $g \in G$, es $g^{-1} \rightharpoonup w \in W$ y, en consecuencia, $p(g^{-1} \rightharpoonup w) = g^{-1} \rightharpoonup w$; se sigue entonces que para cada $w \in W$ se tiene que

  $$\hat{p}(w) = \frac{1}{|G|} \sum_{g \in G} g \rightharpoonup p(g^{-1} \rightharpoonup w) = \frac{1}{|G|} \sum_{g \in G} g \rightharpoonup g^{-1} \rightharpoonup w = w.$$

  Ahora, si $v \in W \cap U$, entonces $p(v) = v$ porque $v \in W$, y $p(v) = 0$ porque $v \in U$: vemos así que $W \cap U = 0$. En segundo lugar, si $v \in V$, entonces $\hat{p}(v - \hat{p}(v)) = \hat{p}(v) - \hat{p}(\hat{p}(v)) = 0$ porque $\hat{p}(v) \in W$, de manera que $v - \hat{p}(v) \in U$, y $\hat{p}(v) \in W$ porque la imagen de $\hat{p}$ es W: entonces $v = \hat{p}(v) + (v - \hat{p}(v)) \in W + U$ y esto nos dice que $V \subseteq W + U$. $\square$

Teorema 1.4.6. *Toda representación de G es suma directa de subrepresentaciones simples.*

Clásicamente, este teorema se enuncia diciendo que toda representación es *completamente reducible*.

Demostración. Sea V una representación y sea $n = \dim V$. Mostremos que V es suma directa de subrepresentaciones simples haciendo inducción en n. Si $n = 0$ no hay nada que probar, así que podemos suponer que $n > 0$.

De acuerdo a la Proposicion 1.3.12, existe una subrepresentación simple $W \subseteq V$. Si $W = V$, entonces V es simple, y por supuesto es suma directa de subrepresentaciones simples. Si, en cambio, $W \subsetneq V$, la Proposición 1.4.5 nos dice que existe una subrepresentación $U \subseteq V$ tal que $V = W \oplus U$. Ahora bien, $\dim U < \dim V$, así que inductivamente podemos suponer que existen $m \geq 1$ y subrepresentaciones $U_1, \dots, U_m \subseteq U$ tales que $U = U_1 \oplus \cdots \oplus U_m$. Pero entonces $V = W \oplus U_1 \oplus \cdots \oplus U_m$ es suma directa de subrepresentaciones simples, como queríamos probar. Esto completa la inducción. $\square$

La descomposición de una representación como suma directa de subrepresentaciones simples no es única. Por ejemplo, si V es una representación trivial de dimensión 2, entonces todo subespacio de V de dimensión 1 es una subrepresentación de V, y si U_1 y U_2 son dos tales subespacios distintos, entonces $V = U_1 \oplus U_2$.

Corolario 1.4.7. *Una representación es simple si y solamente si es indescomponible.*

Demostración. Es claro que una representación simple es indescomponible. Por otro lado, una representación descomponible, siendo suma directa de dos subrepresentaciones propias y no nulas, no es simple. □

1.5. Construcciones

Suma directa

Si (V, ρ_V) y (W, ρ_W) son dos representaciones de G, podemos hay una representación $(V \oplus W, \rho)$ sobre el espacio vectorial suma directa (externa) $V \oplus W$, cuyo homomorfismo de grupos $\rho : G \to \mathrm{GL}(V \oplus W)$ es tal que para cada $g \in G$ es

$$\rho(g) = \begin{pmatrix} \rho_V(g) & 0 \\ 0 & \rho_W(g) \end{pmatrix}.$$

Es fácil verificar que las inclusiones $i_V : V \to V \oplus W$ $i_V : W \to V \oplus W$ y las proyecciones $p_V : V \oplus W \to V$ y $p_W : V \oplus W \to W$ son morfismos de representaciones.

Espacios de homomorfismos

Sean (V, ρ_V) y (W, ρ_W) dos representaciones, y consideremos el espacio vectorial $\hom(V, W)$ de todas las aplicaciones lineales $V \to W$. Consideremos la función $\rho : G \to \mathrm{GL}(\hom(V, W))$ tal que

$$\rho(g)(f) = \rho_W(g) \circ f \circ \rho_V(g^{-1})$$

para cada $g \in G$ y cada $f \in \hom(V, W)$. Es fácil verificar que ρ está bien definida y que se trata de un homomorfismo de grupos, así que tenemos una representación $(\hom(V, W), \rho)$ de G sobre $\hom(V, W)$. Siempre que veamos a $\hom(V, W)$ como representación de G será con respecto a esta estructura.

Notemos que si $\rightharpoonup_V$ y $\rightharpoonup_W$ son las acciones de G sobre V y W, respectivamente, y $\rightharpoonup$ es la acción de G sobre $\hom(V, W)$, entonces para cada $g \in G$, cada $f \in \hom(V, W)$ y cada $v \in V$ se tiene que $(g \rightharpoonup f)(v) = g \rightharpoonup_W f(g^{-1} \rightharpoonup_V v)$.

Proposición 1.5.1. *Si (V, ρ_V) y (W, ρ_W) son representaciones, entonces*

$$\hom_G(V, W) = \hom(V, W)^G.$$

El espacio $\hom(V, W)^G$ que aparece a la derecha en esta igualdad es el subespacio de invariantes de la representación $\hom(V, W)$ definido en el Ejemplo 1.3.6.

Demostración. Sea $f \in \hom(V, W)$. Entonces $f \in \hom(V, W)^G$ sii para todo $g \in G$ es $f = g \rightharpoonup f$, y esto ocurre cuando para todo $v \in V$ se tiene que

$$f(v) = (g \rightharpoonup f)(v) = g \rightharpoonup_W f(g^{-1} \rightharpoonup_V v).$$

Es inmediato que está última condición se cumple exactamente cuando f es un morfismo de representaciones, esto es, cuando $f \in \hom_G(V, W)$. □

Espacio dual

Un caso particular de la construcción anterior es aquél en el que la representación (W, ρ_W) es la representación trivial $(\mathbb{C}, \rho_{\mathsf{triv}})$. Es entonces $\hom(V, \mathbb{C})$ el espacio dual de V, que notamos simplemente V'. Si $(- \mid -) : V' \times V \to \mathbb{C}$ es la evaluación y si $\rightharpoonup_V$ y $\rightharpoonup_{V'}$ son las acciones de G sobre V y V', entonces para cada $f \in V'$ y cada $v \in V$ es

$$(g \rightharpoonup_{V'} f \mid v) = (f \mid g^{-1} \rightharpoonup_V v).$$

Lema 1.5.2. *Sea (V, ρ_V) una representación, sea $(V', \rho_{V'})$ su representación dual, y sea $(V'', \rho_{V''})$ la representación de ésta última. El isomorfismo canónico de espacios vectoriales $\xi : V \to V''$ es un isomorfismo de representaciones.*

Demostración. Recordemos que la función ξ está determinada por la condición de que para todo $v \in V$ y todo $f \in V'$ es $\xi(v)(f) = (f \mid v)$.

Sea $g \in G$ y $v \in V$. Si $f \in V'$, entonces

$$\begin{aligned}(g \rightharpoonup \xi(v))(f) &= \xi(v)(g^{-1} \rightharpoonup f)\\ &= (g^{-1} \rightharpoonup f \mid v)\\ &= (f \mid g \rightharpoonup v)\\ &= \xi(g \rightharpoonup v)(f),\end{aligned}$$

así que $g \rightharpoonup \xi(v) = \xi(g \rightharpoonup v)$. Esto nos dice que ξ es un morfismo de representaciones, y el lema sigue de esto. □

Proposición 1.5.3. *Sea (V, ρ_V) una representación, sea $(V', \rho_{V'})$ la representación dual. Entonces V es simple si y solamente si V' es simple.*

Demostración. Supongamos que V no es simple y sea $W \subsetneq V$ una subrepresentación propia no nula. Sea $W^\perp = \{f \in V' : (f \mid w) = 0 \text{ para todo } w \in W\}$.

Si $f \in W^\perp$ y $g \in G$, entonces para cada $w \in W$ tenemos que

$$(g \rightharpoonup f \mid w) = (f \mid g^{-1} \rightharpoonup w) = 0$$

porque $g^{-1} \rightharpoonup w \in W$, de manera que $g \rightharpoonup f \in W^\perp$. Es así $W^\perp$ una subrepresentación de V' y, como $0 \subsetneq W^\perp \subseteq V'$, concluimos que V' no es simple.

Ahora bien, usando lo ya hecho, sabemos que si V' no es simple, entonces V'' tampoco lo es y, en vista del Lema 1.5.2, esto nos dice que la representación V misma no es simple. Esto completa la prueba. □

Productos tensoriales

Sean (V, ρ_V) y (W, ρ_W) dos representaciones y sea $V \otimes W$ el producto tensorial de los espacios vectoriales subyacentes. Hay un homomorfismo de grupos $\rho : G \to \mathrm{GL}(V \otimes W)$ tal que para cada $g \in G$ es $\rho(g) = \rho_V(g) \otimes \rho_W(g)$, así que tenemos una representación $(V \otimes W, \rho)$. Si $\rightharpoonup_V$ y $\rightharpoonup_W$ son las acciones de G sobre V y W, respectivamente, entonces la acción de G sobre $V \otimes W$ está dada por

$$g \rightharpoonup v \otimes w = (g \rightharpoonup_V v) \otimes (g \rightharpoonup_W w)$$

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

Las propiedades formales usuales que relacionan a hom con $\otimes$ se preservan al extenderlos de los espacios vectoriales a las representaciones lineales de un grupo:

Proposición 1.5.4. *Sean (V, ρ_V), (W, ρ_W) y (U, ρ_U) representaciones de G.*

(*i*) *El isomorfismo canónico de espacios vectoriales*

$$\Phi : \hom(V \otimes W, U) \to \hom(V, \hom(W, U))$$

es un isomorfismo de representaciones.

(*ii*) *El isomorfismo canónico*

$$\Psi : V' \otimes W \to \hom(V, W)$$

es un isomorfismo de representaciones.

Demostración. (*i*) Recordemos que Φ es la transformación lineal tal que

$$\Phi(f)(v)(w) = f(v \otimes w)$$

si $f \in \hom(V \otimes W, U)$, $v \in V$ y $w \in W$. Para probar la proposición, hay que probar Φ es un morfismo de representaciones: sea $g \in G$ y mostremos que $\Phi(g \rightharpoonup f) = g \rightharpoonup \Phi(f)$ para cada $f \in \hom(V \otimes W, U)$ y, para ello, que $\Phi(g \rightharpoonup f)(v)(w) = (g \rightharpoonup \Phi(f))(v)(w)$ para cada $v \in V$ y cada $w \in W$. Esto sigue de un cálculo directo, ya que

$$\begin{aligned}\Phi(g \rightharpoonup f)(v)(w) &= (g \rightharpoonup f)(v \otimes w)\\ &= g \rightharpoonup f(g^{-1} \rightharpoonup v \otimes w)\\ &= g \rightharpoonup f((g^{-1} \rightharpoonup v) \otimes (g^{-1} \rightharpoonup w))\end{aligned}$$

y

$$\begin{aligned}(g \rightharpoonup \Phi(f))(v)(w) &= \big(g \rightharpoonup \Phi(f)(g^{-1} \rightharpoonup v)\big)(w)\\ &= g \rightharpoonup \Phi(f)(g^{-1} \rightharpoonup v)(g^{-1} \rightharpoonup w)\\ &= g \rightharpoonup f\big((g^{-1} \rightharpoonup v) \otimes (g^{-1} \rightharpoonup w)\big)\end{aligned}$$

(*ii*) La aplicación Ψ es tal que

$$\Psi(f \otimes w)(v) = (f \mid v)w$$

para cada $f \in V'$, cada $v \in V$ y cada $w \in W$. Para ver que se trata de un isomorfismo de representaciones basta mostrar que es un morfismo, ya que sabemos que es biyectiva, y para ello hay que probar que $\Psi(g \rightharpoonup f \otimes w) = g \rightharpoonup \Psi(f \otimes w)$ para todo $g \in G$. Esta es una igualdad de elementos de $\hom(V, W)$: para verificarla, sea $v \in V$ y calculemos:

$$\begin{aligned}\Psi(g \rightharpoonup f \otimes w)(v) &= \Psi((g \rightharpoonup f) \otimes (g \rightharpoonup w))(v)\\ &= (g \rightharpoonup f \mid v)(g \rightharpoonup w)\\ &= (f \mid g^{-1} \rightharpoonup v)(g \rightharpoonup w)\\ &= g \rightharpoonup (f \mid g^{-1} \rightharpoonup v)w\\ &= g \rightharpoonup \Psi(f \otimes w)(g^{-1} \rightharpoonup v)\\ &= (g \rightharpoonup \Psi(f \otimes w))(v).\end{aligned}$$

□

Restricción

Supongamos que $H \subseteq G$ es un subgrupo y que (V, ρ_V) es una representación de G. Entonces podemos considerar la restricción $\rho_V|_H : G \to \mathrm{GL}(V)$ de ρ_V al subgrupo H, que nos da una representación $(V, \rho_V|_H)$ de H sobre V. Llamamos a $(V, \rho_V|_H)$ la *restricción* de (V, ρ_V) a H, y la escribimos $V{\downarrow_H}$. Más generalmente, si $\phi : H \to G$ es un homomorfismo de grupos y (V, ρ_V) es una representación de G, entonces hay una representación $(V, \rho_V \circ \phi)$ de G, que escribimos $\phi^*(V)$ y llamamos la *restricción de* (V, ρ) *a lo largo de* ϕ.

Notemos que si $H \subseteq G$ es un subgrupo e $\iota : H \to G$ es la inclusión, para cada representación (V, ρ_G) de G la restricción $\iota^*(V)$ de V a lo largo de ι coincide con la restricción $V{\downarrow_H}$ de V a H. Es en este sentido que la segunda construcción generaliza a la primera.

Fijemos un homomorfismo de grupos $\phi : H \to G$. Si V y W son representaciones de G, entonces es inmediato que si V y W son isomorfas, las representaciones restringidas $\phi^*(V)$ y $\phi^*(W)$ tambien son isomorfas. Por el contrario, es posible que $\phi^*(V)$ y $\phi^*(W)$ sean isomorfas a pesar de que V y W no lo sean.

Ejemplo 1.5.5. Sea $\phi : H \to G$ es el homomorfismo trivial, de manera que $\phi(h) = e_G$ para todo $h \in H$. Es fácil ver que si V y W son representaciones de G, entonces

$$\phi^*(V) \cong \phi^*(W) \iff \dim V = \dim W$$

y que, de hecho, cualquiera sea V, la representaciones restringida $\phi^*(V)$ es trivial. □

Proposición 1.5.6. *Sea $\phi : H \to G$ un homomorfismo sobreyectivo de grupos.*

(*i*) *Sean (V, ρ_V) y (W, ρ_W) representaciones de G. Si $\phi^*(V) \cong \phi^*(W)$, entonces $V \cong W$.*

(*ii*) *Sea (V, ρ_V) una representaciones de G. Entonces V es simple sii $\phi^*(V)$ es simple como representación de H.*

Demostración. □

2. Carácteres

2.1. Definición

Definición 2.1.1. Si (V, ρ) es una representación de G, el *carácter* de (V, ρ) es la función $\chi : G \to \mathbb{C}$ dada por

$$\chi(g) = \operatorname{tr} \rho(g)$$

para cada $g \in G$. Si V es simple, decimos que χ es *irreducible*. Cuando queramos enfatizar el hecho de que χ es el carácter de (V, ρ) escribiremos χ_V. Escribiremos $\mathfrak{X}(G)$ al conjunto de los carácteres irreducibles de G.

Ejemplo 2.1.2. Si (V, ρ) es una representación sobre la que G actúa trivialmente, de manera que $\rho(g) = \mathsf{id}_V$ para todo $g \in G$, entonces el carácter $\chi : G \to \mathbb{C}$ de V satisface $\chi(g) = \dim V$ para todo $g \in G$. En particular, el carácter de la representación trivial $(\mathbb{C}, \rho_{\mathsf{triv}})$ es la función constante $\mathbf{1} : g \in G \mapsto 1 \in \mathbb{C}$. □

Ejemplo 2.1.3. Sea $X = \{x_1, \dots, x_n\}$ un conjunto finito sobre el que G actúa y sea $(\mathbb{C}X, \rho)$ la correspondiente representación de G. Si $g \in G$, la matriz $\|\rho(g)\|_X = (g_{ij})$ de $\rho(g) : \mathbb{C}X \to \mathbb{C}X$ con respecto a la base ordenada $(x_1, \dots, x_n)$ tiene, para cada $i, j \in \{1, \dots, n\}$,

$$g_{ij} = \begin{cases} 1, & \text{si } g \cdot x_i = x_j; \\ 0, & \text{en caso contrario.} \end{cases}$$

Se sigue, entonces, que si $\chi : G \to \mathbb{C}$ es el carácter de $\mathbb{C}X$, entonces

$$\chi(g) = \sum_{i=1}^{n} g_{ii} = \big|\{x \in X : g \cdot x = x\}\big|$$

es la cantidad de elementos de X que g deja fijos.

Si $X = G$ y G actúa por multiplicación, de manera que la representación es la representación regular $(\mathbb{C}G, \rho_{\mathsf{reg}})$, el carácter $\chi_{\mathsf{reg}} : G \to \mathbb{C}$ está entonces dado por

$$\chi_{\mathsf{reg}}(g) = \begin{cases} |G|, & \text{si } g = e; \\ 0, & \text{en caso contrario.} \end{cases}$$ □

Ejemplo 2.1.4. Sea (V, ρ) una representación de grado 1. Hay un isomorfismo de grupos canónico $c : \mathrm{GL}(V) \to \mathbb{C}^\times$, unívocamente determinado por la condición de que sea $f = c(f)\,\mathsf{id}_V$ para todo $f \in \mathrm{GL}(V)$. Es inmediato verificar que el carácter $\chi : G \to \mathbb{C}$ de V es la composición

$$G \xrightarrow{\rho} \mathrm{GL}(V) \xrightarrow{c} \mathbb{C}^\times \hookrightarrow \mathbb{C},$$

así que podemos decir que χ "es" ρ.

Observemos que se sigue, en particular, que en este caso el carácter es una aplicación multiplicativa: esto es, que $\chi(g)\chi(h) = \chi(gh)$ para cada g, $h \in G$. Esto no es cierto en general: por ejemplo, en cuanto G no es el grupo trivial, el carácter de la representación regular $\mathbb{C}C$ calculado en el ejemplo 2.1.3 no es multiplicativo. □

Proposición 2.1.5. *Sea (V, ρ) una representación y sea $n = \dim V$ su grado.*

(*i*) *Se tiene que $\chi(1) = n$.*

(*ii*) *Si $g \in G$, es $\chi(g^{-1}) = \overline{\chi(g)}$.*

(*iii*) *Si g, $h \in G$, entonces $\chi(ghg^{-1}) = \chi(h)$ y $\chi(gh) = \chi(hg)$.*

Demostración. □

Proposición 2.1.6. *Si (V, ρ_V) y (W, ρ_W) son representaciones y $\phi : V \to W$ es un isomorfismo de representaciones, entonces $\chi_V = \chi_W$.*

Demostración. □

Sea $\mathbb{C}(G)$ el espacio vectorial de las funciones $G \to \mathbb{C}$. Se trata de hecho de una $\mathbb{C}$-álgebra: si χ_1, $\chi_2 \in \mathbb{C}(G)$, el producto $\chi_1 \cdot \chi_2 : G \to \mathbb{C}$ es la función tal que $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g)$ para cada $g \in G$. Si $\chi \in \mathbb{C}(G)$, definimos una nueva función $\chi^* : G \to \mathbb{C}$ de manera que se tenga $\chi^*(g) = \chi(g^{-1})$ para todo $g \in G$.

Proposición 2.1.7. *Sean (V, ρ_V) y (W, ρ_W) dos representaciones y sean χ_V y χ_W sus carácteres. Entonces*

(*i*) $\chi_{V \oplus W} = \chi_V + \chi_W$,

(*ii*) $\chi_{V \otimes W} = \chi_V \cdot \chi_W$,

(*iii*) $\chi_{V^*} = \chi_V^*$; *y*

(*iv*) $\chi_{\hom(V,W)} = \chi_V^* \cdot \chi_W$.

Demostración. □

2.2. El producto interno

Definimos sobre el espacio vectorial $\mathbb{C}(G)$ definimos un producto interno $\langle -, - \rangle$ poniendo, para cada par de funciones χ_1, $\chi_2 \in \mathbb{C}(G)$,

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)}.$$

La verificación de que esto define en efecto un producto interno es inmediata.

Definición 2.2.1. Una función $f : G \to \mathbb{C}$ es *central* si para todo g, $h \in G$ es

$$f(ghg^{-1}) = f(g).$$

Escribimos $\mathcal{Z}(G)$ al subconjunto de $\mathbb{C}(G)$ de las funciones centrales.

De hecho, es fácil ver que $\mathcal{Z}(G)$ es un subespacio vectorial y un subanillo de $\mathbb{C}(G)$. La Proposición 2.1.5(*iii*) nos provee ejemplos de elementos de $\mathcal{Z}(G)$: en efecto, afirma que el carácter de toda representación de G es central.

Considaremos a $\mathcal{Z}(G)$ como un espacio con producto interno obtenido por restricción del de $\mathbb{C}(G)$. Si $\chi \in \mathbb{C}(G)$ es el carácter de una representación, la Proposicion 2.1.5(*ii*) nos dice que $\overline{\chi(g)} = \chi(g^{-1})$ para todo $g \in G$: al calcular productos internos de carácteres en lo que sigue, usaremos esto implícitamente. Por otro lado, la siguiente observación es frecuentemente útil:

Lema 2.2.2. *Sean c_1, ..., c_k las clases de conjugación de G y sean g_1, ..., $g_k \in G$ tales que $g_i \in c_i$ para cada $i \in \{1, \dots, k\}$. Si χ_1, $\chi_2 \in \mathcal{Z}(G)$ son funciones centrales, entonces*

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{j=1}^{k} |c_j| \chi_1(g_j)\overline{\chi_2(g_j)}.$$

Demostración. Como las clases de conjugación de G determinan una partición de G, es

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \frac{1}{|G|} \sum_{j=1}^{k} \sum_{g \in c_j} \chi_1(g)\overline{\chi_2(g)},$$

y como χ_1 y χ_2 son centrales, para todo $j \in \{1, \dots, k\}$ es $\chi_1(g) = \chi_1(g_j)$ y $\chi_2(g) = \chi_2(g_j)$ para cada $g \in c_j$, de manera que

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{j=1}^{k} |c_j| \chi_1(g_j)\overline{\chi_2(g_j)},$$

como afirma el enunciado. □

2.3. Relaciones de ortogonalidad entre carácteres

Proposición 2.3.1. *Si χ_1 y χ_2 son los carácteres de dos representaciones simples no isomorfas, entonces $\langle \chi_1, \chi_2 \rangle = 0$. Además, cualquiera sea $g \in G$ se tiene que*

$$\sum_{h \in G} \chi_1(gh^{-1})\chi_2(h) = 0. \tag{3}$$

Demostración. Sean (V, ρ_V) y (W, ρ_W) representaciones tales que sus carácteres sean χ_1 y χ_2, de grados n y m, respectivamente. Sea $\mathscr{B}$ y $\mathscr{B}'$ bases ordenadas de V y V', y sean $r = (\rho_V)_{\mathscr{B}} : G \to \mathrm{GL}(n, \mathbb{C})$ y $s = (\rho_W)_{\mathscr{B}'} : G \to \mathrm{GL}(m, \mathbb{C})$ las representaciones matriciales correspondientes.

Sea $f : V \to W$ es una función lineal y sea $\hat{f} : V \to W$ la función construida en el Lema 1.4.4, que es un morfismo de representaciones. Por hipótesis, V y W son no isomorfas, así que el Lema de Schur 1.3.9 implica que

$$\hat{f} = \frac{1}{|G|} \sum_{g \in G} \rho_W(g) \circ f \circ \rho_V(g^{-1}) = 0.$$

Si (f_{ij}) es la matriz de f con respecto a las bases $\mathscr{B}$ y $\mathscr{B}'$, esta igualdad nos dice que para todo $i \in \{1, \ldots, m\}$ y todo $j \in \{1, \ldots, n\}$ es

$$\sum_{\substack{g \in G \\ 1 \leq k \leq m \\ 1 \leq l \leq n}} s_{ik}(g) f_{kl} r_{lj}(g^{-1}) = 0.$$

Ahora bien, esto es cierto cualquiera sea f, así que podemos concluir, de hecho, que para todo i, $k \in \{1, \ldots, m\}$ y todo j, $l \in \{1, \ldots, n\}$ es

$$\sum_{g \in G} s_{ik}(g) r_{lj}(g^{-1}) = 0. \tag{4}$$

En particular,

$$\begin{aligned}
\langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} \Big(\sum_{1 \leq i \leq n} r_{ii}(g) \Big) \Big(\sum_{1 \leq j \leq m} \overline{s_{jj}(g)} \Big) \\
&= \frac{1}{|G|} \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \Big(\sum_{g \in G} r_{ii}(g) s_{jj}(g^{-1}) \Big) \\
&= 0.
\end{aligned}$$

Esto prueba la primera parte de la proposición. Para ver la segunda, calculamos que

$$\begin{aligned}
\sum_{h \in G} \chi_1(gh^{-1}) \chi_2(h) &= \sum_{h \in G} \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} r_{ii}(gh^{-1}) s_{jj}(h) \\
&= \sum_{h \in G} \sum_{\substack{1 \leq i,k \leq n \\ 1 \leq j \leq m}} r_{ik}(g) r_{ki}(h^{-1}) s_{jj}(h) \\
&= \sum_{\substack{1 \leq i,k \leq n \\ 1 \leq j \leq m}} \Big(\sum_{h \in G} s_{jj}(h) r_{ki}(h^{-1}) \Big) r_{ik}(g) \\
&= 0
\end{aligned}$$

en vista de (4) □

Proposición 2.3.2. *Si χ es un carácter irreducible, entonces $\langle \chi, \chi \rangle = 1$. Si n es el grado de χ, entonces para cada $g \in G$ tenemos que*

$$\sum_{h \in G} \chi(gh^{-1})\chi(h) = \frac{|G|}{n}\chi(g). \tag{5}$$

Demostración. Sean (V, ρ_V) una representación tal que su carácter es χ_1 y sea n su grado. Sea $\mathscr{B}$ una base ordenada de V, y sean $r = (\rho_V)_{\mathscr{B}} : G \to \mathrm{GL}(n, \mathbb{C})$ la representación matricial correspondiente.

Si $f : V \to V$ es una aplicación lineal, entonces, como en la prueba de la proposición anterior, la aplicación $\hat{f} : V \to V$ es un endomorfismo de representaciones, así que —por el Lema de Schur— existe $\lambda \in \mathbb{C}$ tal que $\hat{f} = \lambda \,\mathsf{id}_V$. Usando la última afirmación del Lema 1.4.4, vemos que $\lambda n = \operatorname{tr} \hat{f} = \operatorname{tr} f$, de forma que $\lambda = \frac{1}{n} \operatorname{tr} f$, así que en definitiva es

$$\hat{f} = \frac{1}{|G|} \sum_{g \in G} \rho_V(g) \circ f \circ \rho_V(g^{-1}) = \frac{1}{n} \operatorname{tr} f \,\mathsf{id}_V.$$

Si (f_{ij}) es la matriz de f con respecto a la base $\mathscr{B}$, esta igualdad implica que para cada i, $j \in \{1, \dots, n\}$ es

$$\frac{1}{|G|} \sum_{\substack{g \in G \\ 1 \leq k, l \leq n}} r_{ik}(g) f_{kl} r_{lj}(g^{-1}) = \frac{1}{n} \operatorname{tr} f \, \delta_{ij}.$$

La arbitrariedad de f nos permite concluir que si i, j, k, $l \in \{1, \dots, n\}$ es

$$\frac{1}{|G|} \sum_{g \in G} r_{ik}(g) r_{lj}(g^{-1}) = \frac{1}{n} \delta_{kl} \delta_{ij}, \tag{6}$$

y entonces

$$\begin{aligned}
\langle \chi, \chi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi(g^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \Big(\sum_{1 \leq i \leq n} r_{ii}(g) \Big) \Big(\sum_{1 \leq j \leq n} r_{jj}(g^{-1}) \Big) \\
&= \sum_{1 \leq i, j \leq n} \frac{1}{|G|} r_{ii}(g) r_{jj}(g^{-1}) \\
&= \sum_{1 \leq i, j \leq n} \frac{1}{n} \delta_{ij} \delta_{ij} \\
&= 1.
\end{aligned}$$

Por otro lado, si $g \in G$ es

$$\begin{aligned}
\sum_{h \in G} \chi(gh^{-1})\chi(h) &= \sum_{h \in G} \sum_{1 \leq i, j \leq n} r_{ii}(gh^{-1}) r_{jj}(h) \\
&= \sum_{h \in G} \sum_{1 \leq i, j, k \leq n} r_{ik}(g) r_{ki}(h^{-1}) r_j j(h) \\
&= \sum_{1 \leq i, j, k \leq n} \Big(\sum_{h \in G} r_{jj}(h) r_{ki}(h^{-1}) \Big) r_{ik}(g)
\end{aligned}$$

y usando (6), esto queda

$$\begin{aligned} &= \sum_{1\le i,j,k\le n} \frac{|G|}{n}\delta_{jk}\delta_{ji}r_{ik}(g) \\ &= \frac{|G|}{n}\sum_{1\le j\le n} r_{jj}(g) \\ &= \frac{|G|}{n}\chi(g). \end{aligned}$$

□

2.4. Aplicaciones

Teorema 2.4.1. *Sea (V,ρ_V) una representación y sea χ_V su carácter. Supongamos que W_1, …, W_s son subrepresentaciones de V tales que $V = W_1 \oplus \cdots \oplus W_s$ y sean χ_{W_1}, …, χ_{W_s} sus respectivos carácteres. Si U es una representación simple de carácteres χ_U, entonces*

$$\langle \chi_V, \chi_U\rangle = \Big|\big\{i \in \{1,\dots,s\} : U \cong W_i\big\}\Big|.$$

Demostración. Sea U una representación simple. Sea $i \in \{1,\dots,s\}$. Si $U \ncong W_i$, la Proposición 2.3.1 nos dice que $\langle \chi_{W_i}, \chi_U\rangle = 0$. Si, por el contrario, $U \cong W_i$, entonces $\chi_U = \chi_{W_i}$ y la Proposición 2.3.2 nos dice que $\langle \chi_{W_i}, \chi_U\rangle = 1$.

De acuerdo a la Proposición 2.1.7(i), es $\chi_V = \sum_{i=1}^{s} \chi_{U_i}$, y entonces

$$\langle \chi_V, \chi_U\rangle = \sum_{i=1}^{s} \langle \chi_{W_i}, \chi_U\rangle = \Big|\big\{i \in \{1,\dots,s\} : U \cong W_i\big\}\Big|.$$

□

Definición 2.4.2. Sea V una representación y sean W_1, …, W_s subrepresentaciones de V tales que $V = W_1 \oplus \cdots \oplus W_s$. Si U es una representación simple, la *multiplicidad de U en V* es el número

$$[V : U] = \Big|\big\{i \in \{1,\dots,s\} : U \cong W_i\big\}\Big|.$$

Si $[V : U] > 0$, decimos que U *aparece* en V.

Corolario 2.4.3. *Sea (V,ρ_V) una representación. Supongamos que W_1, …, W_s y W_1', …, W_t' son subrepresentaciones de V tales que $V = W_1 \oplus \cdots \oplus W_s = W_1' \oplus \cdots \oplus W_t'$. Entonces $s = t$ y, si U es una representación simple,*

$$\Big|\big\{i \in \{1,\dots,s\} : U \cong W_i\big\}\Big| = \Big|\big\{i \in \{1,\dots,t\} : U \cong W_i'\big\}\Big|.$$

Demostración. □

Corolario 2.4.4. *Sea (V,ρ_V) una representación y sea χ_V su carácter. Entonces V es simple si y solamente si $\langle \chi_V, \chi_V\rangle = 1$.*

Demostración. □

Corolario 2.4.5. *Sean (V,ρ_V) y (W,ρ_W) dos representaciones y sean χ_V y χ_W sus carácteres. Entonces V y W son isomorfas si y solamente si $\chi_V = \chi_W$.*

Demostración. □

Corolario 2.4.6. *Sea χ_{triv} el carácter de la representación trivial y sean V y W dos representaciones. Entonces*

$$\dim V^G = \langle \chi_V, \chi_{\mathsf{triv}} \rangle$$

y

$$\dim \hom_G(V, W) = \langle \chi_V, \chi_W \rangle.$$

Demostración. □

Proposición 2.4.7. *Sea $(\mathbb{C}G, \rho)$ la representación regular de G. El carácter χ de $\mathbb{C}G$ es tal que*

$$\chi(g) = \begin{cases} |G|, & \text{si } g = e; \\ 0, & \text{en caso contrario.} \end{cases}$$

Toda representación simple U aparece en $\mathbb{C}G$ con multiplicidad $[\mathbb{C}G : U] = \dim U$.

Demostración. □

Corolario 2.4.8. *Hay un número finito de clases de isomorfismo de representaciones simples. Si $U_1, \ldots, U_k$ es un conjunto completo de representantes de esas clases y si $\chi_1, \ldots, \chi_k$ y $n_1, \ldots, n_k$ son sus carácteres y grados, respectivamente, entonces*

$$\sum_{i=1}^{k} n_i^2 = |G|,$$

y el carácter χ_{reg} de la representación regular es

$$\chi_{\mathsf{reg}} = \sum_{i=1}^{k} n_i \chi_i. \tag{7}$$

Demostración. □

2.5. El número de representaciones simples

Proposición 2.5.1. *La dimensión de $\mathcal{Z}(G)$ es la cantidad de clases de conjugación de G.*

Demostración. Sea $C(G)$ el conjunto de las clases de conjugación de G y para cada $c \in C(G)$ sea $\delta_c : G \to \mathbb{C}$ la función tal que para cada $g \in G$ es

$$\delta_c(g) = \begin{cases} 1, & \text{si } g \in c; \\ 0, & \text{en caso contrario.} \end{cases}$$

Se sigue inmediatamente de esta definición que $\delta_c \in \mathcal{Z}(G)$ cualquiera sea $c \in C(G)$ y que el conjunto $\Delta = \{\delta_c : c \in C(G)\}$ es linealmente independiente en $C(G)$.

Sea $f \in C(G)$. Si $c \in C(G)$ y g, $g' \in c$, entonces existe $h \in G$ tal que $g' = hgh^{-1}$ y entonces $f(g') = f(hgh^{-1}) = f(g)$. Vemos así que f es constante sobre cada clase de conjugación de G y, usando esto, que si si para cada $c \in C(G)$ elegimos un elemento $g_c \in c$, entonces $f = \sum_{c \in C(G)} f(g_c)\delta_c$. Esto prueba que el conjunto Δ genera a $C(G)$, así que se trata, en definitiva, de una base de $C(G)$.

Concluimos que $\dim \mathcal{Z}(G) = |C(G)|$, lo que prueba la proposición. □

Si $f \in \mathcal{Z}(G)$ y (V, ρ_V) es una representación, definimos la aplicación lineal

$$\rho_V^f = \sum_{h \in G} f(h)\rho_V(h) : V \to V$$

Lema 2.5.2. *Sea $f \in \mathcal{Z}(G)$.*

(*i*) *Si (V, ρ_V) y (W, ρ_W) son dos representaciones de G y si $(V \oplus W, \rho_{V\oplus W})$ es su suma directa, entonces*

$$\rho_{V\oplus W}^f = \begin{pmatrix} \rho_V^f & 0 \\ 0 & \rho_W^f \end{pmatrix}.$$

(*ii*) *Sea (V, ρ_V) una representación simple de grado n y carácter χ_V. Entonces $\rho_V^f = \nu\, \mathsf{id}_V$ con $\nu = \frac{|G|}{n}\langle f, \chi_V^*\rangle$, .*

Demostración. La parte (i) es inmediata. Veamos (ii).

La aplicación ρ_f es un morfismo de representaciones. En efecto, si $g \in G$ tenemos que

$$\begin{aligned} \rho_V^f \circ \rho_V(g) &= \sum_{h \in G} f(h)\rho_V(h) \circ \rho_V(g) \\ &= \sum_{h \in G} f(h)\rho_V(hg) \end{aligned}$$

y, cambiando la variable h por $k = g^{-1}hg$, esto es

$$= \sum_{k \in G} f(gkg^{-1})\rho_V(gk)$$

que, como f es central, es lo mismo que

$$\begin{aligned} &= \sum_{k \in G} f(k)\rho_V(g) \circ \rho_V(k) \\ &= \rho_V(g) \circ \rho_V^f. \end{aligned}$$

El Lema de Schur 1.3.9 implica que existe $\nu \in \mathbb{C}$ tal que $f = \nu\, \mathsf{id}_V$ y, de hecho, es

$$\nu = \frac{1}{n} \operatorname{tr} f = \frac{1}{n} \sum_{h \in G} f(h) \operatorname{tr} \rho_V(h) = \frac{1}{n} \sum_{h \in G} f(h)\chi(h) = \frac{|G|}{n}\langle f, \chi^*\rangle. \qquad \square$$

Teorema 2.5.3. *El conjunto de los carácteres irreducibles es una base ortonormal de $\mathcal{Z}(G)$.*

Demostración. Sea $\mathfrak{X} \subset \mathcal{Z}(G)$ el conjunto de los carácteres irreducibles. De las Proposiciones 2.3.1 y 2.3.2 sabemos que $\mathfrak{X}$ es un conjunto ortonormal, así que para probar el teorema alcanza con mostrar que si $f \in \mathcal{Z}(G)$ entonces

$$\forall \chi \in \mathfrak{X},\ \langle f, \chi\rangle = 0 \implies f = 0.$$

Sea entonces $f \in \mathcal{Z}(G)$ y supongamos que $\langle f, \chi\rangle = 0$ para todo $\chi \in \mathfrak{X}$. Si (V, ρ) es una representación simple y χ es su carácter, entonces χ^* es el carácter de V' que, según la Proposición 1.5.3 también es simple, así que $\chi^* \in \mathfrak{X}$ y $\langle f, \chi^*\rangle = 0$: de acuerdo al Lema 2.5.2(ii), entonces, tenemos que $\rho_V^f = 0$. Se sigue de esto —usando el Teorema 1.4.6 y el Lema 2.5.2(i)— que, de hecho, $\rho_V^f = 0$ para *cualquier* representación (V, ρ).

En particular, si $(\mathbb{C}G, \rho_{\mathsf{reg}})$ es la representación regular entonces $\rho^f_{\mathsf{reg}} = 0$ y, en consecuencia,

$$\rho^f_{\mathsf{reg}}(e) = \sum_{h\in G} f(h)\rho(h)(e) = \sum_{h\in G} f(h)h = 0.$$

Como G es una base de $\mathbb{C}G$, se sigue inmediatamente de esto que $f = 0$, como queríamos. □

Corolario 2.5.4. *Hay tantas representaciones simples como clases de conjugación en G.*

Demostración. Esto es consecuencia inmediata del Teorema, en vista de la Proposición 2.5.1. □

2.6. Componentes isotípicas de una representación

Proposición 2.6.1. *Sean (V_1, ρ_1), …, (V_k, ρ_k) representantes de las clases de isomorfismo de representaciones simples, sean χ_1, …, χ_k y n_1, …, n_k sus carácteres y sus grados, respectivamente, y sea (W, ρ) una representación. Para cada $i \in \{1, \dots, k\}$, sea $W_i \subseteq V$ la suma de todos las subrepresentaciones de V isomorfas a V_i. Entonces W_1, …, W_k son subrepresentaciones de W y $W = W_1 \oplus \cdots \oplus W_k$. Más aún, el proyector de W sobre el sumando i-ésimo de está descomposición es*

$$p_i = \frac{n_i}{|G|} \sum_{h\in G} \chi_i(h^{-1})\rho(h) : W \to W.$$

En particular, un elemento $w \in W$ pertenece a W_i si y solamente si es

$$w = \frac{n_i}{|G|} \sum_{h\in G} \chi_i(h^{-1})\rho(h)(w).$$

Demostración. Es claro que cada una de W_1, …, W_k es una subrepresentación de W, así que solo tenemos que probar las dos últimas afirmaciones. Supongamos por un instante que

- (i) p_i es un endomorfismo de representaciones para cada $i \in \{1, \dots, k\}$;
- (ii) $\sum_{i=1}^k p_i = \mathsf{id}_W$;
- (iii) $p_i \circ p_j = 0$ si $i, j \in \{1, \dots, k\}$ e $i \neq j$;
- (iv) $p_i \circ p_i = p_i$ para cada $i \in \{1, \dots, k\}$; y
- (v) $p_i(W) = W_i$ para cada $i \in \{1, \dots, k\}$.

Entonces:

- Es $W = \sum_{i=1}^k W_i$. En efecto, si $w \in W$, (ii) implica que $w = \sum_{i=1}^k p_i(w)$ y, como (v) nos dice que $p_i(w) \in W_i$, esto muestra que $w \in \sum_{i=1}^k W_i$.
- Por otro lado, para cada $i \in \{1, \dots, k\}$ es $W_i \cap \sum_{j\neq i} W_j = 0$. Para verlo, supongamos que $w \in W$ pertenece a esa intersección, de manera que por (v) existen w_1, …, $w_k \in W$ tales que $w = p_i(w_i) = \sum_{j\neq i} p_j(w_j)$. Entonces usando (iii) y (iv), tenemos que $w = p_i(w_i) = p_i(p_i(w_i)) = p_i(\sum_{j\neq i} p_j(w_j)) = 0$.

En definitiva, podemos concluir así que $W = W_1 \oplus \cdots \oplus W_k$ y que p_i es el i-ésimo proyector de esta descomposición.

Resta entonces verificar (i)–(v). Para ver (ii), observemos que

$$\sum_{i=1}^{k} p_i = \sum_{i=1}^{k} \frac{n_i}{|G|} \sum_{h\in G} \chi_i(h^{-1})\rho(h) = \frac{1}{|G|} \sum_{h\in G} \Big(\sum_{i=1}^{k} n_i \chi_i(h^{-1}) \Big) \rho(h)$$

y que, de acuerdo a la igualdad (7) del Lema 2.4.8, la suma interior es igual a $\chi_{\mathsf{reg}}(h^{-1})$, así que

$$\sum_{i=1}^{k} p_i = \frac{1}{|G|} \sum_{h\in G} \chi_{\mathsf{reg}}(h^{-1})\rho(h) = \frac{1}{|G|} \chi_{\mathsf{reg}}(e)\rho(e) = \mathsf{id}_W.$$

Para ver (iii), sean i, $j \in \{1, \dots, k\}$ tales que $i \neq j$: tenemos que

$$\begin{aligned}
p_i \circ p_j &= \frac{n_i n_j}{|G|^2} \sum_{h,h'\in G} \chi_i(h^{-1})\chi_j(h'^{-1})\rho(h) \circ \rho(h') \\
&= \frac{n_i n_j}{|G|^2} \sum_{h,h'\in G} \chi_i(h^{-1})\chi_j(h'^{-1})\rho(hh') \\
&= \frac{n_i n_j}{|G|^2} \sum_{g\in G} \Big(\sum_{\substack{h,h'\in G \\ hh'=g}} \chi_i(h^{-1})\chi_j(h'^{-1}) \Big) \rho(g) \\
&= \frac{n_i n_j}{|G|^2} \sum_{g\in G} \Big(\sum_{h\in G} \chi_j(g^{-1}h)\chi_i(h^{-1}) \Big) \rho(g) \\
&= 0
\end{aligned}$$

en vista de la relación (3) de la Proposicion 2.3.1. De manera similar, si $i \in \{1, \dots, k\}$, entonces

$$\begin{aligned}
p_i \circ p_i &= \frac{n_i^2}{|G|^2} \sum_{h,h'\in G} \chi_i(h^{-1})\chi_i(h'^{-1})\rho(h) \circ \rho(h') \\
&= \frac{n_i^2}{|G|^2} \sum_{h,h'\in G} \chi_i(h^{-1})\chi_i(h'^{-1})\rho(hh') \\
&= \frac{n_i^2}{|G|^2} \sum_{g\in G} \Big(\sum_{\substack{h,h'\in G \\ hh'=g}} \chi_i(h^{-1})\chi_i(h'^{-1}) \Big) \rho(g) \\
&= \frac{n_i^2}{|G|^2} \sum_{g\in G} \Big(\sum_{h\in G} \chi_i(g^{-1}h)\chi_i(h^{-1}) \Big) \rho(g) \\
&= \frac{n_i^2}{|G|^2} \sum_{g\in G} \frac{|G|}{n_i} \chi_i(g^{-1})\rho(g) \\
&= p_i
\end{aligned}$$

usando ahora la igualdad (5) de la Proposición 2.3.2: esto prueba (iv).

Finalemente, verifiquemos (v). Sea $i \in \{1, \dots, k\}$. Supongamos que $U \subseteq W$ es una subrepresentación simple y sea χ_U su carácter. Es $\rho(h)(U) \subseteq U$ para todo $h \in G$, así que $p_i(U) \subseteq U$ y podemos entonces considerar la restricción $p_i|_U : U \to U$. Como p_i es un endomorfismo de representaciones, el Lema de Schur nos dice que existe $\lambda_U \in \mathbb{C}$ tal que $p_i|_U = \lambda_U \, \mathsf{id}_U$ y entonces

$$\lambda_U \, \dim U = \operatorname{tr} p_i|_{U_i}$$

$$\begin{aligned}
&= \frac{n_i}{|G|}\sum_{h\in G}\chi_i(h^{-1})\operatorname{tr}\rho(h)|_U \\
&= \frac{n_i}{|G|}\sum_{h\in G}\chi_i(h^{-1})\chi_U(h) \\
&= n_i\langle\chi_i,\chi_U\rangle \\
&= \begin{cases} n_i, & \text{si } U\cong V_i; \\ 0, & \text{en caso contrario.}\end{cases}
\end{aligned}$$

Así, vemos que

$$\lambda_U = \begin{cases} 1, & \text{si } U\cong V_i; \\ 0, & \text{en caso contrario}\end{cases}$$

y, en consecuencia, que

$$p_i(U) = \begin{cases} U, & \text{si } U\cong V_i; \\ 0, & \text{en caso contrario.}\end{cases}$$

Esto nos dice que toda subrepresentación simple de W isomorfa a V_i está contenida en la imágen de p_i y se sigue que $W_i \subseteq p_i(W)$.

Por otro lado, sabemos que existen subrepresentaciones simples $U_1, \ldots, U_r \subseteq W$ tales que $W = U_1 \oplus \cdots \oplus U_r$ y, sin pérdida de generalidad podemos suponer que existe $s \in \{0, \ldots, r\}$ tal que $U_j \cong V_i$ si $1 \leq i \leq s$ y que $U_j \ncong V_i$ si $s < j \leq r$. En consecuencia,

$$p_i(W) \subseteq \sum_{j=1}^{r} p_i(U_j) = \sum_{j=1}^{s} p_i(U_j) = \sum_{j=1}^{s} U_j \subseteq W_i$$

Esto termina la prueba de (v) y, entonces, de la proposición. □

Definición 2.6.2. Sea (W, ρ_W) una representación de G y sea (V, ρ_V) una representación simple de G. La *componente* (V,ρ)*-isotípica* de W es el subespacio $W_{V,\rho_V)}$ de W suma de todas las subrepresentaciones de W isomorfas a V. Si χ es el carácter de (V,ρ), también llamamos a $W_{(V,\rho)}$ la *componente* χ*-isotípica*, y la escribimos en ese caso W_χ.

De acuerdo a la Proposición 2.6.1, si (W, ρ_W) es una representación, las componentes isotípicas de W son subrepresentaciones y se tiene

$$W = \bigoplus_{\chi\in\mathfrak{X}(G)} W_\chi.$$

A diferencia de la descomposición de W como suma directa de subrepresentaciones simples, esta descomposición es canónica y es respetada por todos los morfismos de representaciones:

Proposición 2.6.3. *Sean (W, ρ_W) y $(W', \rho_{W'})$ representaciones de G y sea $\chi \in \mathfrak{X}(G)$. Si $f : W \to W'$ es un morfismo de representaciones, entonces $f(W_\chi) \subseteq W'_\chi$ para todo $\chi \in \mathfrak{X}(G)$.*

Demostración. Sea n el grado de χ. De la Proposición 2.6.1 se sigue que un elemento $w \in W$ pertenece a W_χ si y solamente si

$$w = \frac{n}{|G|}\sum_{h\in G}\chi(h^{-1})\rho_W(h)(w).$$

Si ese es el caso, entonces

$$f(w) = \frac{n}{|G|}\sum_{h\in G}\chi(h^{-1})f(\rho_W(h)(w)) = \frac{n}{|G|}\sum_{h\in G}\chi(h^{-1})\rho_{W'}(h)(f(w)),$$

así que, por la misma razón, $f(w) \in W'_\chi$. □

2.7. Representaciones de grado 1

Es fácil describir todas las representaciones de grado 1 de un grupo:

Proposición 2.7.1. *Escribamos $\xi : \mathbb{C}^\times \to \mathrm{GL}(\mathbb{C})$ al isomorfismo tal que $\xi(\lambda) = \lambda\,\mathsf{id}_{\mathbb{C}}$ para cada $\lambda \in \mathbb{C}^\times$.*

- (*i*) *Si $\chi : G \to \mathbb{C}^\times$ es un homomorfismo de grupos, hay una representación $(\mathbb{C}_\chi, \rho_\chi)$ con espacio vectorial subyacente $\mathbb{C}_\chi = \mathbb{C}$ y $\rho_\chi = \xi \circ \chi : G \to \mathrm{GL}(\mathbb{C}_\chi)$. El carácter de $(\mathbb{C}_\chi, \rho_\chi)$ es la composición $G \xrightarrow{\chi} \mathbb{C}^\times \hookrightarrow \mathbb{C}$, que identificaremos en lo que sigue con χ.*
- (*ii*) *Si (V, ρ) es una representación de G de grado 1, existe exactamente un homomorfismo de grupos $\chi : G \to \mathbb{C}^\times$ tal que $V \cong \mathbb{C}_\chi$.*

En consecuencia, el conjunto $\{(\mathbb{C}_\chi, \rho_\chi) : \chi \in \hom_{\mathsf{Grp}}(G, \mathbb{C}^\times)\}$ es un sistema completo de representantes de las clases de isomorfismo de representaciones de grado 1 de G.

Demostración. Solamente (*ii*) requiere una prueba. Sea (V, ρ_V) una representación de grado 1 y sea $v_0 \in V \setminus 0$. Para cada $g \in G$ existe un escalar $\chi(g) \in \mathbb{C}$ tal que $\rho_V(g)(v_0) = \chi(g)v_0$, y como $\rho_V(g) \in \mathrm{GL}(V)$, es $\chi(g) \neq 0$. Tenemos entonces una función $\chi : G \to \mathbb{C}^\times$. Como ρ_V es un morfismo de grupos, si g, $h \in G$ es

$$\chi(gh)v_0 = \rho_V(gh)(v_0) = \rho_V(g)(\rho_V(h)(v_0)) = \chi(h)\rho_V(g)(v_0) = \chi(g)\chi(h)v_0$$

y, como $v_0 \neq 0$, esto implica que $\chi(gh) = \chi(g)\chi(h)$. Vemos así que χ es un homomorfismo de grupos. Consideremos finalmente la aplicación lineal $f : \lambda \in \mathbb{C}_\chi \mapsto \lambda v_0 \in V$. Se trata de un isomorfismo de representaciones: es claro que es biyectiva, y si $g \in G$ se tiene que

$$f(\rho_\chi(g)(\lambda)) = f(\chi(g)\lambda) = \chi(g)\lambda v_0 = \chi(g)f(\lambda) = \rho_\chi(g)(f(\lambda)).$$

Para terminar, sean χ, $\chi' : G \to \mathbb{C}^\times$ dos homomorfismos distintos tales que existe un isomorfismo $f : \mathbb{C}_\chi \to \mathbb{C}_{\chi'}$. Entonces para cada $g \in G$ es

$$\chi(g)f(1) = f(\chi(g)(1)) = f(\rho_\chi(g)(1)) = \rho_{\chi'}(g)(f(1)) = \chi'(g)f(1)$$

y, como $f(1) \neq 0$ porque f es un isomorfismo, vemos que $\chi(g) = \chi'(g)$. Así, debe ser $\chi = \chi'$: esto prueba la únicidad que se afirma en (*ii*). □

Corolario 2.7.2. *Sea (V, ρ) una representación de G y sea $\chi : G \to \mathbb{C}^\times$ un homomorfismos de grupo. La componente χ-isotípica de V es*

$$V_\chi = \{v \in V : \rho(g)(v) = \chi(g)v \text{ para todo } g \in G\}.$$

Demostración. Notemos U al miembro derecho de la igualdad que queremos probar. Si $v \in U$, entonces

$$\begin{aligned}\frac{1}{|G|}\sum_{h\in G}\chi(h^{-1})\rho(h)(v) &= \frac{1}{|G|}\sum_{h\in G}\chi(h^{-1})\chi(h)v\\ &= \frac{1}{|G|}\sum_{h\in G}\chi(e)v\\ &= v,\end{aligned}$$

así que, de acuerdo a la Proposición 2.6.1, $v \in W_\chi$.

Recíprocamente, si $v \in W_\chi$, entonces $v = \frac{1}{|G|}\sum_{h\in G}\chi(h^{-1})\rho(h)(v)$ y para cada $g \in G$ es

$$\begin{aligned}\rho(g)(v) &= \frac{1}{|G|}\sum_{h\in G}\chi(h^{-1})\rho(g)\rho(h)(v)\\ &= \frac{1}{|G|}\sum_{h\in G}\chi(h^{-1})\rho(gh)(v)\\ &= \frac{1}{|G|}\sum_{h\in G}\chi(h^{-1}g)\rho(h)(v)\\ &= \chi(g)\frac{1}{|G|}\sum_{h\in G}\chi(h^{-1})\rho(h)(v)\\ &= \chi(g)v.\end{aligned}$$

Esto muestra que $v \in U$. □

Proposición 2.7.3. *Sea G un grupo de orden n. Entonces G es abeliano si y solamente si todas sus representaciones simples son de grado 1, y en ese caso posee exactamente n representaciones simples.*

Demostración. Si G es abeliano, cada una de las clases de conjugación de G tiene exactamente un elemento y, en consecuencia, hay n de ellas. El Teorema 2.5.3 implica que hay entonces n representaciones simples. Si $n_1, \ldots, n_n$ son sus grados, entonces $\sum_{i=1}^n n_i^2 = n$, como en el Corolario 2.4.8. Como por supuesto $n_i \geq 1$ para todo $i \in \{1, \ldots, n\}$, es claro que debe ser $n_1 = \cdots = n_n = 1$.

Recíprocamente, si G es tal que los grados $n_1, \ldots, n_r$ de sus representaciones simples son todos 1, del Corolario 2.4.8 sabemos que $r = \sum_{i=1}^r n_i^2 = n$ y entonces, del Teorema 2.5.3, que G tiene n clases de conjugación. Esto implica inmediatamente que cada una de éstas tiene un único elemento y, en definitiva, que G es abeliano. □

Esta proposición tiene como corolario la determinación del número de representaciones de grado 1 de un grupo finito cualquiera. Para probarlo, recordemos primero el siguiente resultado de la teoría elemental de grupos:

Lema 2.7.4. *Para cada g, $h \in G$ escribamos $[g, h] = ghg^{-1}h^{-1}$. Consideramos el conjunto $C = \{[g, h] : g, h \in G\}$ y el subgrupo $G' = \langle C\rangle$ de G generado por C.*

(*i*) *G' es un subgrupo normal de G y el cociente G/G' es abeliano.*

(*ii*) *Sea $p : G \to G/G'$ la proyección canónica. Si $f : G \to A$ es un homomorfismo de grupos con valores en un grupo abeliano A, entonces $G' \subseteq \ker f$ y, en consecuencia, existe un homomorfismo $\bar{f} : G/G' \to A$ tal que $\bar{f} \circ p = f$.*

Demostración. (i) Como $k[g,h]k^{-1} = [kgk^{-1}, khk^{-1}]$ cualesquiera sean g, h, $k \in G$, el conjunto C es invariante por conjugación. El subgrupo G' que genera en G es, en consecuencia, un subgrupo normal.

Sean a, $b \in G/G'$, de manera que existen g, $h \in G$ tales que $a = gG'$ y $b = hG'$. Como $[h^{-1}, g^{-1}] \in G'$, es

$$ab = ghG' = gh[h^{-1}, g^{-1}]G' = hgG = ba.$$

Esto muestra que el grupo cociente G/G' es abeliano.

(ii) Si g, $h \in G$, entonces $f([g,h]) = [f(g), f(h)] = e_A$ porque A es abeliano. Esto dice que $C \subseteq \ker f$, de manera que $G' = \langle C \rangle \subseteq \ker f$. La existencia de $\bar{f} : G/G' \to A$ tal que $\bar{f} \circ p = f$ es ahora inmediata. □

Corolario 2.7.5. *Un grupo G tiene $|G/G'|$ representaciones de grado 1.*

Demostración. Sea $p : G \to G/G'$ la proyección canónica y escribamos $\mathscr{L}(G)$ y $\mathscr{L}(G/G')$ a los conjuntos de clases de isomorfismo de representaciones de grado 1 de G y de G/G'.

Si V es una representación de G/G' de grado 1, entonces la restricción $p^*(V)$ de V a lo largo de p es una representación de G de grado 1. Además, si V y W son representaciones de G/G' de grado 1, se tiene que $V \cong W$ sii $p^*(V) \cong p^*(W)$: esto sigue de la Proposición 1.5.6(i) porque p es sobreyectiva. Esto implica que podemos definir una función $\pi : \mathscr{L}(G/G') \to \mathscr{L}(G)$ poniendo $\pi([V]) = [p^*(V)]$ para cada representación V de G/G' de grado 1 y que, de hecho, esta función resulta inyectiva. Como la Proposición 2.7.3 nos dice que $|\mathscr{L}(G/G')| = |G/G'|$, para probar la proposición bastará mostrar que π es sobreyectiva.

Sea entonces (V, ρ_V) una representación de G de grado 1. Como $\dim V = 1$, el grupo $\mathrm{GL}(V)$ es abeliano, así que, aplicando la Proposición 2.7.4(ii) al homomorfismo $\rho_V : G \to \mathrm{GL}(V)$, podemos concluir que existe un homomorfismo $\bar{\rho}_V : G/G' \to \mathrm{GL}(V)$ tal que $\bar{\rho}_V \circ p = \rho_V$. Tenemos entonces una representación $(V, \bar{\rho}_V)$ de G/G' sobre V y la representación $p^*(V, \bar{\rho}_V)$ que se obtiene restringiéndola a lo largo de p es precisamente (V, ρ_V). Concluímos de esta manera que $\pi([(V, \bar{\rho}_V)]) = [(V, \rho_C)]$ y, en definitiva, que π es sobreyectiva, como queríamos. □

Proposición 2.7.6. *Sea $A \subseteq G$ un subgrupo abeliano de G. El grado de cada representación simple de G es menor o igual al índice $[G : A]$ de A en G.*

Demostración. Sea V una representación simple de G. Sea $L \subseteq V$ un subespacio que es una subrepresentación simple de la restricción $V{\downarrow_A}$. Como A es abeliano, debe ser $\dim L = 1$, así que existe $v \in L \setminus 0$ tal que $L = \langle v \rangle$ y, en particular, para cada $a \in A$ existe $\lambda_a \in \mathbb{C}$ tal que $a \cdot v = \lambda_a v$.

Sea $n = [G : A]$ el índice de A en G, $\{g_1, \ldots, g_n\} \subseteq G$ un sistema de representantes para las coclases derechas de A en G, y $W = \langle g_1 \rightharpoonup v, \ldots, g_n \rightharpoonup v \rangle \subseteq V$.

Si $g \in G$ y $i \in \{1, \ldots, n\}$, existe $j \in \{1, \ldots, n\}$ y $a \in A$ tales que $gg_i = g_i a$, y entonces

$$g \rightharpoonup (g_i \rightharpoonup v) = gg_i \rightharpoonup v = g_i a \rightharpoonup v = g_i \rightharpoonup (a \rightharpoonup v) = \lambda_a g_i \rightharpoonup v \in W.$$

Esto nos dice que W es una subrepresentación de V. Como V es simple y $W \neq 0$, debe ser $W = V$. En particular, $\dim V \leq n$, ya que W puede ser generado por los n elementos $g_1 \rightharpoonup v$, …, $g_n \rightharpoonup v$. Esto prueba el corolario. □

2.8. Los grados de las representaciones simples

Sabemos que el número k de representaciones simples no isomorfas de G es igual al número de clases de conjugación de G. Más aún, si $n_1, \dots, n_k$ son los grados de aquellas, sabemos que $\sum_{i=1}^{k} n_i^2 = |G|$. Es claro que esta condición impone restricciones a los valores que pueden tomar los números n_i. El objetivo de esta sección es dar otras relaciones satisfechas por los grados, que en muchos casos ayudan en su determinación.

Proposición 2.8.1. *Sea (V, ρ) una representación de G y sean n y χ su grado y su carácter, respectivamente. Para cada $g \in G$, $\chi(g)$ es un entero algebraico y $|\chi(g)| \leq n$. Más aún,*

(i) si $|\chi(g)| = n$, existe $\lambda \in \mathbb{C}^\times$ tal que $\rho(g) = \lambda \,\mathsf{id}_V$; y

(ii) si $\chi(g) = n$, entonces $\rho(g) = \mathsf{id}_V$.

Demostración. Sea $g \in G$ y sea n el orden de g, de manera que $g^n = e$. Como ρ es un homomorfismo de grupos, es $\rho(g)^n = \mathsf{id}_V$, así que la transformación lineal $\rho(g) : V \to V$ anula al polinomio $p = X^n - 1 \in \mathbb{C}[X]$. Esto implica que el polinomio minimal $\mu \in \mathbb{C}[X]$ de $\rho(g)$ divide a p y, entonces, que todas sus raíces son raíces de p. Como p tiene sus coeficientes enteros y es mónico, esas raíces son enteros algebraicos; es claro, además, que tienen módulo igual a 1.

Ahora bien, todos los autovalores $\varepsilon_1, \dots, \varepsilon_n$ de $\rho(g)$ son raíces de μ, así que cada uno de ellos es un entero algebraico, y en consecuencia $\chi(g) = \operatorname{tr} \rho(g) = \sum_{i=1}^{n} \varepsilon_i$ es un entero algebraico porque es suma de enteros algebraicos.

La desigualdad triangular implica inmediatamente que $|\chi(g)| \leq \sum_{i=1}^{n} |\varepsilon_i| = n$. Para probar (i), escribamos $\varepsilon = \chi(g)$ y supongamos que $|\varepsilon| = n$. Es $\varepsilon_1\varepsilon^{-1} + \dots + \varepsilon_n\varepsilon^{-1} = 1$, así que

$$\mathsf{Re}(\varepsilon_1\varepsilon^{-1}) + \dots + \mathsf{Re}(\varepsilon_n\varepsilon^{-1}) = 1.$$

Como $\mathsf{Re}(\varepsilon_i\varepsilon^{-1}) \leq |\varepsilon_i\varepsilon^{-1}| \leq \frac{1}{n}$ para cada $i \in \{1, \dots, n\}$, vemos que tienen que valer, de hecho, las igualdades y en consecuencia $\varepsilon_i = \varepsilon/n$ para cada $i \in \{1 \dots, n\}$. Luego si ponemos $\lambda = \varepsilon/n$, es claro que $\rho(g) = \lambda \,\mathsf{id}_V$.

La afirmación (ii) sigue ahora de (i): si $\chi(g) = n$, entonces (i) nos dice que $\rho(g) = \lambda \,\mathsf{id}_V$ y, en consecuencia, que $\chi(g) = \operatorname{tr} \rho(g) = \lambda n$, así que la hipótesis implica que $\lambda = 1$. □

Supongamos que las representaciones simples son $(V_1, \rho_1), \dots, (V_k, \rho_k)$, con (V_1, ρ_1) la representación trivial, y sean $\chi_1, \dots, \chi_k$ y $n_1, \dots, n_k$ los correspondientes carácteres y grados. Sean $c_1, \dots, c_k$ las clases de conjugación, con $c_1 = \{e\}$, y sean $g_1, \dots, g_k \in G$ tales que $g_i \in c_i$ para cada $i \in \{1, \dots, k\}$.

Lema 2.8.2. *Sea (V, ρ) una representación simple. Para cualquier $j \in \{1, \dots, k\}$, la aplicación lineal*

$$r_j = \sum_{h \in c_j} \rho(h) : V \to V$$

es un endomorfismo de representaciones y, en particular $r_1 = \mathsf{id}_V$. Más aún, para cada j, $l \in \{1, \dots, k\}$ se tiene que

$$r_j \circ r_l = \sum_{m=1}^{k} d_m^{j,l}\, r_m \tag{8}$$

con $d_m^{j,l} = \left|\{(h, h') \in c_j \times c_l : hh' = g_m\}\right|$ cualesquiera sean m, j, $l \in \{1, \dots, k\}$.

Demostración. Sea $j \in \{1, \dots, k\}$. Si $g \in G$, entonces

$$r_j \circ \rho(g) = \sum_{h \in c_j} \rho(h) \circ \rho(g) = \sum_{h \in c_j} \rho(hg).$$

Cuando h recorre c_j, $h' = g^{-1}hg$ también lo hace, así que podemos reescribir esta última suma como

$$\sum_{h' \in c_j} \rho(gh') = \sum_{h' \in c_j} \rho(g) \circ \rho(h') = \rho(g) \circ r_j.$$

Vemos así que $r_j \circ \rho(g) = \rho(g) \circ r_j$ para todo $g \in G$, esto es, que $r_j : V \to V$ es un endomorfismo de representaciones, como afirma el enunciado.

Por otro lado, si j, $l \in \{1, \dots, k\}$, es

$$r_j \circ r_l = \sum_{h \in c_j} \rho(h) \sum_{h' \in c_l} \rho(h') = \sum_{h \in c_j,\, h' \in c_l} \rho(h) \circ \rho(h') = \sum_{h \in c_j,\, h' \in c_l} \rho(hh'). \tag{9}$$

Si $g \in G$, consideremos el conjunto $D^{j,l}(g) = \{(h, h') \in c_j \times c_l : hh' = g\}$ y escribamos $d^{j,l}(g) = |D^{j,l}(g)|$. Es claro que $d^{j,l}(g)$ es exactamente la cantidad de sumandos en la suma (9) iguales a $\rho(g)$, y entonces

$$r_j \circ r_l = \sum_{g \in G} d^{i,j}(g)\, \rho(g). \tag{10}$$

Ahora bien, si g_1, g_2 son conjugados, de manera que existe $s \in G$ tal que $g_2 = s g_1 s^{-1}$, es inmediato verificar que la función

$$(h, h') \in D^{j,l}(g_1) \mapsto (shs^{-1}, sh's^{-1}) \in D^{j,l}(g_2)$$

está bien definida y es biyectiva, y entonces $d^{j,l}(g_1) = d^{j,l}(g_2)$. Esto nos dice que $d^{j,l}(g)$ depende solamente de la clase de conjugación de g en G, de manera que, de hecho, $d^{j,l}(g) = d^{j,l}_m$ para todo $g \in c_m$, y que podemos entonces reescribir (10) en la forma

$$r_j \circ r_l = \sum_{m=1}^{k} d^{j,l}_m \sum_{g \in c_m} \rho(g) = \sum_{m=1}^{k} d^{j,l}_m\, r_m.$$

Esto prueba la segunda afirmación del lema. □

Lema 2.8.3. *Sea (V, ρ) una representación simple de grado n y carácter χ. Para cada $j \in \{1, \dots, k\}$, el escalar*

$$\lambda_j = \frac{|c_j| \chi(g_j)}{n} \tag{11}$$

es un entero algebraico y $r_j = \lambda_j \mathsf{id}_V$.

Demostración. Retomemos las notaciones del Lema 2.8.2.

La aplicación lineal $r_j : V \to V$ es, para cada $j \in \{1, \dots, k\}$, un endomorfismo de representaciones. El Lema de Schur 1.3.9, entonces, nos dice que existen escalares $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ tales que

$$r_j = \lambda_j \mathsf{id}_V \text{ para cada } j \in \{1, \dots, k\} \tag{12}$$

Tomando trazas y usando el hecho de que χ es una función central, vemos que

$$n\lambda_j = \sum_{h \in c_j} \operatorname{tr} \rho(h) = |c_j| \chi(g_j),$$

de lo que se deduce la igualdad (11) del enunciado.

Ahora bien, la relación (8) del Lema 2.8.2 implica, en vista de (12), que

$$\lambda_j\lambda_l = \sum_{m=1}^{k} d_m^{j,l}\,\lambda_m$$

para cada j, $l \in \{1,\dots,k\}$. Si fijamos $j \in \{1,\dots,k\}$, esto nos dice que

$$\sum_{m=1}^{k}(d_m^{j,l} - \delta_{l,m}\lambda_j)\lambda_m = 0, \qquad \forall l \in \{1,\dots,k\}$$

o, equivalentemente, que se anula el producto

$$\begin{pmatrix} d_1^{j,1}-\lambda_j & d_2^{j,1} & \cdots & d_k^{j,1} \\ d_1^{j,2} & d_2^{j,2}-\lambda_j & \cdots & d_k^{j,2} \\ \vdots & \vdots & \ddots & \vdots \\ d_1^{j,k} & d_2^{j,k} & \cdots & d_k^{j,k}-\lambda_j \end{pmatrix} \begin{pmatrix} \lambda_i^1 \\ \lambda_i^2 \\ \vdots \\ \lambda_i^k \end{pmatrix}.$$

Como el segundo factor no es nulo —en efecto, es $\lambda_1 = 1$ porque $r_1 = \mathsf{id}_V$,— el determinante de la matriz debe anularse: esto significa que λ_j es un autovalor de la matriz

$$\begin{pmatrix} d_1^{j,1} & d_2^{j,1} & \cdots & d_k^{j,1} \\ d_1^{j,2} & d_2^{j,2} & \cdots & d_k^{j,2} \\ \vdots & \vdots & \ddots & \vdots \\ d_1^{j,k} & d_2^{j,k} & \cdots & d_k^{j,k} \end{pmatrix} \in M_k(\mathbb{Z}),$$

así que es un entero algebraico. □

Teorema 2.8.4. *Los grados de las representaciones simples de G dividen a $|G|$.*

Demostración. Fijemos $i \in \{1,\dots,k\}$ y mostremos que $n_i \mid |G|$.

De acuerdo al Lema 2.8.3, existen enteros algebraicos $\lambda_i^1, \dots, \lambda_i^k$ tales que $r_i^j = \lambda_i^k \mathsf{id}_{V_i}$ para cada $j \in \{1,\dots,k\}$. Es entonces $\operatorname{tr} r_i^j = \lambda_i^j n_i$; como χ_i es una función central, es también

$$\operatorname{tr} r_i^j = \sum_{h\in c_j} \operatorname{tr}\rho_i(h) = \sum_{h\in c_j}\chi_i(h) = |c_j|\chi_i(g_j),$$

así que, de hecho,

$$\lambda_i^j n_i = |c_j|\chi_i(g_j). \tag{13}$$

Finalmente, como V_i es simple, es $\langle\chi_i,\chi_i\rangle = 1$ y, usando el Lema 2.2.2 y la igualdad (13), esto nos dice que

$$|G| = \sum_{j=1}^{k}|c_j|\chi_i(g_j)\overline{\chi_i(g_j)} = n_i\sum_{j=1}^{k}\lambda_i^j\overline{\chi_i(g_j)}.$$

Concluimos de esta forma que el número racional $|G|/n_i$ es igual a $\sum_{j=1}^{k}\lambda_i^j\overline{\chi_i(g_j)}$, que es un entero algebraico porque λ_i^j, $\overline{\chi(g_j)} \in \mathcal{O}$ para cada $j \in \{1,\dots,k\}$. Debe ser entonces $|G|/n_i \in \mathbb{Z}$ y, en definitiva, vemos que n_i divide a $|G|$, como queríamos probar. □

Lema 2.8.5. *Sea $Z(G)$ el centro de G. Si (V,ρ) es una representación simple de G, existe un homomorfismo de grupos $\gamma : Z(G) \to \mathbb{C}^\times$ tal que*

$$\rho(z) = \gamma(z)\mathsf{id}_V$$

para cada $z \in Z(G)$.

Decimos que γ es el *carácter central* de la representación V.

Demostración. Sea $z \in Z(G)$. Para cada $g \in G$ es

$$\rho(g) \circ \rho(z) = \rho(gz) = \rho(zg) = \rho(z) \circ \rho(g),$$

así que $\rho(z) : V \to V$ es un endomorfismo de representaciones. Como V es simple, el Lema de Schur 1.3.9 nos dice que existe un escalar $\gamma(z) \in \mathbb{C}^\times$ tal que $\rho(z) = \gamma(z)\mathsf{id}_V$.

Tenemos así definida una función $\gamma : Z(G) \to \mathbb{C}^\times$ que satisface la identidad del enunciado. Se trata de un homomorfismo de grupos: si z, $z' \in Z(G)$, la definición de γ implica que

$$\gamma(zz')\mathsf{id}_V = \rho(zz') = \rho(z) \circ \rho(z') = \gamma(z)\mathsf{id}_V \circ \gamma(z')\mathsf{id}_V = \gamma(z)\gamma(z')\mathsf{id}_V,$$

y, como $\mathsf{id}_V \neq 0$ porque V no es el espacio nulo, esto nos dice que $\gamma(zz') = \gamma(z)\gamma(z')$. □

Teorema 2.8.6 (G. Frobenius, I. Schur)**.** *Sea $Z(G)$ el centro de G. El grado de toda representación simple de G divide al índice $[G : Z(G)]$ de $Z(G)$ en G.*

Demostración. Mostremos primero que el teorema es consecuencia del siguiente caso especial:

$$\begin{aligned} &\textit{si } (V, \rho) \textit{ es una representación simple de } G \textit{ tal que } Z(G) \cap \ker \rho = (e), \\ &\textit{entonces } \dim V \textit{ divide a } [G : Z(G)]. \end{aligned} \tag{14}$$

Sea, en efecto, $K = Z(G) \cap \ker \rho$; es un subgrupo normal de G contenido en $Z(G)$, así que podemos considerar los cocientes $\bar{G} = G/K$ y $\bar{Z} = Z(G)/K$ y la proyección canónica $p : G \to \bar{G}$. Como $K \subseteq \ker \rho$, existe un homomorfismo $\bar{\rho} : \bar{G} \to \mathrm{GL}(V)$ tal que $\rho = \bar{\rho} \circ p$, de manera que tenemos una representación $(\bar{V}, \bar{\rho})$ de $\bar{G}$ sobre $\bar{V} = V$.

Como $p^*(\bar{V})$, la restricción de $\bar{V}$ a lo largo de p, es precisamente V, la Proposición 1.5.6(ii) implica que $\bar{V}$ es simple. Es inmediato verificar, por otro lado, que $Z(\bar{G}) \cap \ker \bar{\rho} = (e)$, así que si suponemos la validez de la afirmación (14) podemos concluir que $\dim V$ divide a $[\bar{G} : Z(\bar{G})]$. Pero como $\bar{Z} \subseteq Z(\bar{G})$, es

$$[G : Z] = [\bar{G} : \bar{Z}] = [\bar{Z} : Z(\bar{G})]\,[Z(\bar{G}) : \bar{Z}],$$

así que, de hecho, $\dim V$ divide a $[G : Z]$. Vemos de esta forma que la afirmación (14) implica el teorema, como dijimos. Probémosla.

Sea (V, ρ) una representación simple de G de grado n tal que $Z(G) \cap \ker \rho = (e)$, y sean $\chi : G \to \mathbb{C}$ y $\gamma : Z(G) \to \mathbb{C}^\times$ el carácter y el carácter central de V, respectivamente.

Sea $C(G)$ el conjunto de clases de conjugación de G; si $c \in C(G)$, escribamos g_c a uno de sus elementos. Si $z \in Z(G)$ y $c \in C(G)$, entonces el conjunto $z \cdot c = \{zg : g \in c\}$ es también un elemento de $C(G)$. Podemos entonces definir una función

$$(z, c) \in Z(G) \times C(G) \mapsto z \cdot g \in C(G),$$

y es fácil verificar que se trata de una acción de $Z(G)$ sobre $C(G)$. Escribamos $C(G)/Z(G)$ al correspondiente conjunto de órbitas y fijemos un elemento $c_g \in o$ en cada órbita $o \in C(G)/Z(G)$.

Necesitaremos las siguientes observaciones:

- Es claro que si $z \in Z(G)$ y $c \in C(G)$ se tiene que $|z \cdot c| = |c|$. Se sigue de esto inmediatamente que

$$\textit{si } o \in C(G)/Z(G), \textit{ es } |c| = |c_o| \textit{ para toda clase } c \in o. \tag{15}$$

- Si $o \in C(G)/Z(G)$ una órbita, entonces $|o| \leq |Z(G)|$. Afirmamos que

$$\text{si } o \in C(G)/Z(G) \text{ es tal que } |o| < |Z(G)|, \text{ entonces para cada } c \in o \text{ y cada } g \in c \text{ se tiene que } \chi(g) = 0. \tag{16}$$

  En efecto, sea $o \in C(G)/Z(G)$ tal que $|o| < |Z(G)|$ y sea $c \in o$. entonces $z \in Z(G)$ tal que $z \neq e$ y $z \cdot c = c$. Si $g \in c$, entonces esto nos dice que también $zg \in c$, así que existe $h \in G$ tal que $g = zhgh^{-1}$ y, en consecuencia,

$$\rho(g) = \rho(z) \circ \rho(hgh^{-1}) = \gamma(z)\rho(hgh^{-1}).$$

  Tomando trazas en esta igualdad, vemos que $\chi(g) = \gamma(z)\chi(g)$ y, como $\gamma(z) \neq 1$, podemos concluir que $\chi(g) = 0$. Esto prueba (16).

- Se tiene que

$$\text{si } o \in C(G)/Z(G) \text{ y } c, c' \in o, \text{ entonces } |\chi(g_c)| = |\chi(g_{c'})|. \tag{17}$$

  En efecto, en ese caso existe $z \in Z(G)$ tal que $z \cdot c = c'$ y esto implica que zg_c y g'_c son conjugados, de manera que $\chi(g_{c'}) = \chi(zg_c)$. Por otro lado,

$$\chi(zg_c) = \operatorname{tr} \rho(zg_c) = \operatorname{tr} \rho(z) \circ \rho(g_c) = \operatorname{tr} \gamma(z)\rho(g_c) = \gamma(z)\chi(g_c)$$

  así que $|\chi(zg_c)| = |\gamma(z)\chi(g_c)| = |\chi(g_c)|$ porque $|\gamma(z)| = 1$.

Como V es simple, es $\langle \chi, \chi \rangle = 1$ y entonces

$$|G| = \sum_{g \in G} |\chi(g)|^2 = \sum_{o \in C(G)/Z(G)} \sum_{c \in o} \sum_{g \in c} |\chi(g)|^2.$$

De acuerdo a (16), en esta suma los únicos términos posiblemente no nulos son aquellos que corresponden a órbitas $o \in C(G)/Z(G)$ de exactamente m elementos. Entonces

$$\begin{aligned}
|G| &= \sum_{\substack{o \in C(G)/Z(G) \\ |o| = |Z(G)|}} \sum_{c \in o} \sum_{g \in c} |\chi(g)|^2 \\
&= \sum_{\substack{o \in C(G)/Z(G) \\ |o| = |Z(G)|}} \sum_{c \in o} |c| |\chi(g_c)|^2 && \text{porque } \chi \text{ es una función central} \\
&= \sum_{\substack{o \in C(G)/Z(G) \\ |o| = |Z(G)|}} |c_o| \sum_{c \in o} |\chi(g_c)|^2 && \text{por (15)} \\
&= \sum_{\substack{o \in C(G)/Z(G) \\ |o| = |Z(G)|}} |Z(G)|\, |c_o|\, |\chi(g_{c_o})| && \text{por (17).}
\end{aligned}$$

En consecuencia,

$$\frac{[G : Z(G)]}{n} = \frac{|G|}{n|Z(G)|} = \sum_{\substack{o \in C(G)/Z(G) \\ |o| = |Z(G)|}} |c_o| |\chi(g_{c_o})| = \sum_{\substack{o \in C(G)/Z(G) \\ |o| = |Z(G)|}} \frac{|c_o| \chi(g_{c_o})}{n} \chi(g_{c_o}^{-1}).$$

De acuerdo a la Proposición 2.8.1 y al Lema 2.8.3, el último miembro de esta cadena de igualdades es un entero algebraico. Como el primer miembro es evidentemente un número racional, concluimos que se trata, de hecho, de un entero. Esto prueba (14). □

3. Aplicaciones

3.1. La solubilidad de los grupos de orden $p^a q^b$

Definición 3.1.1. Decimos que un grupo G es *soluble* si hay una cadena

$$(e) = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_l = G$$

tal que para cada $i \in \{1, \ldots, l\}$ es subgrupo G_{i-1} es normal en G_i y el cociente G_i/G_{i-1} es abeliano.

Lema 3.1.2. (*i*) *Un grupo abeliano es soluble.*

(*ii*) *Si G es un grupo y $H \subseteq G$ es un subgrupo normal tal que H y G/H son soluble, entonces G es soluble.*

Demostración. □

El objetivo de esta sección es probar el siguiente teorema de William Burnside. Es un resultado muy importante para el estudio de la estructura de los grupos finitos y fue una de las primeras aplicaciones de la teoría de carácteres. Se trata de uno de los primeros resultados del programa de clasificación de los grupos finitos simples.

Hasta la década de 1960, las pruebas que se conocían de este teorema estaban basadas en la teoría de carácteres. En ese momento, John Thompson indicó como, combinando resultados de [FT1963] y [Tho1968], es posible dar una demostración puramente algebraica, pero ésta es extremadamente larga y complicada. Más tarde, a princípios de la década de 1970, Helmut Bender [Ben1972] logró simplicar considerablemente ese argument, y luego David Goldschmidt [Gol1970], para el caso de órdenes impares, y Hiroshi Matsuyama [Mat1973], para el caso de órdenes pares, dieron pruebas mucho más simples independientes de la teoría de carácteres.

Teorema 3.1.3 (W. Burnside, 1904)**.** *Un grupo G de orden $p^a q^b$, con p y q primos, es soluble.*

Lema 3.1.4. *Sea (V, ρ) una representación simple de grado n y carácter χ. Sea $g \in G$, sea $c \subseteq G$ es la clase de conjugación de g y pongamos $m = |c|$. Si $(n : m) = 1$, entonces o bien $\chi(g) = 0$ o bien $\rho(g) = \lambda \,\mathsf{id}_V$ para algún $\lambda \in \mathbb{C}^\times$.*

Demostración. Si $|\chi(g)| = n$, de la Proposición 2.8.1(i) sabemos que existe $\lambda \in \mathbb{C}^\times$ tal que $\rho(g) = \lambda \,\mathsf{id}_V$. Supongamos entonces que $|\chi(g)| < n$.

Por hipótesis, existen α, $\beta \in \mathbb{Z}$ tales que $\alpha n + \beta m = 1$, así que

$$\frac{\chi(g)}{n} = \alpha\chi(g) + \beta\frac{m\chi(g)}{n}$$

Del Lema 2.8.3 sabemos que $\frac{m\chi(g)}{n}$ es un entero algebraico, así que esta ecuación implica que $\frac{\chi(g)}{n}$ también lo es.

Sea t el orden de g, sea $\zeta = \mathrm{e}^{2\pi i/t}$ y consideremos el cuerpo ciclotómico $K = \mathbb{Q}(\zeta)$; se trata de una extension Galoisiana de $\mathbb{Q}$: sea $\Gamma = \mathrm{Gal}(K \mid \mathbb{Q})$ su grupo de Galois. Todos los autovalores $\varepsilon_1, \ldots, \varepsilon_n$ de g son raíces t-ésimas de la unidad, así que $\chi(g) \in K$.

Sea

$$a = \prod_{\sigma \in \Gamma} \frac{\sigma(\chi(g))}{n}.$$

Para cada $\sigma \in \Gamma$ el número $\frac{\sigma(\chi(g))}{n}$ es un entero algebraico, así que a también lo es. Por otro lado, es claro que $\sigma(a) = a$ para todo $\sigma \in \Gamma$, así que $a \in \mathbb{Q}$. Concluimos así que $a \in \mathbb{Z}$.

Ahora bien, si $\sigma \in \Gamma$, entonces $\sigma(\varepsilon_i)$ es una raíz de la unidad para cada $i \in \{1, \dots, n\}$, así que $|\sigma(\varepsilon_i)| = 1$. En consecuencia

$$|\sigma(\chi(g))| = |\sigma(\varepsilon_1) + \cdots + \sigma(\varepsilon_n)| \leq |\sigma(\varepsilon_1)| + \cdots + |\sigma(\varepsilon_n)| = n$$

y

$$|a| = \left| \prod_{\sigma \in \Gamma} \frac{\sigma(\chi(g))}{n} \right| \leq \frac{|\chi(g)|}{n} < 1.$$

Esto implica que debe ser $a = 0$ y, entonces, $\chi(g) = 0$. □

Teorema 3.1.5. *Si un grupo G posee una clase de conjugación $c \neq \{e\}$ tal que $|c| = p^m$ con p primo y $m \geq 0$, entonces G no es simple no abeliano.*

Demostración. Sea $g \in c$; por hipótesis, $g \neq e$. Si $|c| = 1$, entonces $g \in Z(G)$, así que $Z(G)$ es un subgrupo normal no trivial de G: vemos que en este caso G no es simple. Supongamos entonces que $|c| = p^m > 1$.

Sean (V_1, ρ_1), …, (V_k, ρ_k) las representaciones simples de G, y sean n_1, …, n_k y χ_1, …, χ_k sus grados y carácteres, respectivamente; podemos suponer que V_1 es la representación trivial.

De acuerdo al Corolario 2.4.8, tenemos que

$$\sum_{j=1}^{k} n_j \chi_j(g) = \chi_{\mathsf{reg}}(g) = 0.$$

El término que corresponde a $j = 1$ en esta suma es $n_1\chi_1(g) = 1$, así que podemos reescribir esta igualdad en la forma

$$\frac{1}{p} = -\sum_{j \geq 1} \frac{n_j}{p} \chi_j(g). \tag{18}$$

Si para cada $j \geq 2$ se tuviera que

$$p \nmid n_j \implies \chi_j(g) = 0,$$

para cada $j \geq 2$ el número $\frac{n_j}{p}\chi_j(g)$ sería un entero algebraico y, en vista de (18), tendríamos que $\frac{1}{p} \in \mathcal{O}$: esto es absurdo.

Existe, entonces, necesariamente $j \geq 2$ tal que $\chi_j(g) \neq 0$ y $p \nmid n_j$. En ese caso $(n_j : |c|) = 1$ y el Lema 3.1.4 dice que existe $\lambda \in \mathbb{C}^\times$ tal que $\rho_j(g) = \lambda \,\mathsf{id}_{V_j}$. Puede ser que $\ker \rho_j$ sea o no trivial. En el segundo caso, se trata de un subgrupo normal no trivial que es propio —porque ρ_j no es la representación trivial,— así que G no es simple. En el primero, por otro lado, es $g \in Z(G)$, ya que para cada $h \in G$,

$$\rho_j(hg) = \rho_j(h) \circ \rho_j(g) = \lambda\rho_j(h) = \rho_j(g) \circ \rho_j(h) = \rho_j(gh),$$

de manera que $hg = gh$ porque ρ_j es inyectivo: luego $Z(G)$ es no trivial, así que G es abeliano o no simple. □

Corolario 3.1.6. *Si G es un grupo de orden $p^a q^b$ con p y q primos y a, $b \geq 0$, entonces G no es simple no abeliano.*

Demostración. Supongamos, por ejemplo, que $b > 0$, de manera que $q \mid |G|$, y sea $P \subseteq G$ un q-subgrupo de Sylow. El centro $Z(P)$ de P es no trivial porque se trata de un q-grupo: sea entonces $g \in Z(P) \setminus \{e\}$. Si $C_G(g)$ es el centralizador de g en G, la elección de g implica que $P \subseteq C_G(g)$, así que el cardinal $|c| = [G : C_G(g)]$ de la clase de conjugación c de g divide a $[G : P] = p^b$. El corolario sigue entonces inmediatamente del teorema. □

Demostración del Teorema 3.1.3. Hagamos inducción con respecto a G. Si G tiene orden como en el enunciado, entonces el Corolario 3.1.6 nos dice que o G es abeliano o G no es simple. En el primer caso, es inmediato que G es soluble. En el segundo, existe un subgrupo $H \subseteq G$ normal propio maximal. La hipótesis inductiva implica que H es soluble. Por otro lado, elección de H implica que G/H es un grupo simple cuyo orden es como en el enunciado del teorema, de manera que se le aplica el Corolario 3.1.6, y que es entonces abeliano. El Lema 3.1.2(ii) implica entonces que G es soluble, completando la inducción. □

3.2. El teorema de Hurwitz

Decimos que un polinomio $f \in \mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ en *bilineal* si es de la forma

$$f = \sum_{1 \leq i,j \leq n} a_{i,j} x_i y_j.$$

El objetivo de esta sección es probar el siguiente resultado de Adolf Hurwitz siguiendo un argumento propuesto por Beno Eckmann en [Eck1943].

Teorema 3.2.1 (A. Hurwitz [Hur1898])**.** *Si $f_1, \ldots, f_n \in \mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ son polinomios bilineales tales que*

$$\Big(\sum_{i=1}^{n} x_i^2\Big)\Big(\sum_{i=1}^{n} y_i^2\Big) = \sum_{i=1}^{n} f_i^2, \tag{19}$$

entonces $n \in \{1, 2, 4, 8\}$.

Fijemos $n \geq 1$ y supongamos que tenemos tales polinomios $f_1, \ldots, f_n$. Para cada $k \geq 0$ escribamos $[k] = \{1, \ldots, k\}$, e introduzcamos las siguientes notaciones:

- sean $a_{i,j,k} \in \mathbb{C}$, para $i, j, k \in [n]$, los escalares son tales que

  $$f_i = \sum_{j,k \in [n]} a_{i,j,k} x_i y_j$$

- Si i, $k \in [n]$, sea

  $$f_{i,k} = \sum_{j \in [n]} a_{i,j,k} x_j,$$

  de manera que $f_i = \sum_{k \in [n]} f_{i,k} y_k$ para cada $i \in [n]$.

- Para cada $j \in [n]$, consideremos la matriz

  $$A_j = (a_{i,j,k})_{i,k \in [n]} \in M_n(\mathbb{C}),$$

  y sea

  $$A = (f_{i,j})_{i,j \in [n]} \in M_n(\mathbb{C}[x_1, \ldots, x_n])$$

Si j, $k \in [n]$, mirando el coeficiente de $y_j y_k$ en (19), vemos que

$$\delta_{j,k} \sum_{i \in [n]} x_i^2 = \sum_{i \in [n]} f_{i,j} f_{i,k},$$

y entonces

$$\Big(\sum_{i \in [n]} x_i^2 \Big) A = AA^t = A^t A.$$

Mirando ahora los coeficientes de x_1, $\dots$, x_n es esta última igualdad, concluimos que

$$A_i^t A_j + A_j^t A_i = 0 \qquad \text{si } i, j \in [n] \text{ son distintos, y} \tag{20}$$

$$A_i^t A_i = A_i A_i^t = I_n \qquad \text{si } i \in [n].a \tag{21}$$

Lema 3.2.2. *Para cada $i \in [n-1]$, sea $B_i = A_i^t A_n$. Entonces si i, $j \in [n-1]$ e $i \neq j$, es*

$$B_i B_i^t = I_n, \qquad B_i + B_i^t = 0,$$

$$B_i^2 = -I_n, \qquad B_i B_j + B_j B_i = 0.$$

Demostración. Las cuatro identidades con consecuencias inmediatas de (20) y (21). □

Se sigue en particular de este lema que B_1, $\dots$, $B_{n-1} \in \mathrm{GL}(n, \mathbb{C})$. Consideremos el subgrupo $G = \langle B_1, \dots, B_{n-1} \rangle \subseteq \mathrm{GL}(n, \mathbb{C})$ generado por estas $n-1$ matrices.

Para cada $I = \{i_1, \dots, i_r\} \subseteq [n-1]$, con $1 \leq i_1 < \cdots < i_r < n$, escribamos

$$B_I = B_{i_1} B_{i_2} \cdots B_{i_r}.$$

Usando las dos últimas relaciones del lema, es inmediato verificar que

$$G = \{B_I, -B_I : I \subseteq [n-1]\} \tag{22}$$

y que para cada $I \subseteq [n-1]$ con r elementos es

$$B_I^2 = (-1)^{\binom{r+1}{2}} I_n.$$

Más generalmente, si I, $J \subseteq [n-1]$, entonces existe $\varepsilon \in \{\pm 1\}$ tal que

$$B_I B_J = \varepsilon B_{I \triangle J}.$$

Aquí $I \triangle J$ es la diferencia simétrica $(I \setminus J) \cup (J \setminus I)$.

Lema 3.2.3. (*i*) *Si $g \in G$ no es central, entonces la clase de conjugación de g es $\{\pm g\}$.*

(*ii*) *El subgrupo derivado es $G' = \{\pm I_n\}$.*

Demostración. (*i*) Supongamos que $g = \varepsilon B_I$ con $\varepsilon \in \{\pm 1\}$ e $I \subseteq [n-1]$. De las relaciones del Lema 3.2.2 es claro que $B_i B_I B_i^{-1} \in \{\pm B_I\}$ para cada $i \in [n-1]$. Como B_1, $\dots$, B_{n-1} genera a G, esto implica que la clase de conjugación de g es o bien $\{g\}$ o bien $\{\pm g\}$, y el primer caso ocurre exactamente cuando g es central.

(*ii*) Como $G = \langle B_1, \dots, B_{n-1} \rangle$, G' está generado por $\{[B_i, B_j] : i, j \in [n-1], i \neq j\}$. Usando las dos últimas relaciones del Lema 3.2.2, es inmediato ver que $[B_i, B_j] = -I_n$ cualesquiera sean i, $j \in [n-1]$ tales que $i \neq j$. □

Lema 3.2.4. *Sea $I \subseteq [n-1]$. Si $B_I \in Z(G)$, entonces o bien $I = \varnothing$ o bien $I = [n-1]$ y n es par.*

Demostración. Supongamos que $\varnothing \subsetneq I = \{i_1, \dots, i_r\} \subsetneq [n-1]$ es tal que B_I es central en G y $1 \leq i_1 < \cdots < i_r < n$. Entonces

$$\begin{aligned} B_I &= B_{i_1} B_I B_{i_1}^{-1} \\ &= (B_{i_1} B_{i_1} B_{i_1}^{-1})(B_{i_1} B_{i_2} B_{i_1}^{-1}) \cdots (B_{i_1} B_{i_r} B_{i_1}^{-1}) \\ &= B_{i_1}(-B_{i_2}) \cdots (-B_{i_r}) \\ &= (-1)^{r-1} B_I \end{aligned} \tag{23}$$

y, si $j \in [n-1] \setminus I$,

$$\begin{aligned} B_I &= B_j B_I B_j^{-1} \\ &= (B_j B_{i_1} B_j^{-1})(B_j B_{i_2} B_j^{-1}) \cdots (B_j B_{i_r} B_j^{-1}) \\ &= (-B_{i_1})(-B_{i_2}) \cdots (-B_{i_r}) \\ &= (-1)^r B_I, \end{aligned}$$

de manera que $B_I = -B_I$: como $B_I \neq 0$, esto es absurdo.

Esta contradicción nos dice que si $B_I \in Z(G)$, entonces $I = [n-1]$, que $r = n-1$ y, de acuerdo a la ecuación (23), que $n-2$ es par. □

Lema 3.2.5. *Si $n = 2m+1$ es impar, entonces $G' = Z(G) = \langle -I_n \rangle$ es un subgrupo cíclico de orden 2 y $|G| = 2^n$. Hay $2^{n-1}+1$ clases de conjugación y, a menos de isomorfismo, 2^{n-1} representaciones de grado 1 y una representaciones simple de grado 2^{n-1}.*

Demostración. Si $\varepsilon B_I \in Z(G)$, con $\varepsilon \in \{\pm 1\}$ e $I \subseteq [n-1]$, entonces $B_I \in Z(G)$, porque por supuesto $-I \in Z(G)$, y el Lema 3.2.4 nos dice que $I = \varnothing$. Así, es $Z(G) = \{\pm I_n\} = G'$.

Supongamos que I, $J \subseteq [n-1]$ y $\varepsilon \in \{\pm 1\}$ son tales que $B_I = \varepsilon B_J$. Entonces

$$(-1)^{\binom{|I|+1}{2}} I_n = B_I^2 = \varepsilon B_I B_J = \eta B_{I \triangle J}$$

para algún $\eta \in \{\pm 1\}$, así que $B_{I \triangle J} \in Z(G)$. El lema anterior implica que $I \triangle J = \varnothing$, esto es, que $I = J$ y debe ser necesariamente entonces $\varepsilon = 1$. Vemos de esta forma que G tiene exactamente 2^n elementos, porque los elementos listados en (22) son distintos dos a dos.

De acuerdo al Lema 3.2.3(i), las clases de conjugación tienen o uno o dos elementos, y el primer caso el elemento correspondiente es central. Acabamos de probar que hay exactamente dos elementos centrales en G, así que los otros $2^n - 2$ elementos se distribuyen en $2^{n-1} - 1$ clases de conjugación de dos elementos cada una: hay, entonces, $2^{n-1}+1$ clases de conjugación en total.

En vista de esto, el Teorema 2.5.3 nos dice que G posee $2^{n-1}+1$ representaciones simples no isomorfas. Del Corolario 2.7.5 sabemos que G tiene $[G : G'] = 2^{n-1}$ representaciones de grado 1, así que hay exactamente una representaciones de grado $k > 1$. Finalmente, según el Corolario 2.4.8, la suma de los cuadrados de los grados de las representaciones simples es $|G|$, así que $2^n = |G| = 2^{n-1} \cdot 1^2 + k^2$. Se sigue inmediatamente que $k = 2^{n-1}$. □

Lema 3.2.6. *Si $n = 2m$ es par, entonces $G' = \langle -I_n \rangle$, $Z(G) = \{\pm I_n, \pm B_{[n-1]}\}$ y $|G| = 2^n$. Hay $2^{n-1}+2$ clases de conjugación y, a menos de isomorfismo, 2^{n-2} representaciones de grado 1 y dos de grado 2^{m-1}.*

Demostración. El Lema 3.2.4 implica inmediatamente que

$$Z(G) \subseteq \{\pm I_n, \pm B_{[n-1]}\} \tag{24}$$

y, como los cuatro elementos de este último conjunto son centrales —esto sigue de un cálculo directo usando las relaciones del Lema 3.2.2,— vale, de hecho, la igualdad.

Afirmamos que si I, $J \subseteq [n-1]$, entonces

$$B_I Z(G) = B_J Z(G) \iff \text{o } I = J \text{ o } I = [n-1] \setminus J. \tag{25}$$

En efecto, supongamos que $B_I Z(G) = B_J Z(G)$, de manera que $B_I B_J^{-1} \in Z(G)$. Existe $\varepsilon \in \{\pm 1\}$ tal que $B_I B_J^{-1} = \varepsilon B_{I \triangle J}$, así que (24) implica que o bien $I \triangle J = \varnothing$, de manera que $I = J$, o bien $I \triangle J = [n-1]$, de manera que I y J son complementarios en $[n-1]$. Esto prueba la implicación ($\Longrightarrow$) en (25). La implicación recíproca sigue de un cálculo directo: es evidente que si $I = J$ entonces $B_I Z(G) = B_J Z(G)$; si, en cambio, es $I = [n-1] \setminus J$ y ponemos $r = |J|$, existe $\varepsilon \in \{\pm 1\}$ tal que

$$B_I B_J^{-1} = (-1)^{\binom{r+1}{2}} B_I B_J = (-1)^{\binom{r+1}{2}} \varepsilon B_{I \triangle J} = (-1)^{\binom{r+1}{2}} \varepsilon B_{[n-1]} \in Z(G).$$

La equivalencia (25) nos permite contar los elementos de $G/Z(G)$: es $[G : Z(G)] = 2^{n-2}$ y, en consecuencia, $|G| = 2^n$.

Hay 4 clases de conjugación de un elemento, correspondientes a los elementos de $Z(G)$, y, según el Lema 3.2.3(i), todas las demás tienen dos elementos. Esto implica que hay en total $(2^n - 4)/2 + 4 = 2^{n-1} + 2$ clases de conjugación.

Hay el mismo número de representaciones simples no isomorfas, y sabemos que de ellas, $[G : G'] = 2^{n-1}$ tienen grado 1, así que hay exactamente dos de grados más grandes que 1: sean a y b los grados respectivos. Del Corolario 2.4.8, es

$$2^n = |G| = 2^{n-1} \cdot 1^1 + a^2 + b^2,$$

y el teorema 2.8.4 nos dice además que a y b dividen a 2^n. Se sigue inmediatamente que debe ser $a = b = 2^{m-1}$. □

Podemos finalmente probar el resultado principal de esta sección.

Demostración del Teorema 3.2.1. Como $G \subseteq \mathrm{GL}(n, \mathbb{C})$, tenemos una representación natural $(\mathbb{C}^n, \rho)$ de G sobre $\mathbb{C}^n$ en la que el homomorfismo $\rho : G \to \mathrm{GL}(\mathbb{C}^n)$ es *inyectivo* y para el cual es $\rho(-I_n) = -\mathsf{id}_{\mathbb{C}^n}$. Supongamos que $\mathbb{C}^n = V_1 \oplus \cdots \oplus V_r$ es una descomposición de $\mathbb{C}^n$ como suma directa de subrepresentaciones simples.

Si $j \in \{1, \ldots, r\}$ es tal que $\dim V_j = 1$, entonces $-I_n \in G'$ actúa trivialmente sobre V_j, así que $\rho(-I_n)$ tiene a 1 como autovector. Esto es absurdo, y vemos que todas las suprepresentaciones V_1, …, V_r tienen grado mayor que 1.

- Si n es impar, el Lema 3.2.5 nos dice que hay, a menos de isomorfismo, una única representación simple de grado mayor que 1, que tiene grado 2^{n-1}. Cada una de las subrepresentaciones V_1, …, V_r debe ser isomorfa a ésta y, en consecuencua, $2^{n-1} \mid n$. Esto solo es posible si $n = 1$.
- Si, en cambio, $n = 2m$ es par, el Lema 3.2.6 implica que las V_1, …, V_r tienen grado 2^{m-1}, así que $2^{m-1} \mid n$. Es fácil verificar que entonces debe ser $n \in \{2, 4, 8\}$.

Esto prueba el teorema. □

Referencias

Libros de texto

[Col1990] M. J. Collins, *Representations and characters of finite groups*, Cambridge Studies in Advanced Mathematics, vol. 22, Cambridge University Press, Cambridge, 1990. MR1050762 (91f:20001)

[FH1991] William Fulton and Joe Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991. A first course; Readings in Mathematics. MR1153249 (93a:20069)

[Hup1998] Bertram Huppert, *Character theory of finite groups*, de Gruyter Expositions in Mathematics, vol. 25, Walter de Gruyter & Co., Berlin, 1998. MR1645304 (99j:20011)

[Jam1978] G. D. James, *The representation theory of the symmetric groups*, Lecture Notes in Mathematics, vol. 682, Springer, Berlin, 1978. MR513828 (80g:20019)

[Rot1995] Joseph J. Rotman, *An introduction to the theory of groups*, 4th ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995. MR1307623 (95m:20001)

[Sco1987] W. R. Scott, *Group theory*, 2nd ed., Dover Publications Inc., New York, 1987. MR896269 (88d:20001)

[Ser1977] Jean-Pierre Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott; Graduate Texts in Mathematics, Vol. 42. MR0450380 (56 #8675)

Artículos

[Ben1972] Helmut Bender, *A group theoretic proof of Burnside's p^aq^b-theorem*, Math. Z. **126** (1972), 327–338. MR0322048 (48 #412)

[Eck1943] Beno Eckmann, *Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Komposition quadratischer Formen*, Comment. Math. Helv. **15** (1943), 358–366 (German). MR0009936 (5,225e)

[Gol1970] David M. Goldschmidt, *A group theoretic proof of the p^aq^b theorem for odd primes*, Math. Z. **113** (1970), 373–375. MR0276338 (43 #2085)

[Hur1898] Adolf Hurwitz, *Ueber die Composition der quadratischen Formen von beliebig vielen Variabeln*, Gött. Nachr. (1898), 309–316.

[Mat1973] Hiroshi Matsuyama, *Solvability of groups of order 2^ap^b*, Osaka J. Math. **10** (1973), 375–378. MR0323890 (48 #2243)

[FT1963] Walter Feit and John G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029. MR0166261 (29 #3538)

[Tho1968] John G. Thompson, *Nonsolvable finite groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968), 383–437. MR0230809 (37 #6367)

Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires. Ciudad Universitaria, Pabellón I. Buenos Aires (1428) Argentina.

E-mail address: mariano@dm.uba.ar

INTRODUCCIÓN A LA TEORíA DE GALOIS

MARTÍN MOMBELLI Y SEBASTIÁN SIMONDI

RESUMEN. Se introducen los conceptos básicos de la teoría de Galois, los resultados principales y algunas aplicaciones.

ÍNDICE

INTRODUCCIÓN

Estas notas surgen de un curso de 5 sesiones dictado en la *XV Escuela Latinoamericana de Matemática* en el mes de mayo de 2011 en la ciudad de Córdoba, Argentina.

Nuestra intención es que los participantes del curso aprendan las nociones básicas de la teoría de Galois y algunas aplicaciones. Intentamos que las notas fueran lo más autocontenidas posibles, sin embargo, dada la extensión del curso, algunos conocimientos previos de estructuras algebraicas son requeridos.

En la sección 1 recordamos ciertas nociones básicas como la definición de anillo, cuerpo, morfismos de anillos, espacios vectoriales, que luego usaremos. En la sección 2 se introduce la definición de extensión de cuerpos, se muestras los ejemplos básicos y la construcción del cuerpo de raíces de polinomios. En la sección 3 para cada extensión de cuerpos se asocia el grupo de Galois. Se estudian diversas propiedades y algunos cálculos sencillos. En la sección 4 se demuestra el principal resultado de la teoría; los cuerpos intermedios de una extensión de cuerpos están en correspondencia biyectiva con los subgrupos de Galois de la extensión. En la útlima sección se aplican los resultados anteriores para determinar cuando un polinomio dado es resoluble por radicales.

1. NOTACIÓN Y PRELIMINARES

Un *anillo* es un conjunto F munido con dos operaciones binarias, usualmente denotada como suma $+$ y multiplicación, tales que F es un grupo abeliano bajo la suma, la multiplicación es asociativa, es decir que $(ab)c = a(cb)$ para todo $a, b, c \in F$ y es distributiva con respecto a la suma, $a(b + c) = ab + ac$.

Date: 25 de abril de 2011.
2000 *Mathematics Subject Classification.* 11R32, 11S20.

El anillo F se dice *cuerpo* si $F - \{0\}$ es un grupo abeliano bajo el producto, es decir si todo elemento no nulo posee un inverso multiplicativo. Ejemplos de cuerpos son los números racionales $\mathbb{Q}$, los números reales $\mathbb{R}$ y los números complejos $\mathbb{C}$.

Si F y L son dos anillos o dos cuerpos, una función $\phi : F \to L$ es un *homomorfismo de anillo o de cuerpo* respectivamente, si para todo $a, b \in F$

$$\phi(1) = 1, \quad \phi(a+b) = \phi(a) + \phi(b) \quad \text{y} \quad \phi(ab) = \phi(a)\phi(b).$$

Un elemento no nulo $a \in F$ se dice *divisor de cero*, si existe un elemento $b \in F$ no nulo tal que $a.b = 0$ o $b.a = 0$. Un anillo que no contiene divisores de cero se llama *dominio íntegro*.

Un subconjunto S de un anillo F que es cerrado bajo las operaciones de suma y producto se llama *subanillo*. Un subanillo I se dice *ideal* si para $r \in F$ y $x \in I$ tenemos que $rx \in I$ y $xr \in I$. Sea X un subconjunto de F y $\{A_i : i \in J\}$ la familia de todos los ideales de F que contienen a X. Entonces el ideal $\cap_{i \in J} A_i$ se llama *ideal generado por* X y se denota (X) y los elementos de X se llaman generadores. Un ideal (x) generado por un sólo elemento se denomina el *ideal principal*. Un *anillo de ideales principales* es un anillo en el cual todos sus ideales son principales.

Un ideal P de un anillo F se dice *primo* si $P \neq F$ y para cada par de ideales A, B en F

$$AB \subseteq P \Longrightarrow A \subseteq P \quad \text{ó} \quad B \subseteq P.$$

Un ideal M del anillo F se dice *maximal* si $M \neq F$ y para todo ideal N tal que $M \subseteq N \subseteq F$ se tiene que $N = M$ ó $N = F$. Un resultado muy conocido cuya demostración no haremos es el siguiente:

Teorema 1.1. *Sea M un ideal en un anillo conmutativo con identidad $1_F \neq 0$. Entonces M es un ideal maximal si y sólo si el anillo cociente F/M es un cuerpo.* □

De este resultado se desprende lo siguiente:

Corolario 1.2. *Las siguientes condiciones sobre un anillo F conmutativo con identidad $1_F \neq 0$ son equivalentes*

1. *F es un cuerpo.*
2. *F no posee ideales propios.*
3. *El ideal (0) es un ideal maximal en F.*
4. *Si S es otro anillo, todo homomorfismo de anillos $F \to S$ es un monomorfismo.*

□

Sea F un anillo conmutativo con identidad, un elemento $c \in F$ se dice *irreducible* si c es no inversible y además si $c = ab$ entonces a o b es inversible. Por otro lado $p \in F$ se dice *primo* si no es inversible y además si $p|ab$ entonces $p|a$ o $p|b$.

Teorema 1.3. *Sean p y c dos elementos no nulos en un dominio integral F.*

1. *El elemento p es primo si y sólo si (p) es un ideal primo no nulo.*
2. *El elemento c es irreducible si y sólo si (c) es maximal en el conjunto de todos los ideales principales propios.*
3. *Todo elemento primo de F es irreducible.*
4. *Si F es un dominio de ideales principales, entonces p es primo si y sólo si p es irreducible.* □

Un dominio íntegro F tal que todo elemento no inversible distinto de cero se puede escribir como producto de irreducibles de manera única, se llama *dominio de factorización única*.

Si F es un cuerpo definimos el conjunto de todos los polinomios de una variable con coeficientes en F como

$$F[x] = \{p(x) = a_0 + a_1x + ... + a_nx^n : n \in \mathbb{N}_0 \text{ y } a_i \in F\}$$

Con la suma y el producto definidos de manera usual, $F[x]$ es un anillo. Como F es un cuerpo, $F[x]$ no contine divisores de cero, por lo tanto es un dominio íntegro. Más aún $F[x]$ es un *dominio euclídeo*, es decir dados dos polinomios $f(x), g(x) \in F[x]$ con $g(x) \neq 0$ existen polinomios únicos $q(x), r(x) \in F[x]$ tales que

$$f(x) = q(x)g(x) + r(x) \text{ con } r = 0 \text{ o } gr(r) < gr(g).$$

Este algoritmo de división es análogo al aprendido en la escuela secundaria para $\mathbb{R}[x]$. Como $F[x]$ es un dominio euclideano, entonces es un dominio de ideales principales y consecuentemente un dominio de factorización única.

Si $f \in F[x]$ tal que $gr(f) \geq 1$, del Teorema 1.3 se deduce que las siguientes propiedades son equivalentes

1. Si $f(x)|g(x)h(x)$ entonces $f(x)|g(x)$ o $f(x)|h(x)$.
2. $f(x)$ es un polinomio irreducible.
3. El ideal (f) es un ideal maximal.
4. El ideal (f) es un ideal primo.
5. El anillo cociente $F[x]/(f)$ es un cuerpo.

En general decidir si un polinomio $f(x) \in F[x]$ es irreducible es un problema difícil, estudiemos un criterio de irreducibilidad

Criterio de irreducibilidad de Eisenstein: Si A es un dominio de factoriazación única y F es su cuerpo cociente, si $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, con $n \geq 1$ y existe un primo $p \in A$ tal que $p \not| a_n$, $p|a_i$, con $i = 1, ..., n-1$ y $p^2 \not| a_0$, entonces $f(x)$ es irreducible en $F[x]$.

Por ejemplo sea $f(x) = 2x^5 - 6x^3 + 9x^2 - 15 \in \mathbb{Z}[x]$, entonces por el criterio de Eisenstein tomando $p = 3$ tenemos que $f(x)$ es irreducible en $\mathbb{Q}[x]$ y en $\mathbb{Z}[x]$.

Ejercicio 1. Demostrar que el polinomio $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ es irreducible sobre $\mathbb{Q}$ para todo número primo p.

Ejercicio 2. Sea $f \in \mathbb{Z}[x]$ un polinomio mónico. Si p es un número primo, denotamos por $\overline{f} \in \mathbb{Z}_p[x]$ a la imagen de f bajo la proyección canónica $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$.

(i) Demostrar que si $\overline{f}$ es irreducible en $\mathbb{Z}_p[x]$ entonces f es irreducible en $\mathbb{Z}[x]$.
(ii) Demostrar que el polinomio $x^3 - 5x + 36$ es irreducible sobre $\mathbb{Z}[x]$.
(iii) Demostrar que el polinomio $x^6 + x^3 + 1$ es irreducible sobre $\mathbb{Z}[x]$.
(iv) Demostrar que la recíproca de (i) no es cierta.

Un *espacio vectorial* V sobre un cuerpo F es un conjunto no vacío junto con dos operaciones, una suma y una operación producto externa entre el conjunto V y el cuerpo F llamado producto por escalar tales que:

1. V es un grupo abeliano con la suma.
2. El producto por escalar $\cdot : F \times V \to V$. A la imagen de (r, v) la denotaremos rv. Se satisface las siguientes propiedades para todo $v, w \in V$ y para todo $r, s \in F$:
   a) $r(v + w) = rv + rw$,
   b) $(r + s)v = rv + sv$,
   c) $s(rv) = (sr)v$,
   d) $1_F v = v$.

Dados dos espacios vectoriales V, W sobre un cuerpo F una función T de V en W es una *transformación lineal* si para todo $v, w \in V$ y $k \in F$ se satisface que $T(v+w) = T(v) + T(w)$ y $T(kv) = kT(v)$. El conjunto de todas las transformaciones lineales forman a su vez un espacio vectorial con la suma y producto por escalar usual de funciones. Denotamos por $\mathrm{Hom}_F(V, W)$ al espacio vectorial de las transformaciones F-lineales de V en W, $\mathrm{End}_F(V) = \mathrm{Hom}_F(V, V)$ y

$$\mathrm{Aut}_F(V) = \{T \in \mathrm{End}_F(V) : T \text{ es biyectiva } \}.$$

2. Extensiones de cuerpos

Un cuerpo L es una *extensión* de un cuerpo F si F es un subcuerpo de L y se denota L/F. El cuerpo L posee una estructura natural de F-espacio vectorial, este induce la siguiente definición:

Definición 2.1. La dimensión de L como F-espacio vectorial se denomina el *grado de* L/F y se denota por $[L : F]$. L se dice una *extensión finita* o *infinita* de F según si $[L : F]$ es finito o no.

Por ejemplo el cuerpo de los números complejos $\mathbb{C}$ es una extensión de grado 2 de los números reales dado que $\{1, i\}$ es una base de $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial, mientras que $\mathbb{R}$ es una extensión infinita de los números racionales $\mathbb{Q}$.

Si L es una extensión de F y A es un subconjunto de L denotamos por $F[A]$ al subanillo de L generado por F y A, es decir a la intersección de todos los subanillos de L que contienen a F y a A y denotamos $F(A)$ al subcuerpo generado por F y A, que es la intersección de todos los subcuerpos de L que contienen a F y a A. Si A es un conjunto finito, $A = \{\alpha_1, \ldots, \alpha_n\}$ $F[A]$ y $F(A)$ se escriben $F[\alpha_1, \ldots, \alpha_n]$ y $F(\alpha_1, \ldots, \alpha_n)$ respectivamente.

Teorema 2.2. *Si L/F es una extensión y A es un subconjunto de L no vacio, entonces:*

1. $F[A] = \{f(\alpha_1, \ldots, \alpha_n) : n \in \mathbb{N},\ f \in F[X_1, \ldots X_n],\ \alpha_1, \ldots, \alpha_n \in A\}$.
2.

$$F(A) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : n \in \mathbb{N},\ f, g \in F[X_1, \ldots X_n],\ \alpha_1, \ldots, \alpha_n \in A, \right.$$
$$\left. g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

La demostración queda como ejercicio a desarrollar en las horas de práctico del curso.

Definición 2.3. Sea L una extensión de F. Un elemento $\alpha \in L$ se dice *algebraico* sobre F si existe un polinomio $p \in F[x]$ tal que $p(\alpha) = 0$. Si todo elemento de L es algebraico sobre F se dice que la extensión L/F es *algebraica*. Si α no es algebraico se dice *trascendente*.

Por ejemplo $i \in \mathbb{C}$ es algebraico sobre $\mathbb{R}$ y $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$. Por otro lado Hermite probó en 1873 que el número e es trascendente y Lindemann que π lo es en 1882.

Si $\alpha \in L$ es algebraico, se define a $p_{F,\alpha}$ al polinomio mónico en $F[x]$ de menor grado de todos los $p \in F[x]$ tales que $p(\alpha) = 0$. Resulta que $p_{F,\alpha}$ es el generador del ideal $Ker(ev_\alpha) \subseteq F[x]$, donde $ev_\alpha : F[x] \to L$ es la función $ev_\alpha(f) = f(\alpha)$. Si F/K es una extensión entonces $p_{K,\alpha}$ divide a $p_{F,\alpha}$.

Ejercicio 3. Sea $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Demostrar que $\sqrt[4]{2}$ es algebraico sobre $\mathbb{Q}$ y sobre $\mathbb{Q}(\sqrt{2})$. Comprobar que sobre $\mathbb{Q}$ el polinomio minimal de $\sqrt[4]{2}$ es $x^4 - 2$ pero no es minimal sobre $\mathbb{Q}(\sqrt{2})$.

Proposición 2.4. *Sea L una extensión de F y $\alpha \in L$ algebraico sobre F. Entonces*

1. *el polinomio $p_{F,\alpha}$ es irreducible.*
2. *Si $g \in F[x]$, entonces $g(\alpha) = 0$ si y sólo si $p_{F,\alpha}$ divide a g.*
3. *Si $n = gr(p_{F,\alpha})$ entonces $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es base de $F(\alpha)$ como F-espacio vectorial. Además $F(\alpha) = F[\alpha]$.*

Demostración. (1) Como $F[x]/(p_{F,\alpha}) \simeq F[\alpha]$ que es un dominio íntegro, entonces el ideal $(p_{F,\alpha})$ es primo y así/ $p_{F,\alpha}$ es irreducible.

(2) Sea $g \in F[x]$ tal que $g(\alpha) = 0$, entonces $g \in Ker(ev_\alpha)$ pero como este ideal está generado por $p_{F,\alpha}$ entonces $p_{F,\alpha}$ divide a g. La recíproca es evidente.

(3) Como el ideal $(p_{F,\alpha})$ es maximal, el cociente $F[x]/(p_{F,\alpha}) \simeq F[\alpha]$ es un cuerpo y por lo tanto $F[\alpha] = F(\alpha)$. Si $\beta \in F(\alpha)$ entonces $\beta = g(\alpha)$ par algun $g \in F[x]$. Entonces existen polinomios $q, r \in F[x]$ tales que

$$g(x) = q(x)p_{F,\alpha}(x) + r(x),$$

donde $r = 0$ o bien $gr(r) < n$. Entonces $\beta = r(\alpha)$. Lo cual demuestra que el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es un sistema de generadores de $F(\alpha)$. Sean $a_i \in F$ tales que

$$\sum_{i_0}^{n-1} a_i \alpha^i = 0,$$

entonces $f(x) = \sum_{i_0}^{n-1} a_i\, x^i$ es divisible por $p_{F,\alpha}$ lo cual implica, ya que $gr(f) \leq n-1$, que $f = 0$. Luego $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base. □

Ejercicio 4. Sea $\zeta \neq 1$ una raíz de $x^3 - 1$. Demostrar que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.

Ejercicio 5. Demostrar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ y hallar el índice $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$.

Ejercicio 6. Demostrar que $[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}] = 8$.

Lema 2.5. *Sea L/F una extensión y K un cuerpo intermedio $K \subset F \subset L$ entonces*

1. *Si L/F es una extensión es finita entonces L es algebraico sobre F.*
2. *$[L : F] = [L : K]\,[K : F]$.*
3. *Si $\{\alpha_1, \ldots, \alpha_n\} \in L$ es un conjunto de escalares algebraicos sobre F entonces $F[\alpha_1, \ldots, \alpha_n]$ es un cuerpo y*

$$[F[\alpha_1, \ldots, \alpha_n] : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F].$$

Demostración. (1) Supongamos que $[L : F] = n$ y sea $a \in L$. El conjunto $\{1, a, \ldots, a^n\}$ es linealmente dependiente y por lo tanto existen $\lambda_i \in F$ no todos nulos tal que $\sum_{i=0}^{n} \lambda_i a^i = 0$. Si denotamos $f = \sum_{i=0}^{n} \lambda_i x^i \in F[x]$ entonces $f \neq 0$ y $f(a) = 0$ por lo tanto a es algebraico sobre F.

(2) Sea $\{a_1, \ldots, a_n\}$ una base de K como F-espacio vectorial y sea $\{b_1, \ldots, b_m\}$ una base de L como K-espacio vectorial. El conjunto $\{a_i b_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ es una base de L como F-espacio vectorial. La demostración de este hecho queda como ejercicio para el lector.

(3) Lo demostraremos por inducción en n. Asumamos que $n = 1$. Consideramos la aplicación $ev_{\alpha_1} : F[x] \to L$, $ev_{\alpha_1}(f) = f(\alpha_1)$. Como α_1 es algebraico entonces el nucleo de ev_{α_1} es un ideal no nulo de $F[x]$ que es primo. Como todo ideal primo de $F[x]$ es maximal se tiene que $F[x]/ker(ev_{\alpha_1}) \simeq F[\alpha_1]$ es un cuerpo y por lo tanto $F[\alpha_1] = F(\alpha_1)$.

Sea $K = F[\alpha_1, \ldots, \alpha_{n-1}]$. Por inducción se tiene que K es un cuerpo y $[K : F] \leq \prod_{i=1}^{n-1} [F(\alpha_i) : F]$. Como p_{K,α_n} divide a p_{F,α_n} entonces tenemos que

$$[F[\alpha_1, \ldots, \alpha_n] : K] \leq [F(\alpha_n) : F],$$

por lo tanto usando el resultado anterior se deduce que

$$[F[\alpha_1, \ldots, \alpha_n] : F] = [F[\alpha_1, \ldots, \alpha_n] : K][K : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F].$$

□

La desigualdad anterior puede ser estricta. Como los polinomios $x^4 - 18$ y $x^4 - 2$ son irreducibles sobre $\mathbb{Q}$ (demostrar) se tiene que $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4 = [\mathbb{Q}(\sqrt[4]{18}) : \mathbb{Q}]$. Demostremos que $[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}] = 8$. Para esto demostremos que $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$. Para ver esta igualdad notemos que $(\frac{\sqrt[4]{18}}{\sqrt[4]{2}})^2 = 3$, por lo tanto $\sqrt{3} \in \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18})$, es decir $\mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$ es un subcuerpo de $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18})$. Como $\sqrt[4]{18}$ es raíz del polinomio $x^2 - 3\sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})[x]$ entonces $[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}(\sqrt[4]{2})] \leq 2$. Luego

$$[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \leq 8 = [\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}].$$

Corolario 2.6. *Si L es una extensión de F entonces $\alpha \in L$ es algebraico si y sólo si $[F(\alpha) : F] < \infty$.* □

Ejercicio 7. Sea $\Bbbk$ un cuerpo. Consideremos el cuerpo de funciones racionales $\Bbbk(t)$ en una variable. Sea $\phi \in \Bbbk(t)$ tal que $\phi \notin \Bbbk$. Demostrar que $[\Bbbk(t) : \Bbbk(t)(\phi)] < \infty$.

Definición 2.7. Sea L/F una extensión y $f \in F[x]$ un polinomio.

1. Decimos que f se *factorea* sobre L si existen $a_1, \ldots a_n \in L$ tales que
$$f(x) = a_1(x - a_2) \ldots (x - a_n).$$
2. Se dice que L es un *cuerpo de raíces* de f si f se factorea sobre L y además $L = F(\alpha_1, \ldots \alpha_n)$ donde α_i son las raíces de f, éste es el menor subcuerpo de L que satisface esta propiedad.

El siguiente resultado muestra la existencia del cuerpo de raíces de un polinomio dado.

Teorema 2.8. *Si F es un cuerpo y $f(x) \in F[x]$ un polinomio de grado mayor o igual a uno, entonces existe una extensión de L de F tal que $f(x) = a(x - c_1)...(x - c_n)$ con $a \in F$ y $c_1, ..., c_n \in L$.*

Demostración. La existencia se demuestra por inducción en el grado del polinomio. Si $f(x) \in F[x]$ tiene grado 1, $L = F$ satisface el teorema. Sea $gr(f) = n$ y supongamos que el teorema es válido para todo polinomio no constante de grado menor que n. Si $f(x)$

es irreducible $F_1 = F[x]/(f(x))$ es un cuerpo que contiene a F, pues como $F[x]$ es un dominio euclideano y f es irreducible entonces el ideal $(f(x))$ es maximal, por lo tanto el anillo cociente $F[x]/(f(x))$ es un cuerpo. Si identificamos a cada $k \in F$ con su clase de equivalencia $\overline{k}$ en $F[x]/(f(x))$, tenemos que F_1 es una extensión de F. Si $c_1 = \overline{x} \in F_1$ es la clase de equivalencia que contiene al polinomio x entonces $f(\overline{x}) = \overline{f(x)} = 0$. Luego $f(x) = (x - c_1)g(x)$ en $F_1[x]$. Por hipótesis inductiva existe una extensión F_2 de F_1 tal que $g(x) = (x - c_2)...(x - c_n)$ con $c_2, ..., c_n \in F_2$. Entonces $L = F_2$. Si $f(x)$ no es irreducible, entonces $f(x) = g(x)h(x)$ con $1 \leq gr(g(x)), gr(h(x)) < n$. Por hipótesis inductiva, existe una extensión F_1 de F tal que $g(x) = a(x - c_1)...(x - c_r)$ con $c_1, ..., c_r \in F_1$. Como $F[x] \subset F_1[x]$, podemos aplicar la hipótesis inductiva en el polinomio $h(x) \in F_1[x]$. Entonces existe una extensión F_2 de F_1, y por lo tanto una extensión de F. Por lo tanto podemos tomar $L = F_2$. □

Por ejemplo, consideremos $f(x) = x^2 + x + 1$ sobre $\mathbb{Z}_2$. El polinomio f es irreducible pues $p(0) = 1 = p(1)$. Dado que $\mathbb{Z}_2$ no está contenido en $\mathbb{C}$ usaremos la construcción básica del cuerpo de raíces de f.

Como f es irreducible, entonces se puede construir una extensión $\mathbb{Z}_2(\zeta)$ de $\mathbb{Z}_2$ siguiendo el método del teorema, donde ζ es una raíz de f. Sea $\varphi : \mathbb{Z}_2[x] \to \mathbb{Z}_2[x]/(f(x))$ siendo $\zeta = \varphi(x)$. El número ζ tiene a f como polinómio minimal sobre $\mathbb{Z}_2$, luego $[\mathbb{Z}_2(\zeta), \mathbb{Z}_2] = 2$ y $\zeta^2 + \zeta + 1 = 0$, por lo que $\zeta^2 = 1 + \zeta$. El conjunto $\{1, \zeta\}$ es una base de $\mathbb{Z}_2(\zeta)$ sobre $\mathbb{Z}_2$, de modo que los elementos de $\mathbb{Z}_2(\zeta)$ son $0, 1, \zeta, 1 + \zeta$.

Las tablas de suma y producto son las siguientes:

$+$	0	1	ζ	$1+\zeta$
0	0	1	ζ	$1+\zeta$
1	1	0	$1+\zeta$	ζ
ζ	ζ	$1+\zeta$	0	1
$1+\zeta$	$1+\zeta$	ζ	1	0

$\cdot$	0	1	ζ	$1+\zeta$
0	0	0	0	0
1	0	1	ζ	$1+\zeta$
ζ	0	ζ	$\zeta+1$	1
$1+\zeta$	0	$1+\zeta$	1	ζ

En $\mathbb{Z}_2(\zeta)[x]$ el polinomio f se descompone como

$$f(x) = (x - \zeta)(x - 1 - \zeta).$$

Ejercicio 8. Sea F un cuerpo, $f \in F[x]$ un polinomio de grado n. Si L es su cuerpo de raíces entonces $[L : F] \leq n!$. Ayuda: demostrarlo por inducción en n.

Ejercicio 9. Demostrar que los polinomios $p(x) = x^2 - 2x + 2$ y $q(x) = x^2 + 1$ son irreducibles sonbre $\mathbb{Q}$ y ambos tienen a $\mathbb{Q}(i)$ como cuerpo de raíces sobre $\mathbb{Q}$.

Ejercicio 10. Construir los cuerpos de raíces de $f(x) = x^3+2x+1$ y $g(x) = x^3+x^2+x+2$ sobre $\mathbb{Z}_3$. Son isomorfos entre si?

Ejercicio 11. Sea $f(x) = x^3 - 2$. Encontrar el cuerpo L de raíces de f. Existe un $\zeta \in \mathbb{C}$ tal que $L = \mathbb{Q}(\zeta)$?

Teorema 2.9. *Sea $F \subseteq K \subseteq L$ una extensión de cuerpos. Si K es algebraico sobre F y L es algebraico sobre K entonces L es algebraico sobre F.*

Demostración. Sea $\alpha \in L$. Denotemos $p_{K,\alpha}(x) = a_0 + a_1x - \cdots + a_nx^n$. Como K/F es una extensión algebraica el cuerpo $K_0 = F(a_0, \ldots, a_n)$ es una exensión finita de F. El polinomio $p_{K,\alpha}$ pertenece a $K_0[x]$ por lo tanto α es algebraico sobre K_0 y por lo tanto

$$[K_0(\alpha) : F] = [K_0(\alpha) : K_0][K_0 : F] < \infty.$$

Como $F(\alpha) \subseteq K_0(\alpha)$ tenemos que $[F(\alpha) : F] < \infty$ y así α es algebraico sobre F. □

Definición 2.10. Sea L/F una extensión. El conjunto

$$\{\alpha \in L : \alpha \text{ es algebraico sobre } L\}$$

es llamado *la clausura algebraica* de F en L.

El siguiente corolario se deja como ejercicio para el lector.

Corolario 2.11. *Sea L/F una extensión y sea K la clausura algebraica de F en L. Entonces K es un cuerpo y es la extensión algebraica más grande contenida en L.*

Ejercicio 12. Sea L/F una extensión y sea $\alpha \in L$ tal que $[F(\alpha) : F]$ es impar. Demostrar que $F(\alpha) = F(\alpha^2)$

Ejercicio 13. Sea L una extensión algebraica de F y sea $F \subseteq R \subseteq L$ un subanillo. Demostrar que R es un cuerpo.

3. El grupo de Galois de una extensión

Si L es un cuerpo los automorfismos de anillo de L forman un grupo $\mathrm{Aut}(L)$ con respecto a la composición de aplicaciones.

Definición 3.1. Si L/F es una extensión, llamaremos el *grupo de Galois* de L sobre F al subgrupo $\mathrm{Aut}_F(L)$ de $\mathrm{Aut}(L)$ formado por los F-automorfismos y lo denotamos por $\mathrm{Gal}(L/F)$. Es decir aquellos automorfismos que además son transformaciones lineales de F-espacios vectoriales.

Ejercicio 14. Demostrar que $\mathrm{Aut}(\mathbb{R}) = \{id\}$.

Por ejemplo si $F = L$ entonces $\mathrm{Gal}(L/F) = \{id\}$. Notemos que si $\sigma \in \mathrm{Aut}_F(L)$ entonces $\sigma_{|F} = id$ pues como es un homomorfismo de anillo $\sigma(1_L) = 1_L$ y si $\alpha \in F$

$$\sigma(\alpha) = \sigma(\alpha 1_L) = \alpha\sigma(1_L) = \alpha 1_L = \alpha$$

para analizar ejemplos más complejos estudiemos primero el siguiente resultado

Lema 3.2. *Sea F/L una extensión y $p \in F[x]$. Si $\alpha \in F$ es una raíz de p y $\sigma \in \mathrm{Aut}_F(L)$, entonces $\sigma(\alpha) \in F$ es también raíz de p.*

Demostración. Si $p = \sum_{i=1}^{n} k_i x^i$, entonces $p(\alpha) = 0$ implica

$$0 = \sigma(p(\alpha)) = \sigma\left(\sum_{i=1}^{n} k_i \alpha^i\right) = \sum_{i=1}^{n} k_i \sigma(\alpha)^i = p(\sigma(\alpha)).$$

□

Una de las principales aplicaciones de este resultado es en la situación donde α es algebraico sobre F con polinomio irreducible $p \in F[X]$ de grado n, pues cualquier $\sigma \in \mathrm{Aut}_F(F(\alpha))$ esta completamente determinado por su acción en α, pues $\{1, \alpha, ..., \alpha^{n-1}\}$ es una base de $F(\alpha)$ sobre F.

Por ejemplo $\mathbb{C} = \mathbb{R}(i)$ y $\pm i$ son raíces de $p(x) = x^2 + 1$, entonces $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ tiene orden a lo sumo dos. Es fácil verificar que la conjugación compleja $(a + ib \to a - ib)$ es un $\mathbb{R}$-automorfismo de $\mathbb{C}$ que es distinto a la identidad, por lo tanto $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}_2$. De manera análoga pruebe que $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}_2$.

Ejemplo 3.3. Consideremos el polinomio $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$. El cuerpo de raíces de f es $\mathbb{Q}(\sqrt{2},\sqrt{3})$ y sabemos que $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$, es decir que

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}.$$

Nos preguntamos cual es el grupo de Galois de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

Si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ entonces σ aplicada a una raíz de x^2-2 da como resultado otra raíz de x^2-2. Lo mismo ocurre con las raíces de x^2-3. Por lo tanto $\sigma(\sqrt{2}) = \pm\sqrt{2}$ y $\sigma(\sqrt{3}) = \pm\sqrt{3}$. El valor de $\sigma(\sqrt{6})$ queda determinado por los anteriores valores. Por lo tanto $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ tiene cuatro elementos: $\{id, \sigma_1, \sigma_2, \sigma_3\}$ donde

$$\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6},$$
$$\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6},$$
$$\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.$$

Se puede comprobar facilmente que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Ejemplo 3.4. En el anterior ejemplo teníamos que el cardinal del grupo de Galois coincidía con el índice de la extensión. Veamos un ejemplo en el cual esto no se cumple. Determinemos que grupo de Galois de la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Un automorfismo de $\mathbb{Q}(\sqrt[3]{2})$ que fije a $\mathbb{Q}$ debe aplicar $\sqrt[3]{2}$ a otra raíz del polinomio x^3-2, pero $\sqrt[3]{2}$ es la única raíz del polinomio x^3-2 en el cuerpo $\mathbb{Q}(\sqrt[3]{2})$ por lo tanto $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ es trivial. Sin embargo $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Ejercicio 15. Demostrar que si $\Bbbk$ es un cuerpo entonces $\mathrm{Gal}(\Bbbk(t)/\Bbbk) \simeq PGL_2(\Bbbk)$. Recordemos que el grupo $PGL_2(\Bbbk)$ es llamado el *grupo general lineal proyectivo* y se define como el cociente $GL_2(\Bbbk)/\{\Bbbk Id\}$.

Ayuda: Definamos $\phi : GL_2(\Bbbk) \to \mathrm{Gal}(\Bbbk(t)/\Bbbk)$ como sigue. Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ entonces

$$\phi(A)(t) = \frac{at+b}{ct+d}.$$

De esta manera queda bien definida la función $\phi(A) : \Bbbk(t) \to \Bbbk(t)$

Lema 3.5. *Si L/F es una extensión finita entonces* $|\ \mathrm{Gal}(L/F)\ | \leq [L:F]$.

Demostración. Asumamos que $m = |\ \mathrm{Gal}(L/F)\ | > [L:F] = n$.

Sea $\{\sigma_1,\ldots,\sigma_m\} = \mathrm{Gal}(L/F)$ y sea $\{\alpha_1,\ldots,\alpha_n\}$ una base de L como F-espacio vectorial. Como $m > n$ el sistema de ecuaciones

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_m(\alpha_1)x_m = 0 \\ \sigma_1(\alpha_2)x_1 + \cdots + \sigma_m(\alpha_2)x_m = 0 \\ \cdots \\ \sigma_1(\alpha_n)x_1 + \cdots + \sigma_m(\alpha_n)x_m = 0 \end{cases}$$

posee una solución no trivial, digamos $(\lambda_1,\ldots,\lambda_m) \in L^m$. Esto implica que $\sum_{i=0}^m \lambda_i\sigma_i = 0$ en $\mathrm{Aut}(L)$. Esto es una contradicción pues cualquier conjunto finito de elementos distintos de un grupo son linealmente independientes en el álgebra de grupo. □

Si $G \subseteq \mathrm{Aut}(L)$ es un subconjunto, definimos

$$\mathcal{F}(G) = \{a \in L : \sigma(a) = a \ \text{ para todo } \sigma \in G\}.$$

Las siguientes propiedades son inmediatas de verificar.

Lema 3.6. 1. *$\mathcal{F}(G)$ es un subcuerpo de L.*
2. *Si $k \subseteq K \subseteq L$ entonces* $\mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/k)$.
3. *Si $G_1 \subseteq G_2 \subseteq \mathrm{Aut}(L)$ entonces $\mathcal{F}(G_2) \subseteq \mathcal{F}(G_1)$.*
4. *Si $G \subseteq \mathrm{Aut}(L)$ entonces $G \subseteq \mathrm{Gal}(L/\mathcal{F}(G))$.*
5. *Si $G \subseteq \mathrm{Aut}(L)$ entonces $\mathcal{F}(G) = \mathcal{F}(\mathrm{Gal}(L/\mathcal{F}(G)))$.*
6. *Si L/K es una extensión entonces* $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/\mathcal{F}(\mathrm{Gal}(L/K)))$.

Demostración. Las partes (1),(2),(3) y (4) son inmediatas y se dejan como ejercicio para el lector.

Sea $G \subseteq \mathrm{Aut}(L)$ un subconjunto y $F = \mathcal{F}(G) \subseteq L$. Entonces por definición $G \subseteq \mathrm{Gal}(L/F)$ por lo tanto $\mathcal{F}(\mathrm{Gal}(L/F)) \subseteq \mathcal{F}(G) = F$. Pero $F \subseteq \mathcal{F}(\mathrm{Gal}(L/F))$, luego $F = \mathcal{F}(\mathrm{Gal}(L/\mathcal{F}(G)))$ y (5) queda demostrado.

Para la parte (6) sabemos que $K \subseteq \mathcal{F}(\mathrm{Gal}(L/K)) \subseteq L$, luego sigue de la parte (2) que

$$\mathrm{Gal}(L/\mathcal{F}(\mathrm{Gal}(L/K))) \subseteq \mathrm{Gal}(L/K).$$

La parte (4) implica que $\mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/\mathcal{F}(\mathrm{Gal}(L/K)))$, lo cual finaliza la demostración. □

En conclusión, si L/F es una extensión se tiene una correspondencia:

$$\left\{\begin{array}{c}\text{Subgrupos } G \subseteq \mathrm{Gal}(L/F)\\ \text{de la forma } G = \mathrm{Gal}(L/K)\\ \text{para alguna}\\ \text{extensión } F \subseteq K \subseteq L\end{array}\right\} \begin{array}{c}\xrightarrow{\mathcal{F}(-)}\\ \xleftarrow{Gal(L/-)}\end{array} \left\{\begin{array}{c}\text{Subcuerpos de } K \subseteq L\\ \text{tales que } F \subseteq K\\ \text{y } K = \mathcal{F}(G) \text{ para algun}\\ \text{subgrupo } G \subseteq \mathrm{Aut}(L)\end{array}\right\}$$

Cabe preguntarse ahora bajo que hipótesis la correspondecia $K \longleftrightarrow \mathrm{Gal}(L/K)$ establece una biyección entre *todos* los sucuerpos de L que contienen a F y *todos* los subgrupos de $\mathrm{Gal}(L/F)$. La parte (5) del Lema anterior nos dice que una condición necesaria es que $K = \mathcal{F}(\mathrm{Gal}(L/K)$. Veremos más adelante que esta condición es también suficiente.

Proposición 3.7. *Sea L/F una extensión finita. Si $F = \mathcal{F}(G)$ para un grupo finito $G \subseteq \mathrm{Aut}(L)$, entonces $\mid G \mid = [L : F]$ y por lo tanto $G = \mathrm{Gal}(L/F)$.*

Demostración. Por el lema 3.6 parte (4) se tiene que $G \subseteq \mathrm{Gal}(L/\mathcal{F}(G))$ y por lo tanto

$$\mid G \mid \leq \mid \mathrm{Gal}(L/\mathcal{F}(G)) \mid \leq [L : \mathcal{F}(G)] \leq [L : F].$$

Asumamos que $n = \mid G \mid < [L : F]$. Sean $\alpha_1, \ldots, \alpha_{n+1} \in L$ elementos linealmente independientes sobre F y $G = \{\sigma_1, \ldots, \sigma_n\}$. Definamos la matriz

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_{n+1}) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_{n+1}) \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_{n+1}) \end{pmatrix}.$$

Las columnas de A son linealmente dependientes sobre L. Elijamos un k minimal de tal manera que las primeras k columnas de la matriz A son linealmente dependientes (permutandolas si es necesario). Por lo tanto existen escalares $c_i \in L$ tales que

$$\sum_{i=1}^{k} c_i \sigma_j(\alpha_i) = 0 \tag{3.1}$$

para todo j. La minimalidad de k implica que $c_i \neq 0$ para todo $i = 1 \dots k$, por lo que podemos asumir que $c_1 = 1$.

No todos los c_i pertenecen a F ya que, en este caso, $0 = \sum_{i=1}^{k} \sigma_j(c_i\alpha_i)$ pero esto implica que $0 = \sum_{i=1}^{k} c_i\alpha_i$ lo cual no puede ser por que $\alpha_1, \dots, \alpha_{n+1}$ son F-independientes. Tomemos $\sigma \in G$ un elemento y se lo aplicamos a la ecuación (3.1):

$$0 = \sum_{i=1}^{k} \sigma(c_i)\sigma\sigma_j(\alpha_i).$$

Como multiplicar por un elemento en un grupo permuta los elementos, obtenemos que $0 = \sum_{i=1}^{k} \sigma(c_i)\sigma_j(\alpha_i)$ para todo $\sigma \in G$. De esta útlima igualdad y (3.1) obtenemos que

$$0 = \sum_{i=2}^{k} (\sigma(c_i) - c_i)\sigma_j(\alpha_i).$$

Recordemos que elegimos $c_1 = 1$. La minimalidad de k implica que $\sigma(c_i) - c_i = 0$ para todo $i = 2 \dots k$. Como esto es cierto para todo $\sigma \in G$ entonces $c_i \in F$. Pero hemos visto que esto no puede ser por lo cual $| G | = [L : F]$. □

Ejemplo 3.8. Sea $\Bbbk$ un cuerpo y $F = \Bbbk(t_1, \dots, t_n)$ el cuerpo de funciones racionales en n variables sobre $\Bbbk$. Podemos ver al grupo simétrico $\mathbb{S}_n$ como un subgrupo de $\mathrm{Aut}(F)$ de la siguiente manera:

$$\sigma\left(\frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)}\right) = \frac{f(t_{\sigma(1)}, \dots, t_{\sigma(n)})}{g(t_{\sigma(1)}, \dots, t_{\sigma(n)})},$$

para todo $\sigma \in \mathbb{S}_n$. Sea $K = \mathcal{F}(\mathbb{S}_n)$ el *cuerpo de funciones simétricas*. Por la Proposición 3.7 tenemos que $\mathbb{S}_n = \mathrm{Gal}(F/K)$ y $[F : K] = n!$.

Sean $s_1, \dots, s_n$ las funciones simétricas elementales, es decir

$$s_1 = t_1 + \cdots + t_n, \quad s_2 = \sum_{i \neq j} t_i t_j, \quad \dots \quad s_n = t_1 \dots t_n.$$

Entonces $\Bbbk(s_1, \dots, s_n) \subseteq \mathcal{F}(\mathbb{S}_n)$. Afirmamos que $\Bbbk(s_1, \dots, s_n) = \mathcal{F}(\mathbb{S}_n)$. En efecto, sea

$$f(t) = t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n \in \Bbbk(s_1, \dots, s_n)[t].$$

Se puede verificar que $f(t) = (t - x_1) \dots (t - x_n) \in F[t]$, esto implica que el cuerpo de raíces de $f(t)$ sobre $\Bbbk(s_1, \dots, s_n)$ es F. El ejercicio 8 implica que $[F : \Bbbk(s_1, \dots, s_n)] \leq n!$ pero como $[F : K] = n!$ esto implica que necesariamente $\Bbbk(s_1, \dots, s_n) = \mathcal{F}(\mathbb{S}_n)$. En otras palabras, cualquier función simétrica puede ser escrita en terminos de las funciones simétricas elementales.

Definición 3.9. Si L/F es una extensión algebraica se dice que L es *Galois* sobre F si $F = \mathcal{F}(\mathrm{Gal}(L/F))$.

Corolario 3.10. *Sea L/F una extensión finita. Entonces L/F es una extensión Galois si y sólo si $|\mathrm{Gal}(L/F)| = [L : F]$.* □

El siguiente corolario queda como ejercicio para el lector.

Corolario 3.11. *Sea L/F una extensión y sea $\alpha \in L$ algebraico sobre F, entonces*

1. *$|\mathrm{Gal}(F(\alpha)/F)|$ es igual al número de raíces distintas de $p_{F,\alpha}$ en $F(\alpha)$.*
2. *$F(\alpha)$ es Galois sobre F si y sólo si $p_{F,\alpha}$ posee n raíces distintas, donde $n = gr(p_{F,\alpha})$.* □

Ejercicio 16. Demostrar que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es Galois.

Ejercicio 17. Sea $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ y sea F el cuerpo de raíces de f. Demostrar que $\mathrm{Gal}(F/\mathbb{Q}) = \mathbb{S}_5$.

Ejercicio 18. Sea $\Bbbk$ un cuerpo de caracteristica $p > 0$. Demostrar que $\mathrm{Gal}(\Bbbk(t)/\Bbbk(t^p)$ es trivial y que la extensión $\Bbbk(t)/\Bbbk(t^p)$ no es Galois.

4. El teorema fundamental de la teoría de Galois

Sea L/F una extensión y $\alpha \in L$. Por el Corolario 3.11 la extensión $F(\alpha)/F$ no es Galois cuando $p_{F,\alpha}$ no tiene todas las raíces en $F(\alpha)$ o $p_{F,\alpha}$ posee raíces repetidas. Estas dos situaciones son tratadas en el contexto de extensiones separables y normales.

Definición 4.1. Si L/F es una extensión, L se dice *normal* sobre F si L es el cuerpo de raíces de un conjunto de polinomios con coeficientes en F.

Definición 4.2.
(a) Sea F un cuerpo. Un polinomio irreducible $f \in F[x]$ se dice *separable* sobre F si f no posee raíces repetidas en su cuerpo de raíces. Un polinomio $g \in F[x]$ se dice *separable* sobre F si todos los factores irreducibles de g son separables.
(b) Sea L/F una extensión y $\alpha \in L$. Se dice que α es *separable* sobre F si $p_{F,\alpha}$ es separable sobre F. L se dice separable sobre F si todo elemento en L es separable sobre F.

El siguiente resultado se utilizará más adelante. Para su demostración el lector puede consutlar a [M].

Teorema 4.3. *Sea L una extensión algebraica sobre F. Las siguientes afirmaciones son equivalentes:*

(i) *L es Galois sobre F.*
(ii) *L es normal y separable sobre F.*
(iii) *L es el cuerpo de raíces de un conjunto de polinomios separables sobre F.*

□

Teorema 4.4. *Sea L/F una extensión finita Galois y $G = \mathrm{Gal}(L/F)$. Existe una correspondencia biunívoca entre cuerpos intermedios de la extensión L/F y subgrupos de G. Además*

1. *Si K se corresponde al subgrupo H entonces*

$$[L : K] = |H| \quad y \quad [K : F] = [G : H].$$

2. *Si K se corresponde al subgrupo H entonces H es un subgrupo normal si y sólo si K/F es una extensión normal y en este caso* $\mathrm{Gal}(K/F) \simeq G/H$.

Demostración. Sea $F \subseteq K \subseteq L$ extensiones de cuerpos. Como L/F es Galois entonces L/F es normal y separable, lo que implica que L/K es normal y separable y por lo tanto Galois. Entonces $K = \mathcal{F}(\mathrm{Gal}(L/K))$. Es decir todo cuerpo intermedio es de la forma $\mathcal{F}(H)$ para algún subgrupo H de G.

Sea $H \subseteq G$ un subgrupo. Como H es finito entonces por la Proposición 3.7 se tiene que $H = \mathrm{Gal}(L/\mathcal{F}(H))$. Luego la corresponcencia del Lema 3.6 establece una correspondencia entre todos los subcuerpos intermedios y los subgrupos de G.

Si K se corresponde con el subgrupo H entonces por la Proposición 3.7 se tiene que $\mid H \mid = [L : K]$ además

$$[G : H] = \frac{\mid G \mid}{\mid H \mid} = \frac{[L : F]}{[L : K]} = [K : F].$$

□

Ejercicio 19. Sea F un cuerpo de caracteristica distinta a 2 y sea L un extensión de F tal que $[L : F] = 2$. Demostrar que $L = F(\alpha)$ para algun $\alpha \in L$ tal que $\alpha^2 \in F$. Demostrar que L es Galois sobre F.

Ejercicio 20. Determinar cuales de los siguientes cuerpos son extensiones Galois de $\mathbb{Q}$.

(a) $\mathbb{Q}(\omega)$ donde $\omega = e^{\frac{2\pi i}{3}}$,
(b) $\mathbb{Q}(\sqrt[4]{2})$,
(c) $\mathbb{Q}(\sqrt{5}, \sqrt{7})$.

Veamos una consecuencia del Teorema 4.4.

Teorema 4.5. *Sea F un cuerpo infinito y sea L/F una extensión. Existe un $\alpha \in L$ tal que $L = F(\alpha)$ si y sólo si la cantidad de cuerpos intermedios $F \subseteq K \subseteq L$ es finita.*

Demostración. Asumamos que existen finitos cuerpos intermedios $F \subseteq K \subseteq L$. Entonces $L = F(\alpha_1, \ldots, \alpha_n)$ para algunos $\alpha_1, \ldots, \alpha_n \in L$. Razonemos por inducción en n. Si $n = 1$ el resultado es trivial. Si denotamos $K = F(\alpha_1, \ldots, \alpha_{n-1})$, entonces como todo cuerpo intermedio entre F y K es un cuerpo intermedio de la extensión L/F por inducción $K = F(\beta)$ y así/ $L = F(\beta, \alpha_n)$. Para cada $a \in F$ denotamos el cuerpo $\Bbbk_a = F(a\beta + \alpha_n)$. Como F es infinito y los cuerpos intermedios de la extensión L/F son finitos, existen $a, b \in F$ tales que $\Bbbk_a = \Bbbk_b$. Por lo tanto

$$\beta = \frac{(a\beta + \alpha_n) - (b\beta + \alpha_n)}{a - b} \in \Bbbk_b.$$

Por lo tanto $\alpha_n = (a\beta + \alpha_n) - a\beta \in \Bbbk_a$, luego $L = \Bbbk_a$.

Recíprocamente, supongamos que $L = F(\alpha)$ y sea K un cuerpo tal que $F \subseteq K \subseteq L$. Entonces $L = K(\alpha)$. Sabemos que $p_{K,\alpha}$ divide a $p_{F,\alpha}$ en $K[x]$. Supongamos que

$$p_{K,\alpha} = a_0 + a_1 x + \cdots + x^r \in K[x].$$

Denotemos $K_0 = F(a_0, \ldots, a_{r-1}) \subseteq K$. Entonces $p_{K_0,\alpha}$ divide a $p_{K,\alpha}$. Por lo tanto

$$[L : K] = deg(p_{K,\alpha}) \geq deg(p_{K_0,\alpha}) = [L : K_0] = [L : K][K : K_0].$$

Entonces $[K : K_0] = 1$ y $K = K_0$, y por lo tanto K está determinado por $p_{K,\alpha}$. Como hay finitos divisores mónicos de $p_{F,\alpha}$ en $L[x]$ entonces existen finitas extensiones intermedias. □

Corolario 4.6. *Sea F un cuerpo infinito y sea L/F una extensión finita y separable. Entonces existe un $\alpha \in L$ tal que $L = F(\alpha)$.*

Demostración. Como la extensión L/F es finita y separable existen $\alpha_1, \ldots, \alpha_n \in L$ tales que $L = F(\alpha_1, \ldots, \alpha_n)$. Sea K el cuerpo de raíces del conjunto de polinomios $\{p_{F,\alpha_i} : 1 \leq i \leq n\}$. Como cada polinomio p_{F,α_i} es separable por el Teorema 4.3 la extensión K/F es Galois. Además $K \subseteq L$. Luego por el Teorema 4.4 los cuerpos intermedios $F \subseteq K' \subseteq K$ están en correspondencia con los subgrupos de $\mathrm{Gal}(K/F)$. Como $\mathrm{Gal}(K/F)$ es finito la cantidad de dichos cuerpos intermedios es finita. Por lo tanto los cuerpos intermedios de la extensión L/F es finita y el resultado sigue del Teorema 4.5.

□

Ejercicio 21. Sea p un número primo, $f(x) = x^n - p \in \mathbb{Q}[x]$ y L el cuerpo de raíces de f. Demostrar que para todo $n \geq 3$ el grupo $\mathrm{Gal}(L/\mathbb{Q})$ no es Abeliano.

Ejercicio 22. Sea F un cuerpo y $f \in F[x]$ un polinomio separable. Denotamos por L al cuerpo de raíces de f. Si $\alpha \in L$ es una raíz cualqueira y p es un primo que divide a $[L : F]$ demostrar que existe un subcuerpo $F \subseteq K \subseteq L$ tal que $L = K(\alpha)$ y $[L : K] = p$.

Ejercicio 23. Sea $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$ un polinomio irreducible. Demostrar que si F es el cuerpo de raíces de f y que $b > 0$ entonces $\mathrm{Gal}(F/\mathbb{Q}) = \mathbb{S}_3$.

Ejercicio 24. Sea $f(x) = x^6 - 14x^3 - 1 \in \mathbb{Q}[x]$. Sea F el cuerpo de raíces de f. Encontrar a F y calcular $\mathrm{Gal}(F/\mathbb{Q})$. Ayuda: $\alpha = \sqrt[3]{7 + 5\sqrt{2}}$ es raíz de f y $\alpha = \beta^3$ donde $\beta = 1 + \sqrt{2}$.

5. Solubilidad por radicales

Definición 5.1.
1. Una extensión L/F se dice una *extensión por radicales* si el cuerpo $L = F(a_1, \ldots, a_m)$ y existen enteros $n_1, \ldots, n_m$ tales que $a_1^{n_1} \in F$ y $a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$ para todo $i > 1$. Si $n = n_1 = \cdots = n_m$ entonces L se dice una extensión n-radical.
2. Un polinomio $f \in F[x]$ se dice *resoluble por radicales* si su cuerpo de raíces está contenido en una extensión por radicales de F.

Claramente si L es una extensión radical entonces es n-radical. Basta con tomar $n = n_1 \ldots n_m$.

Ejemplo 5.2. $\mathbb{Q}(\sqrt[4]{2})$ es una extensión 4-radical de $\mathbb{Q}$, pero también es una extensión 2-radical. Para ver esto último hay que considerar las extensiones

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{\sqrt{2}}) = \mathbb{Q}(\sqrt[4]{2}).$$

El siguiente resultado debido a Galois caracteriza aquellos polinomios que son resolubles por radicales.

Teorema 5.3. *Sea F un cuerpo de caracteristica cero y $f \in F[x]$. Si L es el cuerpo de raíces de f sobre F entonces f es resoluble por radicales si y sólo si el grupo* $\mathrm{Gal}(L/F)$ *es soluble.*

Ejercicio 25. Sea F la clausura algebraica de $\mathbb{F}_p$. Sea $L = F(x)$ y sea $f \in L[t]$ definido por $f(t) = t^p - t - x$. Llamemos a K al cuerpo de raíces de f sobre L. Demostrar que f no es resoluble por radicales sobre L y que el grupo de Galois $\mathrm{Gal}(K/L)$ es cíclico.

6. Apéndice: Grupos solubles

Un grupo G se dice soluble si existe una cadena de subgrupos

$$\{1\} \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G,$$

tal que G_i es un subgrupo normal en G_{i+1} y G_{i+1}/G_i es Abeliano.

Lema 6.1. *Sea G un grupo. Las siguientes afirmaciones se satisfacen:*

(i) *Si G es Abeliano entonces es soluble.*
(ii) *Si G es soluble entonces todo subgrupo y todo cociente de G son solubles.*
(iii) *Si $N \subseteq G$ es un subgrupo normal entonces G es soluble si y sólo si N y G/N son solubles.*

Ejemplo 6.2.
1. Los grupos $\mathbb{S}_2, \mathbb{S}_3, \mathbb{S}_4$ son solubles.
2. Los grupos $\mathbb{S}_n$ con $n \geq 5$ no son solubles.
3. Los grupos simples no Abelianos no son solubles.
4. Todo grupo finito de orden $p^a q^b$ con p, q primos es soluble (Teorema de Burnside).
5. Todo grupo de orden menor a 60 es soluble.
6. Todo grupo de orden impar es soluble (Teorema de Feit-Thompson).

Referencias

[E] H. Edwards, *Galois theory*, Graduate texts in mathematics, Springer-Verlag **101**, (1984).
[G] M. Gastaminza, *Extensiones Algebraicas y Teoría de Galois*, Notas de Curso (1), Universidad Nacional del Sur (1991).
[M] P. Morandi, *Field and Galois theory*, Graduate texts in mathematics, Springer-Verlag **167**, (1996).
[W] S. Weintraub, *Galois theory*, Universitext, Springer (2009).

Universidad Nacional de Córdoba, Universidad Nacional de Cuyo.
E-mail address: martin10090@gmail.com, sebastian.simondi@gmail.com

TEORÍA DE MÓDULOS

MARÍA JULIA REDONDO (TEORÍA), IGNACIO ZURRIAN (PRÁCTICA)

RESUMEN. Comenzamos este curso con la definición de módulo. Veremos que esta noción es una generalización natural de las nociones conocidas de grupo abeliano, de ideal de un anillo y de espacio vectorial. Presentaremos ejemplos de módulos. La manera natural de comparar módulos entre sí es considerar aplicaciones que respeten las estructuras definidas: morfismos de módulos. Introduciremos el concepto de sucesiones exactas para obtener herramientas que nos permitan probar diversos teoremas de isomorfismos de esta teoría. Estudiaremos los módulos libres, esto es, módulos que admiten bases. Veremos que no todo módulo admite base, y que dos bases de un módulo pueden no ser coordinables. Finalizaremos presentando una caracterización de aquellos anillos que tienen la propiedad IBN (invariant basis number), esto es, las bases de cualquier módulo libre tienen el mismo cardinal.

ÍNDICE

1. DEFINICIÓN Y EJEMPLOS

La noción de módulo es una generalización natural de las nociones de grupo abeliano, de ideal y de espacio vectorial.

Si M es un **grupo abeliano**, existe un morfismo de grupos $f_x : \mathbb{Z} \to M$ definido por $f_x(1) = x$. Dado $n \in \mathbb{Z}$, notemos $nx = f_x(n)$. Tenemos entonces que la aplicación $\mathbb{Z} \times M \to M$ dada por $(n, x) \mapsto nx$ verifica las siguientes propiedades:

(1) $(n + m)x = nx + mx$;
(2) $n(x + y) = nx + ny$;
(3) $(nm)x = n(mx)$;
(4) $1x = x$

para todo $n, m \in \mathbb{Z}$ y $x, y \in M$.

Los **espacios vectoriales** sobre un cuerpo K son otro ejemplo de una estructura similar. Recordemos que un espacio vectorial V sobre un cuerpo K es un grupo abeliano V con una aplicación $K \times V \to V$, $(k, v) \mapsto kv$, que satisface las condiciones:

(1) $(k + k')v = kv + k'v$;
(2) $k(v + w) = kv + kw$;

Date: 17 de abril de 2011.

(3) $(kk')v = k(k'v)$;
(4) $1v = v$

para todo $k, k' \in K$ y $v, w \in V$.

La similitud de estas estructuras sugiere que ellas son simplemente ejemplos de una noción más general.

Definición 1.1. Sea A un anillo. Un A-**módulo** consiste en un grupo abeliano M con una aplicación $A \times M \to M$ que notamos $(a, m) \mapsto am$ que verifica:

(1) $(a + b)m = am + bm$;
(2) $a(m + n) = am + an$;
(3) $(ab)m = a(bm)$;
(4) $1m = m$

para todo $a, b \in A$ y $m, n \in M$.

Así tenemos que todo grupo abeliano es un $\mathbb{Z}$-módulo, y todo espacio vectorial es un K-módulo. De manera similar se puede observar que todo ideal I de un anillo A es un A-módulo.

Ejemplo 1.2. Dado un anillo A, la multiplicación define una estructura de A-módulo sobre el grupo abeliano A de manera evidente con la operación $A \times A \to A$ dada por $(a, b) \mapsto ab$.

Ejemplo 1.3. Si $f : A \to A'$ es un morfismo de anillos, la aplicación $A \times A' \to A'$ dada por $(a, a') \mapsto f(a)a'$ define una estructura de A-módulo sobre el grupo abeliano A'.

Ejemplo 1.4. Si V es un K-espacio vectorial, $\mathrm{End}_K(V)$ es un anillo y V admite una estructura de $\mathrm{End}_K(V)$-módulo vía la aplicación $\mathrm{End}_K(V) \times V \to V$ dada por $(T, v) \mapsto T(v)$.

Observación 1.5. En general, dados un anillo A y un grupo abeliano M, es posible definir distintas estucturas de A-módulo sobre M. Por ejemplo, el cuerpo $\mathbb{C}$ de los números complejos admite estructura de $\mathbb{C}$-módulo vía las aplicaciones $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ dadas por $(z_1, z_2) \mapsto z_1 z_2$ y $(z_1, z_2) \mapsto \overline{z_1} z_2$.

2. Morfismos

Fijado un anillo A estamos interesados en estudiar la familia de todos los A-módulos. La manera natural de comparar módulos entre sí es considerar aplicaciones que respeten las estructuras definidas, esto es, aplicaciones $f : M \to N$ que sean morfismos de grupos abelianos compatibles con la estructura de A-módulo.

Definición 2.1. Sean M, N dos A-módulos. Un **morfismo** de A-módulos de M en N es un morfismo de grupos abelianos $f : M \to N$ que satisface $f(am) = af(m)$ para todo $a \in A$ y $m \in M$.

Es fácil ver que una función $f : M \to N$ es un morfismo de A-módulos si y sólo si

$$f(am + bn) = af(m) + bf(n)$$

para todo $a, b \in A$ y $m, n \in M$. Cuando no haya lugar a dudas, llamaremos simplemente A-morfismo al morfismo de A-módulos.

Definición 2.2. Un A-morfismo $f : M \to N$ se dice un **isomorfismo** si existe un A-morfismo $g : N \to M$ tal que $fg = id_N$ y $gf = id_M$.

Lema 2.3. *Un A-morfismo $f : M \to N$ es un isomorfismo si y sólo si la función f es biyectiva.*

Definición 2.4. Sea $f : M \to N$ un A-morfismo.

(a) f se dice un **monomorfismo** si $fg = 0$ implica $g = 0$;
(b) f se dice un **epimorfismo** si $gf = 0$ implica $g = 0$.

Definición 2.5. Un subconjunto N de un A-módulo M se dice un A-**submódulo** de M si N es un A-módulo con las operaciones que hereda de M, es decir, la inclusión $N \hookrightarrow M$ es un morfismo de A-módulos.

Si N es un A-submódulo de M, la operación

$$A \times M/N \to M/N$$

definida por $(a, m + N) \mapsto am + N$ está bien definida y verifica los axiomas necesarios para dar a M/N una estructura de A-módulo. Diremos que M/N es el **módulo cociente** de M sobre N. Observar que la estructura de A-módulo definida sobre M/N es la única posible para asegurar que la proyección canónica $M \to M/N$ sea un A-morfismo.

Notemos que la estrucutra de A-submódulo de N es necesaria para que el cociente tenga una estructura de A-módulo inducida por la de M. Por ejemplo, si consideramos el $\mathbb{Q}$-módulo $\mathbb{Q}$, y tomamos su subgrupo aditivo $\mathbb{Z}$, el cociente $\mathbb{Q}/\mathbb{Z}$ no tiene estructura de $\mathbb{Q}$-módulo.

Observación 2.6. Si N es un A-submódulo de M entonces:

(1) La inclusión $N \hookrightarrow M$ es un monomorfismo;
(2) La proyección canónica $M \to M/N$ es un epimorfismo.

Dado $f : M \to N$ un A-morfismo, notaremos

(a) $\operatorname{Ker} f = \{m \in M : f(m) = 0\}$ y $\ker f : \operatorname{Ker} f \hookrightarrow M$ a la inclusión;
(b) $\operatorname{Im} f = f(M)$ e $\operatorname{im} f : \operatorname{Im} f \hookrightarrow N$ a la inclusión;
(c) $\operatorname{Coker} f = N/\operatorname{Im} f$ y $\operatorname{coker} f : N \twoheadrightarrow \operatorname{Coker} f$ a la proyección canónica.

Una demostración directa muestra que $\operatorname{Ker} f$ es un A-submódulo de M y que $\operatorname{Im} f$ es un A-submódulo de N.

Lema 2.7. *Sea $f : M \to N$ un A-morfismo.*

(a) *f es un monomorfismo si y sólo si f es inyectiva;*
(b) *f es un epimorfismo si y sólo si f es sobreyectiva;*
(c) *f es un isomorfismo si y sólo si f es monomorfismo y epimorfismo.*

Demostración.

(a) Si f es un monomorfismo, como la inclusión $\ker f : \operatorname{Ker} f \to M$ verifica $f \ker f = 0$ tenemos que $\ker f = 0$, y por lo tanto $\operatorname{Ker} f = 0$. Recíprocamente, si f es inyectiva y $fg = 0$, tenemos que $f(g(x)) = 0$ y por lo tanto $g(x) = 0$. Y esto para cualquier x en el dominio de g, luego $g = 0$.
(b) Si f es un epimorfismo, como la proyección canónica $\operatorname{coker} f : N \to \operatorname{Coker} f$ verifica que $\operatorname{coker} f f = 0$ tenemos que $\operatorname{coker} f = 0$, y por lo tanto $\operatorname{Coker} f = N/\operatorname{Im} f = 0$. Luego $\operatorname{Im} f = N$. Recíprocamente, si f es sobreyectiva y $gf = 0$, dado $n \in N$ existe $m \in M$ tal que $f(m) = n$, y por lo tanto $g(n) = gf(m) = 0$, y esto para todo $n \in N$. Luego $g = 0$.
(c) Inmediata por (a), (b) y el Lema 2.3.

□

Corolario 2.8. *Sea $f : M \to N$ un A-morfismo.*

(a) *f es un monomorfismo si y sólo si* $\operatorname{Ker} f = 0$*;*
(b) *f es un epimorfismo si y sólo si* $\operatorname{Coker} f = 0$*;*
(c) *f es un isomorfismo si y sólo si* $\operatorname{Ker} f = 0$ *y* $\operatorname{Coker} f = 0$.

3. Sucesiones exactas

Definición 3.1. Una sucesión de A-módulos y A-morfismos

$$\cdots \to M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \to \cdots$$

se dice **exacta** en M_i si $\operatorname{Im} f_{i+1} = \operatorname{Ker} f_i$. Se dice exacta si lo es en cada M_i.

Observemos que si la sucesión es exacta, las composiciones $f_i f_{i+1}$ son nulas, o equivalentemente, $\operatorname{Im} f_{i+1} \subseteq \operatorname{Ker} f_i$. Una sucesión que verifica $f_i f_{i+1} = 0$ para todo i se dice un **complejo**. Es evidente que toda sucesión exacta es un complejo, pero la recíproca no es cierta.

Sea $f : M \to N$ un A-morfismo. Las siguientes afirmaciones se deducen directamente de la definición:

(1) f es un monomorfismo si y sólo si $0 \to M \xrightarrow{f} N$ es exacta;
(2) f es un epimorfismo si y sólo si $M \xrightarrow{f} N \to 0$ es exacta;
(3) f es un isomorfismo si y sólo si $0 \to M \xrightarrow{f} N \to 0$ es exacta;
(4) La sucesión $0 \to \operatorname{Ker} f \hookrightarrow M \xrightarrow{f} N \twoheadrightarrow \operatorname{Coker} f \to 0$ es exacta.

Proposición 3.2. *Dado un diagrama conmutativo de A-módulos y A-morfismos con filas exactas de la forma*

$$\begin{array}{ccccccc} 0 & \longrightarrow & S & \xrightarrow{f} & M & \xrightarrow{g} & N \\ & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} \\ 0 & \longrightarrow & S' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' \end{array}$$

existe un único A-morfismo u que hace el primer cuadrado conmutativo. Además u es un monomorfismo si v lo es.

Demostración. Dado $s \in S$, $g'vf(s) = wgf(s) = 0$, entonces $vf(s) \in \operatorname{Ker} g' = \operatorname{Im} f'$. Por lo tanto $vf(s) = f'(s')$, y además s' es único pues f' es inyectiva. Definimos $u(s) = s'$. Veamos que u es A-morfismo. Dados $s_1, s_2 \in S$ existen únicos $s_1', s_2' \in S'$ tales que $vf(s_1) = f'(s_1')$ y $vf(s_2) = f'(s_2')$. Como

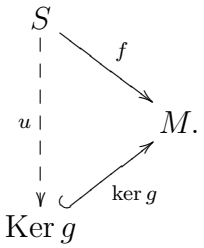
$$f'(as_1' + bs_2') = af'(s_1') + bf'(s_2') = avf(s_1) + bvf(s_2) = vf(as_1 + bs_2),$$

tenemos que $u(as_1 + bs_2) = as_1' + bs_2' = au(s_1) + bu(s_2)$.
La unicidad de u es clara por construcción, y u es un monomorfismo si v lo es pues $f'u = vf$.

□

Corolario 3.3. *Dada $0 \to S \xrightarrow{f} M \xrightarrow{g} N$ una sucesión exacta de A-módulos y A-morfismos, existe un único A-isomorfismo $u : S \to \operatorname{Ker} g$ que hace conmutativo al*

diagrama



Demostración. La proposición anterior nos dice que existe un único A-morfismo u que hace el diagrama

$$\begin{array}{ccccccc} 0 & \longrightarrow & S & \xrightarrow{f} & M & \xrightarrow{g} & N \\ & & \downarrow{\scriptstyle u} & & \| & & \| \\ 0 & \longrightarrow & \operatorname{Ker} g & \xrightarrow{\ker g} & M & \xrightarrow{g} & N \end{array}$$

conmutativo. Como id_M es monomorfismo, u también lo es. Por otro lado, dado $x \in \operatorname{Ker} g$, como $g \ker g(x) = 0$ y $\operatorname{Ker} g = \operatorname{Im} f$, existe $s \in S$ tal que $f(s) = \ker g(x)$. Por definición de u, tenemos que $u(s) = x$ y, por lo tanto, u es un epimorfismo.

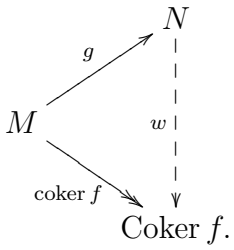
□

Proposición 3.4. *Dado un diagrama conmutativo de A-módulos y A-morfismos con filas exactas de la forma*

$$\begin{array}{ccccccccc} S & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} & & \\ S' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & \longrightarrow & 0 \end{array}$$

existe un único A-morfismo w que hace el tercer cuadrado conmutativo. Además w es un epimorfismo si v lo es.

Corolario 3.5. *Dada $S \xrightarrow{f} M \xrightarrow{g} N \to 0$ una sucesión exacta de A-módulos y A-morfismos, existe un único A-isomorfismo $w : N \to \operatorname{Coker} f$ que hace conmutativo al diagrama*



Lema 3.6 (Lema de los cinco)**.** *Dado un diagrama conmutativo de A-módulos y A-morfismos con filas exactas de la forma*

$$\begin{array}{ccccccccccc} M_1 & \xrightarrow{u_1} & M_2 & \xrightarrow{u_2} & M_3 & \xrightarrow{u_3} & M_4 & \xrightarrow{u_4} & M_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ N_1 & \xrightarrow{v_1} & N_2 & \xrightarrow{v_2} & N_3 & \xrightarrow{v_3} & N_4 & \xrightarrow{v_4} & N_5 \end{array}$$

tenemos:

(a) *Si f_5 es un monomorfismo y f_2, f_4 son epimorfismos, entonces f_3 es un epimorfismo;*
(b) *Si f_1 es un epimorfismo y f_2, f_4 son monomorfismos, entonces f_3 es un monomorfismo;*
(c) *Si f_5 es un monomorfismo, f_1 un epimorfismo y f_2, f_4 son isomorfismos, entonces f_3 es un isomorfismo.*

Demostración.

(a) Sea $n_3 \in N_3$. Como f_4 es un epimorfismo, existe $m_4 \in M_4$ tal que $f_4(m_4) = v_3(n_3)$. Ahora

$$f_5 u_4(m_4) = v_4 f_4(m_4) = v_4 v_3(n_3) = 0$$

y como f_5 es un monomorfismo, $u_4(m_4) = 0$. Como $\operatorname{Ker} u_4 = \operatorname{Im} u_3$, existe $m_3 \in M_3$ tal que $u_3(m_3) = m_4$. Entonces

$$v_3(n_3 - f_3(m_3)) = f_4(m_4) - f_4 u_3(m_3) = 0$$

y $\operatorname{Ker} v_3 = \operatorname{Im} v_2$ implica que existe $n_2 \in N_2$ tal que $v_2(n_2) = n_3 - f_3(m_3)$. Usando que f_2 es un epimorfismo tenemos que existe $m_2 \in M_2$ tal que $n_2 = f_2(m_2)$. Esto nos dice que

$$n_3 - f_3(m_3) = v_2(n_2) = v_2 f_2(m_2) = f_3 u_2(m_2)$$

y por lo tanto $n_3 = f_3(m_3 + u_2(m_2))$.

(b) Sea $m_3 \in M_3$ con $f_3(m_3) = 0$. Como f_4 es un monomorfismo y

$$f_4 u_3(m_3) = v_3 f_3(m_3) = 0$$

se tiene que $u_3(m_3) = 0$. Usando que $\operatorname{Ker} u_3 = \operatorname{Im} u_2$, tenemos que existe $m_2 \in M_2$ tal que $u_2(m_2) = m_3$. Ahora

$$v_2 f_2(m_2) = f_3 u_2(m_2) = f_3(m_3) = 0$$

y como $\operatorname{Ker} v_2 = \operatorname{Im} v_1$, existe $n_1 \in N_1$ con $v_1(n_1) = f_2(m_2)$. Como f_1 es un epimorfismo, existe $m_1 \in M_1$ tal que $f_1(m_1) = n_1$. Entonces

$$f_2(m_2) = v_1(n_1) = v_1 f_1(m_1) = f_2 u_1(m_1).$$

Como f_2 es un monomorfismo, $m_2 = u_1(m_1)$ y por lo tanto

$$m_3 = u_2(m_2) = u_2 u_1(m_1) = 0.$$

(c) Es inmediato a partir de (a) y (b).

□

Lema 3.7 (Lema de la serpiente)**.** *Todo diagrama conmutativo de A-módulos y A-morfismos con filas exactas de la forma*

$$\begin{array}{ccccccc} & & S & \xrightarrow{u} & M & \xrightarrow{v} & N \longrightarrow 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ 0 & \longrightarrow & S' & \xrightarrow{u'} & M' & \xrightarrow{v'} & N' \end{array}$$

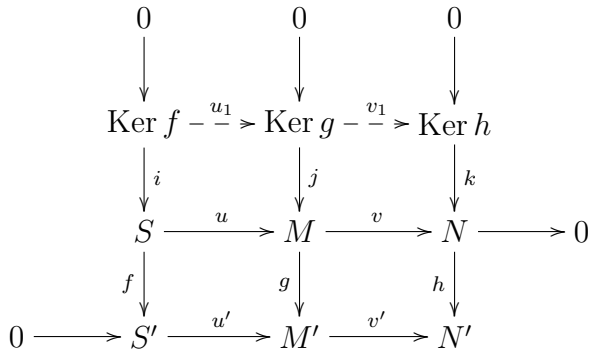
induce una sucesión exacta

$$\operatorname{Ker} f \xrightarrow{u_1} \operatorname{Ker} g \xrightarrow{v_1} \operatorname{Ker} h \xrightarrow{\delta} \operatorname{Coker} f \xrightarrow{u_1'} \operatorname{Coker} g \xrightarrow{v_1'} \operatorname{Coker} h$$

donde los morfismos u_1, v_1, u_1', v_1' son los inducidos por los correspondientes morfismos u, v, u', v' respectivamente. Además, si u es un monomorfismo, el morfismo inducido

entre los núcleos también lo es, y si v' es un epimorfismo, el morfismo inducido entre los conúcleos también lo es.

Demostración. Aplicando dos veces la Proposición 3.2 al diagrama conmutativo



obtenemos los morfismos u_1, v_1 que completan el diagrama de manera conmutativa.
Veamos la exactitud de la sucesión en $\operatorname{Ker} g$.
La unicidad establecida en la Proposición 3.2 aplicada al diagrama que se obtiene considerando sólo la primer y tercer columna nos dice que $v_1 u_1 = 0$.
Falta probar entonces que $\operatorname{Ker} v_1 \subseteq \operatorname{Im} u_1$.
Sea $x \in \operatorname{Ker} v_1$. Entonces $vj(x) = kv_1(x) = 0$. Como $\operatorname{Ker} v = \operatorname{Im} u$, existe $s \in S$ tal que $u(s) = j(x)$. Ahora

$$u'f(s) = gu(s) = gj(x) = 0$$

y como u' es un monomorfismo, $f(s) = 0$. Por otro lado, $\operatorname{Ker} f = \operatorname{Im} i$, entonces existe $x' \in \operatorname{Ker} f$ tal que $i(x') = s$. Entonces

$$j(x) = u(s) = ui(x') = ju_1(x')$$

y como j es un monomorfismo, $x = u_1(x')$.
Ahora definiremos el morfismo $\delta : \operatorname{Ker} h \to \operatorname{Coker} f$.
Dado $x'' \in \operatorname{Ker} h$, como v es un epimorfismo, existe $m \in M$ tal que $v(m) = k(x'')$. Ahora

$$v'g(m) = hv(m) = hk(x'') = 0$$

y como $\operatorname{Ker} v' = \operatorname{Im} u'$, existe s' tal que $u'(s') = g(m)$. Definimos $\delta(x'') = p(s')$, donde $p : S' \to \operatorname{Coker} f$ es la proyección canónica.
Observemos que el proceso para definir δ es el siguiente:

$$\boxed{x''} \Rightarrow \boxed{m : v(m) = k(x'')} \Rightarrow \boxed{s' : u'(s') = g(m)}$$

y que como u' es inyectiva, elegido m, el elemento s' es único. Entonces para demostrar la buena definición basta ver que $p(s')$ no depende del m elegido.
Dado x'', repasemos la construcción anterior a partir de m_1, m_2 verificando $v(m_1) = k(x'') = v(m_2)$, y sean s'_1, s'_2 tales que $u'(s'_1) = g(m_1), u'(s'_2) = g(m_2)$. Entonces $v(m_1 - m_2) = 0$ y como $\operatorname{Ker} v = \operatorname{Im} u$, existe $s_1 \in S$ tal que $u(s_1) = m_1 - m_2$, y se tiene

$$u'f(s_1) = gu(s_1) = g(m_1 - m_2) = u'(s'_1 - s'_2).$$

Como u' es un monomorfismo, $s'_1 - s'_2 \in \operatorname{Im} f$ y por lo tanto $p(s'_1) = p(s'_2)$.
Veamos que δ es A-morfismo. Sean $x''_1, x''_2 \in \operatorname{Ker} h$, $m_1, m_2 \in M$ tales que $v(m_1) = k(x''_1)$, $v(m_2) = k(x''_2)$, y s'_1, s'_2 tales que $u'(s'_1) = g(m_1), u'(s'_2) = g(m_2)$. Como k, v, g y u' son A-morfismos, tenemos que

$$v(am_1 + bm_2) = k(ax''_1 + bx''_2) \qquad \text{y} \qquad u'(as'_1 + bs'_2) = g(am_1 + bm_2).$$

Entonces $\delta(ax_1'' + bx_2'') = p(as_1' + bs_2') = ap(s_1') + bp(s_2') = a\delta(x_1'') + b\delta(x_2'')$.
Veamos ahora que la sucesión encontrada es exacta en $\operatorname{Ker} h$, esto es, $\operatorname{Ker}\delta = \operatorname{Im} v_1$.
$\operatorname{Im} v_1 \subseteq \operatorname{Ker}\delta$: Sea $x'' = v_1(x)$ para $x \in \operatorname{Ker} g$. Entonces $v(j(x)) = kv_1(x) = k(x'')$ y $u'(0) = g(j(x))$, por lo tanto $\delta(x'') = p(0) = 0$.
$\operatorname{Ker}\delta \subseteq \operatorname{Im} v_1$: Sea $x'' \in \operatorname{Ker} h$ tal que $\delta(x'') = 0$. Esto signfica que el s' asociado a x'' es tal que $p(s') = 0$, y por lo tanto, $s' = f(s_1')$. Entonces

$$g(m) = u'(s') = u'f(s_1') = gu(s_1').$$

Como $m - u(s_1') \in \operatorname{Ker} g$, $m - u(s_1') = j(m_0)$ con $m_0 \in \operatorname{Ker} g$. Entonces

$$k(x'') = v(m) = v(j(m_0) + u(s_1')) = vj(m_0) = kv_1(m_0).$$

Como k es un monomorfismo, tenemos que $x'' = v_1(m_0) \in \operatorname{Im} v_1$.
El resto de las afirmaciones del lema se prueban de manera similar.

□

4. Teoremas de isomorfismos

Teorema 4.1. *Sea $f : M \to N$ un A-morfismo. Existe un único A-morfismo $\overline{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$ que hace el diagrama*

$$\begin{array}{ccc} M & \xrightarrow{\ f\ } & N \\ {\scriptstyle p}\downarrow & & \uparrow \\ M/\operatorname{Ker} f & \xrightarrow{\ \overline{f}\ } & \operatorname{Im} f \end{array}$$

conmutativo. Además, $\overline{f}$ es un isomorfismo.

Demostración. La conmutatividad del diagrama nos dice que si $\overline{f}$ existe, debe estar definido por la fórmula

$$\overline{f}(\overline{m}) = \overline{f}(m + \operatorname{Ker} f) = \overline{f}p(m) = f(m).$$

Veamos entonces que esta fórmula define un A-morfismo. Es una función bien definida pues dados $m_1, m_2 \in M$ tales que $\overline{m}_1 = \overline{m}_2$, sabemos que $m_1 - m_2 \in \operatorname{Ker} f$ y por lo tanto $f(m_1) = f(m_2)$.
Además $\overline{f}$ es A-morfismo pues dados $m_1, m_2 \in M$, $a, b \in A$

$$\begin{aligned} \overline{f}(a\overline{m}_1 + b\overline{m}_2) &= \overline{f}p(am_1 + bm_2) = f(am_1 + bm_2) \\ &= af(m_1) + bf(m_2) = a\overline{f}(\overline{m}_1) + b\overline{f}(\overline{m}_2). \end{aligned}$$

La inyectividad de $\overline{f}$ es inmediata pues $0 = \overline{f}(\overline{m}) = f(m)$ nos dice que $m \in \operatorname{Ker} f$ y por lo tanto $\overline{m} = 0$. Por otro lado, $\overline{f}$ es sobreyectiva pues dado $n \in \operatorname{Im} f$, $n = f(m)$, tenemos que $\overline{f}(\overline{m}) = f(m) = n$.

□

Del teorema anterior se deduce que todo morfismo se puede escribir como la composición de un epimorfismo, un isomorfismo y un monomorfismo.

Teorema 4.2. *Sean S, N dos submódulos del A-módulo M. Entonces*

$$(S + N)/S \xrightarrow{\sim} N/(S \cap N).$$

Demostración. Consideremos el diagrama conmutativo con filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S\cap N & \xrightarrow{i} & N & \xrightarrow{p} & N/(S\cap N) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle k} & & \downarrow{\scriptstyle w} & & \\ 0 & \longrightarrow & S & \xrightarrow{h} & S+N & \xrightarrow{q} & (S+N)/S & \longrightarrow & 0 \end{array}$$

donde i, j, k, h son las inclusiones, p, q las proyecciones canónicas, y w existe por la Proposición 3.4.
Veamos que w es un isomorfismo. Si $w(\overline{n}) = 0$, entonces $qk(n) = 0$ y como k es la inclusión y q la proyección, tenemos que $n \in S$. Luego $n \in S \cap N$ y $\overline{n} = 0$. Por otro lado, si $(\overline{s+n}) \in (S+N)/S$ entonces $(\overline{s+n}) = \overline{n} = q(n) = qk(n) = wp(n) = w(\overline{n})$.

□

Teorema 4.3. *Sean S, N dos submódulos del A-módulo M tales que $S \subseteq N$. Entonces existe un único A-morfismo $w : M/S \to M/N$ que hace conmutativo al diagrama*

$$\begin{array}{ccccc} & & M & & \\ & \swarrow^{p_S} & & \searrow^{p_N} & \\ M/S & & \xrightarrow{w} & & M/N. \end{array}$$

Además, w es un epimorfismo con núcleo N/S e induce un isomorfismo

$$M/N \xrightarrow{\sim} (M/S)/(N/S).$$

Demostración. Por la Proposición 3.4 existe un diagrama conmutativo con filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S & \xrightarrow{i} & M & \xrightarrow{p_S} & M/S & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle j} & & \| & & \downarrow{\scriptstyle w} & & \\ 0 & \longrightarrow & N & \xrightarrow{k} & M & \xrightarrow{p_N} & M/N & \longrightarrow & 0 \end{array}$$

donde i, j, k son las inclusiones y p_S, p_N las proyecciones canónicas. Si aplicamos el Lema de la serpiente a este diagrama, tenemos que existe una sucesión exacta

$$0 \to \operatorname{Ker} j \to \operatorname{Ker} \mathrm{id} \to \operatorname{Ker} w \xrightarrow{\delta} \operatorname{Coker} j \to \operatorname{Coker} \mathrm{id} \to \operatorname{Coker} w \to 0.$$

Como $\operatorname{Coker} \mathrm{id} = 0$, tenemos que $\operatorname{Coker} w = 0$ y por lo tanto w es un epimorfismo. Para calcular su núcleo observemos que $\operatorname{Ker} \mathrm{id} = 0 = \operatorname{Coker} \mathrm{id}$, y por lo tanto $\delta : \operatorname{Ker} w \to \operatorname{Coker} j$ es un isomorfismo, donde $\operatorname{Coker} j = N/S$.

□

5. Módulos libres

Comenzamos estas notas mencionando que la definición de módulos generaliza a la de los espacios vectoriales. Ahora bien, todo espacio vectorial tiene base, y este resultado no es cierto en la teoría de módulos, por ejemplo, el $\mathbb{Z}$-módulo $\mathbb{Z}/2\mathbb{Z}$ no admite base. Tampoco es cierto que todo conjunto de generadores minimal sea una base, ni que todo conjunto linealmente independiente maximal lo sea. Por ejemplo, el $\mathbb{Z}$-módulo $\mathbb{Z}$ tiene base $\{1\}$; el conjunto $\{2\}$ es un conjunto linealmente independiente maximal que no es base y $\{2, 3\}$ es un conjunto de generadores minimal que tampoco es base.

Sea M un A-módulo. Un conjunto $(x_\lambda)_{\lambda\in\Lambda}$ se dice **libre o linealmente independiente** si, para toda familia $(a_\lambda)_{\lambda\in\Lambda}$ de elementos de A tal que $(a_\lambda x_\lambda)_{\lambda\in\Lambda}$ tiene soporte

finito, la relación $\sum_{\lambda\in\Lambda} a_\lambda x_\lambda = 0$ implica $a_\lambda = 0$ para todo $\lambda \in \Lambda$. Una **base** de un A-módulo M es un conjunto libre de elementos de M que lo genera.

Definición 5.1. Sea X un conjunto. Un A-módulo **libre** está dado por un A-módulo $L(X)$ y una función $j_X : X \to L(X)$ tal que, si M es un A-módulo y $f : X \to M$ una función, existe un único morfismo de A-módulos $\overline{f} : L(X) \to M$ tal que el diagrama

$$\begin{array}{ccc} X & \xrightarrow{j_X} & L(X) \\ & \searrow^{f} & \downarrow{\scriptstyle \overline{f}} \\ & & M \end{array}$$

conmuta.

Lema 5.2. *Sea X un conjunto. Un módulo libre sobre X, si existe, es único a menos de isomorfismos.*

Demostración. Sean L, L' dos A-módulos libres con las correspondientes funciones $j : X \to L$, $j' : X \to L'$. Por la definición anterior sabemos que existen A-morfismos $f : L \to L'$ y $f' : L' \to L$ que hacen el diagrama

$$\begin{array}{ccc} X & \xrightarrow{j} & L \\ {\scriptstyle \mathrm{id}_X}\downarrow & & \downarrow{\scriptstyle f} \\ X & \xrightarrow{j'} & L' \\ {\scriptstyle \mathrm{id}_X}\downarrow & & \downarrow{\scriptstyle f'} \\ X & \xrightarrow{j} & L \end{array}$$

conmutativo. La conmutatividad del cuadrado externo, y la unicidad del morfismo de L en L que lo haga conmutativo, nos dice que $f'f = \mathrm{id}_L$. Análogamente se prueba que $ff' = \mathrm{id}_{L'}$.

□

Teorema 5.3. *Para todo conjunto X existe un A-módulo libre sobre X, único a menos de isomorfismos.*

Demostración. La unicidad sigue del lema anterior. Para demostrar la existencia, consideremos $L(X) = \bigoplus_X A$, esto es, la suma directa de copias del A-módulo A indexada por X, y $j_X : X \to L(X)$ la función dada por $j_X(\lambda) = e_\lambda = (e_\lambda^\mu)_{\mu\in\Lambda}$ donde $e_\lambda^\lambda = 1$ y $e_\lambda^\mu = 0$ si $\mu \neq \lambda$. Sabemos que todo elemento de $L(X)$ se escribe como $\sum_{\lambda\in X} a_\lambda e_\lambda$ con $(a_\lambda)_{\lambda\in\Lambda}$ una familia de elementos de A de soporte finito. Si M es un A-módulo y $f : X \to M$ una función, basta considerar la aplicación $\overline{f} : L(X) \to M$ definida por

$$\overline{f}(\sum_{\lambda\in X} a_\lambda e_\lambda) = \sum_{\lambda\in X} a_\lambda \overline{f}(e_\lambda) = \sum_{\lambda\in X} a_\lambda \overline{f} j_X(\lambda) = \sum_{\lambda\in X} a_\lambda f(\lambda).$$

Esta fórmula define un A-morfismo que hace conmutativo al triángulo correspondiente.

□

Teorema 5.4. *Un A-módulo M es libre si y sólo si admite una base.*

Demostración. Si L es libre sobre X, entonces L es isomorfo a $L(X) = \bigoplus_X A$ vía un isomorfismo $f : L(X) \to L$. Es fácil ver entonces que el conjunto $(f(e_\lambda))_{\lambda\in X}$ es un conjunto linealmente independiente que genera a L, y por lo tanto, L admite base.

Recíprocamente, si L admite una base X consideremos la función inclusión $j : X \hookrightarrow L$ y veamos que $(L, j : X \hookrightarrow L)$ satisface la propiedad que define a los módulos libres, ver Definición 5.1. Si M es un A-módulo y $f : X \to M$ es una función, tomemos para cada $u \in L$ su descomposicón, única por definición, como combinación lineal en término de los elementos de la base X, $u = \sum_{x\in X} a_x x$. Es claro entonces que $\overline{f} : L \to M$ definido por

$$\overline{f}(u) = \overline{f}(\sum_{x\in X} a_x x) = \sum_{x\in X} a_x \overline{f} j(x) = \sum_{x\in X} a_x f(x)$$

es un A-morfismo que hace conmutar al triángulo

$$\begin{array}{ccc} X & \xrightarrow{j} & L \\ & \searrow^{f} & \downarrow{\scriptstyle \overline{f}} \\ & & M. \end{array}$$

□

Vimos que todo módulo libre $L(X)$ admite una base que se puede indentificar con el conjunto X. La propiedad universal que define a un módulo libre, vista en la Defición 5.1, nos dice que todo A-morfismo $\overline{f} : L(X) \to M$ está unívocamente determinado por los valores $f(x)$ que toma en los elementos de la base.

Es natural preguntarse si dos bases de un A-módulo libre tiene el mismo cardinal. Sabemos que esto es cierto si A es un cuerpo. En la próxima sección daremos respuesta a esta pregunta.

Proposición 5.5. *Todo A-módulo es cociente de un A-módulo libre. Además, si M es finitamente generado, el módulo libre puede elegirse con base finita.*

Demostración. Sea M un A-módulo, y sea X un conjunto de generadores de M (por ejemplo, podríamos tomar $X = M$). Tomemos $L(X)$ el A-módulo libre sobre X. La inclusión $i : X \hookrightarrow M$ induce un morfismo $f : L(X) \to M$ que hace conmutativo al diagrama

$$\begin{array}{ccc} X & \xrightarrow{j_X} & L(X) \\ & \searrow^{i} & \downarrow{\scriptstyle f} \\ & & M. \end{array}$$

Como $X \subseteq \operatorname{Im} f$ y X genera a M, tenemos que f es un epimorfismo y por lo tanto $M \cong L(X)/\operatorname{Ker} f$.

□

Corolario 5.6. *Sea M un A-módulo. Existe una sucesión exacta $L_1 \to L_0 \to M \to 0$ con L_0, L_1 dos A-módulos libres.*

Demostración. Por la proposición anterior sabemos que existen módulos libre L_0, L_1 tales que

$$L_0 \xrightarrow{f} M \to 0, \qquad L_1 \xrightarrow{g} \operatorname{Ker} f \to 0$$

son exactas. Entonces

$$L_1 \xrightarrow{\ker f \circ g} L_0 \xrightarrow{f} M \to 0$$

es exacta.

□

Vimos en el corolario anterior que todo A-módulo M admite una sucesión exacta $L_1 \to L_0 \to M \to 0$ con L_0, L_1 dos A-módulos libres. Esta sucesión se llama **presentación libre** de M. Diremos que M es finitamente presentado, o que admite una presentación finita, si L_0, L_1 son finitamente generados.

Es claro que todo módulo finitamente presentado es finitamente generado, pero la recíproca no es cierta.

Una presentación libre de un módulo se puede pensar como una aproximación del módulo por módulos libres. La existencia de presentaciones libres es útil cuando se estudian propiedades que son fáciles de demostrar sobre los módulos libres. Si esta propiedad es compatible con los conúcleos, la validez del resultado en los módulos libres implicará la validez en módulos arbitrarios.

6. Problema IBN (invariant basis number)

Se dice que un anillo A tiene la **propiedad IBN (invariant basis number)** si las bases de cualquier A-módulo libre tienen el mismo cardinal.

Veamos un ejemplo de un anillo A que no satisface la propiedad IBN. En particular, veremos que $A \cong A \oplus A$. Sea $A = \overline{M}_{\mathbb{N}}(K)$ el conjunto de matrices de tamaño $\mathbb{N} \times \mathbb{N}$ cuyas columnas tienen sólo un número finito de elementos no nulos. El conjunto A tiene estructura de anillo con la suma y el producto de matrices, y la aplicacion

$$f : A \to A \oplus A$$

definida por $f(M) = (M_1, M_2)$, con M_1, M_2 las matrices que se obtienen a partir de M quitando las columnas impares y pares respectivamente, es un isomorfismo de A-módulos.

Teorema 6.1. *Todo anillo conmutativo tiene la propiedad IBN.*

Demostración. Por el Lema de Zorn, el anillo conmutativo A tiene un ideal maximal $\mathfrak{M}$, y por lo tanto $A/\mathfrak{M}$ es un cuerpo. Sea $\{m_i\}_{i\in J}$ una base del A-módulo libre M. El A-módulo cociente $M/\mathfrak{M}M$ tiene estructura de $A/\mathfrak{M}$-módulo, es decir, es un $A/\mathfrak{M}$-espacio vectorial. Como $M = \oplus_{i\in J} Am_i$, entonces $\mathfrak{M}M = \oplus_{i\in J}\mathfrak{M}m_i$, y por lo tanto

$$M/\mathfrak{M}M \cong \oplus_{i\in J} Am_i/\mathfrak{M}m_i \cong \oplus_{i\in J} A/\mathfrak{M}.$$

Entonces el cardinal de J es la dimensión del $A/\mathfrak{M}$-espacio vectorial $M/\mathfrak{M}M$. Como los cuerpos tienen la propiedad IBN, toda base de M tendrá el mismo cardinal que J.

□

Proposición 6.2. *Sea M un A-módulo con X un conjunto de generadores minimal. Si X es infinito de cardinal α, todo conjunto de generadores de M tiene cardinal al menos α. En particular, M no es finitamente generado y todo conjunto de generadores minimal tiene cardinal α.*

Demostración. Sea Y un conjunto de generadores de M de cardinal β. Cada $y \in Y$ se escribe como combinación lineal de un número finito de elementos de X. Sea X_y el conjunto finito formado por estos elementos. Es claro entonces que

$$\bigcup_{y\in Y} X_y \subseteq X.$$

Por otro lado, el submódulo generado por $\bigcup_{y\in Y} X_y$ contiene a Y, y por lo tanto, es igual a M. La minimalidad de X nos dice que

$$\bigcup_{y\in Y} X_y = X.$$

Si Y fuera finito, X se podría expresar como una unión finita de conjuntos finitos, contradicción pues X es infinito. Entonces Y es infinito y

$$\alpha = |X| \leq \sum_{y\in Y} |X_y| \leq \aleph_0\beta = \beta.$$

Esto muestra que Y tiene cardinal al menos α. Si además Y fuera minimal, intercambiando los roles entre X e Y, tendríamos $\beta \leq \alpha$, y por lo tanto, $\beta = \alpha$.

□

Corolario 6.3. *Un anillo A tiene la propiedad IBN si y sólo si las bases de cualquier A-módulo libre finitamente generado tienen el mismo cardinal.*

Proposición 6.4. *Dado un anillo A, las siguientes condiciones son equivalentes:*

(1) *A tiene la propiedad IBN;*
(2) *$A^n \cong A^m$ implica $n = m$;*
(3) *Si $C \in M_{n\times m}(A)$, $D \in M_{m\times n}(A)$ y $CD = \mathrm{Id}_n$, $DC = \mathrm{Id}_m$, entonces $n = m$.*

Demostración. La equivalencia entre (1) y (2) es inmediata por definición y el Corolario 6.3. La equivalencia entre (2) y (3) se obtiene considerando a C y D como las matrices que describen al isomorfismo entre A^n y A^m.

□

Proposición 6.5. *Sea $f : A \to A'$ un morfismo de anillos. Si A' tiene la propiedad IBN entonces A también.*

Demostración. Si A no tiene la propiedad IBN, existen matrices $C \in M_{n\times m}(A)$, $D \in M_{m\times n}(A)$ tales que $CD = \mathrm{Id}_n$, $DC = \mathrm{Id}_m$, con $n \neq m$. Aplicando f a dichas matrices, obtenemos dos matrices rectangulares (no cuadradas) de elementos en A' que verifican las mismas igualdades. Contradicción pues A' tiene la propiedad IBN.

□

Ejercicios.

1. Sea $\Phi : A \to S$ un morfismo de anillos. Probar que si M es un S-módulo, entonces M es un A-módulo con la acción dada por $am := \Phi(a)m$. Decimos que la estructura de A-módulo de M está dada por el pullback a lo largo de Φ.
2. Demuestre que si N es un A-submódulo de M entonces la operación $A\times M/N \to M/N$ definida por $(a, m+N) \mapsto am+N$ está bien definida y verifica los axiomas necesarios para dar a M/N una estructura de A-módulo.
3. Sea M un A-módulo. Pruebe 0 y M son submódulos de M .
4. Sea A un anillo, y sea M el módulo regular. Demuestre que los submódulos de M son exactamente los ideales izquierdos de A.
5. Sea M un grupo abeliano, es decir un $\mathbb{Z}$-módulo. Pruebe que todo subgrupo de M es un submódulo de M.
6. Sea M un A-módulo. Demuestre que el morfismo de M en M que manda a todos los elementos de M al elemento neutro 0 es un morfismo de A-mdulos, llamado morfismo cero. Demuestre también que la función identidad de M en M es un isomorfismo de A-módulos.

7. *a*) Sea M un A-módulo tal que para cualquier A-módulo N existe un único morfismo $f : M \to N$. Demuestre que $M = 0$.
   b) Sea M un A-módulo tal que para cualquier A-módulo N existe un único morfismo $f : N \to M$. Demuestre que $M = 0$.
8. Sea A un anillo cualquiera (no necesariamente conmutativo), y sea M un A-módulo. Sea $a \in A$ arbitrario, y sea $f : M \to M$ dada por $f(m) = am$. Demuestre que f es un morfismo de A-módulos.
9. Demuestre que la composición de dos morfismos de módulos es un morfismo de módulos.
10. Demuestre que el inverso de un isomorfismo de módulos es un isomorfismo de módulos. Concluya que si $M \cong N$ entonces $N \cong M$.
11. Demuestre que un A-morfismo $f : M \to N$ es un isomorfismo si y sólo si la función f es biyectiva.
12. Demuestre que si $M \cong N$ y $N \cong K$ entonces $M \cong K$.
13. Dé un ejemplo de un anillo A y dos A-módulos M y N distintos de cero tales que el único morfismo de M en N sea el morfismo cero, y el único morfismo de N en M sea también cero.
14. Sea $f : M \to N$ un morfismo de módulos.
   a) Demuestre que $\operatorname{Ker} f$ es un submódulo de M .
   b) Demuestre que $\operatorname{Im} f$ es un submódulo de N.
15. Sea $f : M \to N$ un epimorfismo de A-módulos, S un submódulo de M y $j : S \to M$ la inclusión. Mostrar que:
   a) Si $S \cap \operatorname{Ker} f = 0$ entonces fj es un monomorfismo;
   b) Si $S + \operatorname{Ker} f = M$ entonces fj es un epimorfismo.
16. Sea M un A-módulo y $f : M \to M$ un morfismo de A-módulos tal que $f \circ f = f$. Probar que $M = \operatorname{Ker} f \oplus \operatorname{Im} f$.
17. Sea
$$0 \longrightarrow M \longrightarrow N \longrightarrow K \longrightarrow 0$$
una sucesión exacta de módulos. Demuestre que $K \cong (N/M)$.
18. Demuestre que toda sucesión exacta es un complejo, y que la recíproca no es cierta.
19. Dado un diagrama conmutativo de A-módulos y A-morfismos con filas exactas de la forma
$$\begin{array}{ccccccc} L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} & & \\ L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & \longrightarrow & 0 \end{array}$$
existe un único A-morfismo w que hace al último cuadrado conmutativo. Además w es un epimorfismo si v lo es.
20. Sea A un anillo. Probar que todo A-módulo cíclico es isomorfo a un A-módulo de la forma A/J, donde J es un ideal a izquierda de A.
21. Sean K cuerpo, V un K-espacio vectorial y $T : V \to V$ una transformación lineal. Probar que:
   a) V es un $K[x]$-módulo con la acción dada por $fv = f(T)(v)$, para todo $f \in K[x]$, $v \in V$.
   b) $S \subseteq V$ es un $K[x]$-submódulo si y sólo si S es un K-subespacio vectorial y $T(S) \subseteq S$.

22. Dados los A-módulos M, N, S y $f : M \to N$ un morfismo de A-módulos, probar que la aplicación $f_* : \mathrm{Hom}_A(S, M) \to \mathrm{Hom}_A(S, N)$ dada por $f_*(h) = f \circ h$ es un morfismo de grupos abelianos.
23. Sea A anillo y sean M, N, C y D A-módulos. Probar que si
$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} C$$
es una sucesión exacta, entonces
$$0 \longrightarrow \mathrm{Hom}_A(D, M) \xrightarrow{f_*} \mathrm{Hom}_A(D, N) \xrightarrow{g_*} \mathrm{Hom}_A(D, C)$$
es una sucesión exacta de grupos abelianos.
24. Demuestre que $\mathbb{Q}$ no es un $\mathbb{Z}$-módulo finitamente generado.
25. Probar que $\mathbb{Z}$ no admite ninguna estructura de $\mathbb{Q}$-módulo. ¿Admite $\mathbb{Q}$ alguna estructura de $\mathbb{R}$-módulo?
26. Decidir si las siguientes afirmaciones son verdaderas o falsas.
    a) $\mathbb{Q}$ es un $\mathbb{Z}$-módulo libre.
    b) $\mathbb{R}$ es un $\mathbb{Q}$-módulo libre.
27. Si V es un K-espacio vectorial de dimensión infiinta, probar que $A = \mathrm{End}_k(V)$ no posee la propiedad IBN.

Referencias

[1] I. Assem. *Algèbres et modules*, Série Enseignement des Mathématiques, Presses de l'Université d'Ottawa (Ottawa) / Masson (Paris), 1997.
[2] M. Auslander y D. Buchsbaum. *Groups, rings, modules*, Harper's Series in Modern Mathematics, Harper & Row, Publishers, New York-London, 1974.
[3] P. M. Cohn. *Algebra*, **Vol. 2**, Second edition, John Wiley & Sons, Ltd., Chichester, 1989.
[4] J. Rotman. *Advanced modern algebra*, Prentice Hall, Inc., Upper Saddle River, NJ, 2002.

MJR: Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca.
E-mail address: mredondo@uns.edu.ar

IZ: FaMAF, Universidad de Córdoba, Córdoba.
E-mail address: zurrian@gmail.com