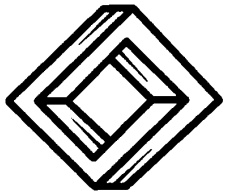
Publicaciones Electrónicas
Sociedad Matemática Mexicana

Módulos Semisimples y Representación de Grupos Finitos

Humberto Cárdenas Trigos
Emilio Lluis Riera

www.smm.org.mx

Serie: Textos. Vol. 16 (2012)



Módulos semisimples y representación de grupos finitos

1

SERIE SOCIEDAD MATEMATICA MEXICANA

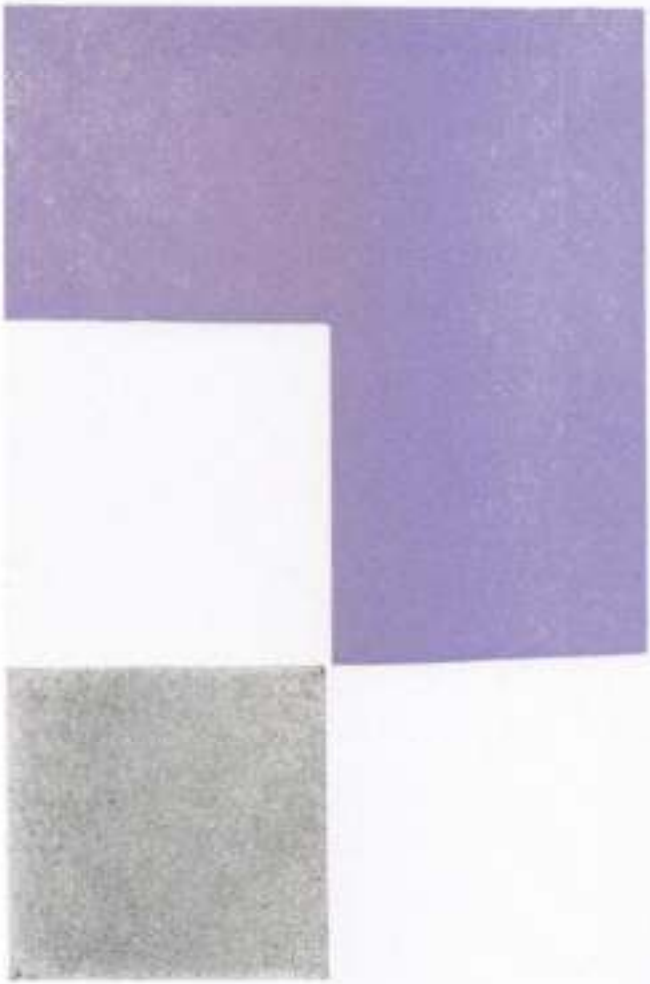
Humberto Cárdenas
Doctor en Matemáticas, Princeton
Investigador del Instituto de Matemáticas
Catedrático de la Facultad de Ciencias de la
Universidad Nacional Autónoma de México

Emilio Lluis
Doctor en Matemáticas, UNAM
Investigador del Instituto de Matemáticas
Catedrático de la Facultad de Ciencias de la
Universidad Nacional Autónoma de México

SOCIEDAD MATEMÁTICA MEXICANA

Módulos semisimples y representación de grupos finitos

Humberto Cárdenas
Emilio Lluis



Editorial F. Trillas, S. A.
México, 1970

PROLOGO

Este libro aparece como respuesta a un llamado de la Sociedad Matemática Mexicana para fomentar la publicación en México, de libros de texto a nivel superior.

La primera parte fue redactada para servir de texto al curso de *Representación de grupos finitos* del Primer Coloquio Mexicano de Matemáticas que tuvo lugar en Oaxtepec, Morelos (1968). Para completar el tema se han agregado dos capítulos en los cuales se incluyen más resultados y se da un buen número de ejemplos y aplicaciones.

Esta obra está hecha para utilizarse como texto en un curso sobre *Módulos semisimples y representación de grupos finitos*. Su lectura requiere los conocimientos que se adquieren en los cursos ordinarios de álgebra en la licenciatura.

Ya que el estudio de las representaciones de un grupo equivale al estudio de los módulos sobre el anillo de grupo, hemos considerado conveniente hacer primero una exposición sistemática de la teoría de los módulos sobre un anillo arbitrario y después interpretar los resultados obtenidos en el lenguaje de las representaciones.

Los capítulos 1 y 3 están dedicados exclusivamente a la teoría de los módulos y son independientes del 2 y el 4. En el primer capítulo se dan las definiciones básicas y se tratan los resultados generales de la teoría de los módulos sobre anillos arbitrarios. El tercero está dedicado al estudio de los módulos semisimples, incluyendo el teorema generalizado de Wedderburn, del que se deriva el teorema de estructura de los anillos simples.

En el capítulo 2 se definen los conceptos básicos acerca de las representaciones y se aplican los resultados del capítulo 1. Además se establece claramente la relación entre representaciones y módulos. En el capítulo 4 se utilizan los resultados del capítulo 3 y se describen los anillos de representaciones de algunos grupos.

En el capítulo 4 se dan más caracterizaciones de las álgebras simples y semisimples (teoremas de Maschke, Schur, Burnside y Frobenius). Se utilizan los resultados del capítulo 3 para obtener el anillo de las representaciones.

El capítulo 5 está dedicado a ilustrar los conceptos y resultados expuestos en los capítulos previos. Se calculan las representaciones de ciertos tipos de grupos (cíclicos, abelianos, diédricos, cuaternios) y se determina la estructura de sus anillos de representaciones. En particular, como ejemplo, se calculan las representaciones de todos los grupos de orden menor que doce.

El original de Módulos Semisimples y Representación de Grupos Finitos fue elaborado por los autores bajo los auspicios de la Sociedad Matemática Mexicana, para el Primer Coloquio Mexicano de Matemáticas, celebrado en Oaxtepec, Estado de Morelos, en agosto de 1968. Se publicó inicialmente en forma de preedición, con aportaciones del Fondo de Fomento Educativo y del Instituto Nacional de la Investigación Científica.

La presente edición, notablemente ampliada, es publicada por Editorial Trillas, S. A., con autorización expresa de sus autores y de la Sociedad Matemática Mexicana.

Primera edición, enero 1970

Prohibida la reproducción parcial o total de esta obra sin autorización, por escrito, de los editores

Derechos reservados conforme a la ley
© *1970, Editorial F. Trillas, S. A.*
Av. 5 de Mayo 43-105, México 1, D. F.

Miembro de la Cámara Nacional de la Industria Editorial. Reg. núm. 158

Impreso en México

INDICE GENERAL

Capítulo 1

Resultados preliminares sobre la teoría de los módulos 9

1. Módulos – 2. Módulos cociente – 3. Teoremas de isomorfismos – 4. Productos y sumas directas – 5. Módulos libres – 6. Módulos noetherianos y artinianos – 7. Series de composición – 8. Módulos inescindibles – 9. Producto tensorial de módulos – 10. Matrices y transformaciones lineales.

Capítulo 2

Representaciones de un grupo finito 39

1. Representaciones – 2. Suma y producto de representaciones matriciales – 3. Álgebra de un grupo finito – 4. Representaciones de un grupo y módulos sobre el álgebra del grupo – 5. Restricción de una representación y representaciones inducidas.

Capítulo 3

Módulos semisimples 59

1. Módulos semisimples – 2. Radical de un módulo – 3. Anillos simples – 4. Estructura de los anillos simples.

Capítulo 4

Anillo de las representaciones 75

1. Anillo de las representaciones de un grupo finito – 2. Teorema de Maschke – 3. Teoremas de Schur, Burnside y Frobenius – 4. Representaciones completamente reducibles.

Capítulo 5

Cálculo de las representaciones de algunos grupos finitos 89

1. Representaciones de los grupos cíclicos – 2. Anillo de las representaciones de un grupo cíclico – 3. Anillo de las representaciones de un grupo abeliano – 4. Representaciones de los grupos de simetrías de los polígonos regulares (grupos diédricos) – 5. Anillo de las representaciones de un grupo diédrico – 6. Representaciones del grupo de los cuaternios – 7. Anillo de las representaciones del grupo de los cuaternios – 8. Ejemplos: representaciones de grupos de orden pequeño.

Indice analítico 123

CAPITULO 1

Resultados preliminares sobre la teoría de los módulos

1. Módulos

En este capítulo designaremos con A a un anillo con elemento unitario.

Definición 1.1. *Un* A*-módulo izquierdo* M *consiste en un grupo abeliano* M *y una operación* $\mathrm{A} \times \mathrm{M} \to \mathrm{M}$ *denotada* $(\mathrm{a}, \mathrm{x}) \mapsto \mathrm{ax}$ *tal que*

1) $a(x + y) = ax + ay$,
2) $(a + b)x = ax + bx$,
3) $(ab)x = a(bx)$,
4) $1x = x$, $\qquad (a, b \in A, x, y \in M)$.

Si en lugar de (3) se cumple

3′) $(ab)x = b(ax)$,

se dice que M es un A-módulo derecho.

Si A es un anillo conmutativo, las condiciones (3) y (3′) coinciden y, por tanto, todo módulo izquierdo es derecho. Si A es un campo, M se llama un espacio vectorial.

Salvo mención específica, todos los A-módulos que se consideren serán izquierdos. Cuando se trate de A-módulos derechos, la operación de $A \times M \to M$ se denotará

$$(a, x) \mapsto xa$$

y así, la propiedad (3′) queda en la forma siguiente

3') $x(ab) = (xa)b$.

Con 0 se denotará el módulo cuyo grupo es el trivial.

Sean M y N dos A-módulos.

Definición 1.2. *Una función* $f: M \to N$ *se llama un* A-*homomorfismo de* M *en* N *si*

1) $f(x+y) = f(x) + f(y)$,
2) $f(ax) = af(x)$, $(a \in A, x, y \in M)$.

La transformación idéntica de M en M es un A-homomorfismo que se denotará con 1_M o simplemente con 1 si no se presta a confusión.

Al conjunto de todos los A-homomorfismos de M en N se le denota

$$\mathrm{Hom}_A(M, N)$$

y éste se vuelve un grupo abeliano si se define la operación con la fórmula

$$(f+g)(x) = f(x) + g(x), \quad (f, g \in \mathrm{Hom}_A(M, N), x \in M).$$

El cero de este grupo, es decir, la función que transforma todo elemento en 0 se denotará también con 0.

Si A es conmutativo, $\mathrm{Hom}_A(M, N)$ se puede considerar como un A-módulo, definiendo

$$(af)(x) = a(f(x)), \quad (a \in A, f \in \mathrm{Hom}_A(M, N), x \in M).$$

(En el caso no conmutativo af puede no ser un A-homomorfismo.)

Si $f: M \to N$ y $g: N \to P$ son A-homomorfismos, su composición gf: $M \to P$ lo es también, y por tanto, la composición determina una aplicación

$$\mathrm{Hom}_A(M, N) \times \mathrm{Hom}_A(N, P) \to \mathrm{Hom}_A(M, P),$$
$$(f, g) \mapsto gf$$

la cual es bilineal, es decir,

$$(g_1 + g_2)f = g_1 f + g_2 f,$$
$$g(f_1 + f_2) = gf_1 + gf_2.$$

Si, además, A es conmutativo, la bilinealidad significa también que vale

$$g(af) = (ag)f = a(gf).$$

$f \in \mathrm{Hom}_A(M, N)$ se escribirá también $f: M \to N$ o bien $M \xrightarrow{f} N$. Además $(fg)h = f(gh)$.

En el caso de que $M = N = P$ esta composición define una multiplicación en

$$\mathrm{Hom}_A(M, M)$$

con la cual este grupo resulta ser un anillo con elemento unitario 1_M. Además, con la estructura de A-módulo resulta ser un A-álgebra.

Definición 1.3. *Un* A-*módulo* N *es submódulo de un* A-*módulo* M *si*

1) N *es un subgrupo de* M,
2) *la inclusión de* N *en* M *es un* A-*homomorfismo.*

Si N es un subgrupo de M tal que para toda $a \in A$ y toda $x \in N$ se tenga que $ax \in N$, la operación de $A \times M \to M$ induce en N una estructura de A-módulo y determina así un submódulo de M.

Si $f: M \to N$ es un A-homomorfismo de módulos, el *núcleo de* f, denotado Ker f es el A-submódulo de M formado por los elementos $x \in M$ tales que $f(x) = 0$ y la imagen de f, denotada Im f es el A-submódulo de N formado por los elementos $y \in N$ de la forma $y = f(x)$ con $x \in M$.

El homomorfismo $f: M \to N$ se llama monomorfismo (resp. epimorfismo), si f es una función inyectiva (resp. suprayectiva). Se dice que f es un isomorfismo si existe un A-homomorfismo $g: N \to M$ tal que $gf = 1_M$, $fg = 1_N$. Evidentemente f es un monomorfismo (resp. epimorfismo) si y sólo si Ker $f = 0$ (resp. Im $f = N$). Un homomorfismo es isomorfismo si y sólo si es monomorfismo y epimorfismo.

Una sucesión

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

de A-homomorfismo de módulos se dice que es exacta si

$$\mathrm{Im}\ f = \mathrm{Ker}\ g.$$

Por ejemplo $f: M' \to M$ es un monomorfismo si y sólo si la sucesión

$$0 \to M' \xrightarrow{f} M$$

es exacta, en donde $0 \to M'$ es el único A-homomorfismo posible de 0 en M'. Análogamente $g: M \to M''$ es un epimorfismo si y sólo si la sucesión

$$M \xrightarrow{g} M'' \to 0$$

es exacta, siendo $M'' \to 0$ el único posible A-homomorfismo de M'' en 0.

Una sucesión

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_{n+1}$$

de A-homomorfismos de módulos es exacta si $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$, $(1 \leq i < n)$.

2. Módulos cociente

Sea M un A-módulo y M' un submódulo de M.

Definición 2.1. *El módulo cociente* M/M' *de* M *con respecto a* M', *es el* A*-módulo cuyos elementos son las clases de equivalencia de* M *determinadas por la relación* $x \sim y$ *si* $x - y \in M'$, *con las operaciones inducidas por las de* M.

Se tiene el A-homomorfismo

$$g: M \to M/M'$$

llamado canónico definido por

$$g(x) = \text{clase de equivalencia de } x.$$

Si $i: M' \to M$ es la inclusión, entonces es inmediato que

Proposición 2.2. *La sucesión*

$$0 \to M' \xrightarrow{i} M \xrightarrow{g} M/M' \to 0$$

es exacta.

Proposición 2.3. *Sea*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

una sucesión exacta de A*-homomorfismos. Entonces, para cada* A*-homomorfismo* $h: M \to N$ *tal que* $h f = 0$, *existe un* A*-homomorfismo único* $\bar{h}: M'' \to N$ *tal que* $\bar{h} g = h$.

$$\begin{array}{ccccccc} 0 \to & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \to 0 \\ & & & \downarrow{\scriptstyle h} & \swarrow{\scriptstyle \bar{h}} & & \\ & & & N & & & \end{array}$$

Demostración. Sea $y \in M''$; por ser g suprayectiva existe $x \in M$ tal que $y = g(x)$. Si también $y = g(x')$ se tiene que $g(x) = g(x')$, de donde $g(x - x') = 0$ y por ser la sucesión exacta $x - x' \in \operatorname{Im} f$. Puesto que $hf = 0$, $h(x - x') = 0$, es decir, $h(x) = h(x')$. Esto demuestra que podemos definir la función $\bar{h}: M'' \to N$ con la fórmula

$$\bar{h}(y) = \bar{h}(g(x)) = h(x).$$

Esta función es un A-homomorfismo:

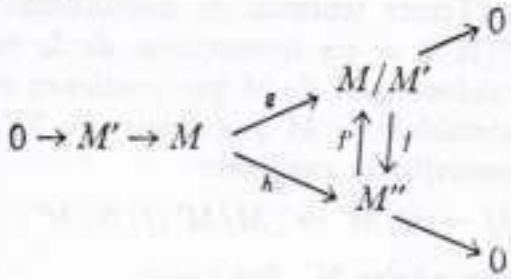
$$\bar{h}(y_1 + y_2) = \bar{h}(g(x_1) + g(x_2)) = \bar{h}(g(x_1 + x_2)) = h(x_1 + x_2) =$$
$$= h(x_1) + h(x_2) = \bar{h}(y_1) + \bar{h}(y_2);$$
$$\bar{h}(ay) = \bar{h}(ag(x)) = \bar{h}(g(ax)) = h(ax) = ah(x) = a\bar{h}(y).$$

Sean $\bar{h}_1 : M'' \to N$, $\bar{h}_2 : M'' \to N$ dos A-homomorfismos tales que $\bar{h}_1 g = h$, $\bar{h}_2 g = h$. Entonces, ya que g es epimorfismo resulta que $\bar{h}_1 = \bar{h}_2$; en efecto, si $y \in M''$, $y = g(x)$ y se tiene

$$\bar{h}_1(y) = \bar{h}_1(g(x)) = \bar{h}_2(g(x)) = \bar{h}_2(y)$$

con lo cual queda probada la unicidad de $\bar{h}$.

Corolario 2.4. (Primer teorema de isomorfismo.) *Si* $\mathrm{h} : \mathrm{M} \to \mathrm{M}''$ *es un epimorfismo con núcleo* M', *entonces existe un isomorfismo* $\mathrm{f} : \mathrm{M}/\mathrm{M}' \to \mathrm{M}''$ *tal que* $\mathrm{f}\,\mathrm{g} = \mathrm{h}$.



Demostración. De acuerdo con la proposición anterior, existen $f : M/M' \to M''$ $f' : M'' \to M/M'$ tales que $fg = h$ y $f'h = g$, de donde, $ff'h = h$ y $f'fg = g$. Pero como g y h son epimorfismos, se tiene que $f'f = 1_{M/M'}$ y $ff' = 1_{M''}$.

3. Teoremas de isomorfismos

Si $(N_i)_{i \in I}$ es una familia de submódulos de A-módulo M, la intersección $\cap_{i \in I} N_i$ es un submódulo de M. Si S es un subconjunto de M, el submódulo generado por S es la intersección de todos los submódulos de M que contienen a S. En particular $\sum_{i \in I} N_i$ denota el submódulo generado por la unión $\cup_{i \in I} N_i$. En el caso de dos submódulos, el generado por $N \cup N'$ se denota $N + N'$. En este caso los elementos de $N + N'$ son de la forma $x + x'$ con $x \in N$, $x' \in N'$.

Proposición 3.1. (Segundo teorema de isomorfismo.) *Si* N *y* N′ *son submódulos de un* A*-módulo* M, *entonces la composición de* A*-homomorfismos*

$$N \xrightarrow{j} N + N' \xrightarrow{e} (N + N')/N'$$

(en donde j es la inclusión y q el homomorfismo canónico) *es un epimorfismo con núcleo* $N \cap N'$. *Por tanto,*

$$N/N \cap N' \cong (N + N')/N'.$$

Demostración. Sea $y \in (N + N')/N$. Por ser q suprayectiva existen $x \in N$, $x' \in N'$ tales que $y = q(x + x')$, de donde, $y = q(x) + q(x') = q(j(x))$. Es decir, qj es suprayectiva. Si $qj(x) = 0$, entonces $x = j(x) \in N'$, o sea $x \in N \cap N'$. Inversamente, si $x \in N \cap N'$, $qj(x) = 0$, ya que $j(x) \in N'$.

Sea ahora

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

una sucesión exacta de A-módulos. Si N'' es un submódulo de M'', $g^{-1}(N'')$ es un submódulo de M y se tiene:

Proposición 3.2. (Tercer teorema de isomorfismo.) a) *La correspondencia* $N'' \mapsto g^{-1}(N'')$ *es un isomorfismo de la red de submódulos de* M'' *en la red de submódulos de* M *que contienen a* M'.

b) *Si* N *es un submódulo de* M *que contiene a* M', *entonces la composición de los homomorfismos canónicos*

$$M \to M/M' \to (M/M')/(N/M')$$

es un epimorfismo con núcleo N. *Por tanto,*

$$M/N \cong (M/M')/(N/M')$$

(a) significa que la correspondencia es biyectiva y conserva las inclusiones. La demostración es simple, (b) se sigue de las definiciones.

4. Productos y sumas directas

Sea $(M_\alpha)_{\alpha \in I}$ una familia de A-módulos izquierdos.

Definición 4.1. *El producto directo*

$$\Pi M_\alpha \quad (\alpha \in I)$$

de la familia (M_α) *es el* A*-módulo izquierdo cuyos elementos son las funciones*

$$u : I \to \cup M_\alpha \quad (\alpha \in I)$$

tales que $u(\alpha) \in M_\alpha$ (es decir, los elementos del producto cartesiano) *con las operaciones*

$$(u + v)(\alpha) = u(\alpha) + v(\alpha),$$
$$(au)(\alpha) = au(\alpha), \qquad (u, v \in M,\ a \in A,\ \alpha \in I).$$

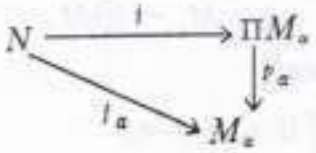
Para cada α se tiene el A-homomorfismo

$$p_\alpha\colon \Pi M_\alpha \to M_\alpha$$

llamado *proyección*, definido por

$$p_\alpha\ (u) = u(\alpha).$$

Proposición 4.2. (Propiedad universal del producto directo.) *Para cada* A*-módulo* N *y cada familia* $f_\alpha : N \to M_\alpha$ $(\alpha \in I)$ *de* A*-homomorfismos existe un* A*-homomorfismo único* $f: N \to \Pi M_\alpha$ *tal que* $p_\alpha f = f_\alpha$, *es decir, tal que hace conmutativos los diagramas*



Demostración. La función $f: N \to \Pi M_\alpha$ definida por

$$f(x)(\alpha) = f_\alpha(x) \qquad (x \in N, \alpha \in I)$$

es un A-homomorfismo:

$$f(x+y)(\alpha) = f_\alpha(x+y) = f_\alpha(x) + f_\alpha(y) = f(x)(\alpha) + f(y)(\alpha) = \\ = (f(x) + f(y))(\alpha),$$

$$f(ax)(\alpha) = f_\alpha(ax) = af_\alpha(x) = af(x)(\alpha) = (af(x))(\alpha),$$

o sea, $f(x+y) = f(x) + f(y)$ y $f(ax) = af(x)$.

Además $p_\alpha f(x) = f(x)(\alpha) = f_\alpha(x)$, o sea, $p_\alpha f = f_\alpha$ para cada α. Falta solamente ver la unicidad de la f. Si $g: N \to M$ es tal que $p_\alpha g = f_\alpha$, entonces,

$$g(x)(\alpha) = p_\alpha g(x) = f_\alpha(x) = p_\alpha f(x) = f(x)(\alpha),$$

de donde $g(x) = f(x)$.

La propiedad universal del producto directo suele expresarse diciendo que para definir un homomorfismo en un producto directo basta definir homomorfismos en sus factores.

Corolario 4.3. *La propiedad universal caracteriza al producto directo.*

Demostración. Sean M' un módulo y $p'_\alpha: M' \to M_\alpha$ homomorfismos tales que para todo módulo N y toda familia de homomorfismos g_α: $N \to M_\alpha$ existe un homomorfismo $g: N \to M'$ único tal que $p'_\alpha g = g_\alpha$. Según la propiedad universal de M y las hipótesis sobre M' existen

entonces $h: M' \to M$ y $h': M \to M'$ tales que $p_\alpha h = p'_\alpha$ y $p'_\alpha h' = p_\alpha$, de donde, $p_\alpha hh' = p_\alpha = p_\alpha 1_M$, y $p'_\alpha h'h = p'_\alpha = p'_\alpha 1_{M'}$. De acuerdo con las unicidades, $hh' = 1_M$ y $h'h = 1_{M'}$, por lo cual M' y ΠM_α son isomorfos.

Definición 4.4. *La suma directa*

$$M = \oplus M_\alpha \ (\alpha \in I)$$

de la familia (M_α) *es el* A*-submódulo de* $\Pi \mathrm{M}_\alpha$ *cuyos elementos son las funciones* $\mathrm{u}: \mathrm{I} \to \cup \mathrm{M}_\alpha$ *tales que para toda* α*, excepto un número finito de ellas,* $\mathrm{u}(\alpha) = 0$.

En este caso, para cada α existe un A-homomorfismo

$$i_\alpha : M_\alpha \to \oplus M_\alpha$$

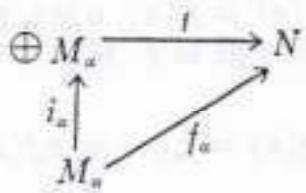
llamado *inclusión* dado por

$$i_\alpha(x_\alpha)(\beta) = \begin{cases} 0 \text{ si } \beta \neq \alpha, \\ x_\alpha \text{ si } \beta = \alpha, \end{cases} \quad (\alpha, \beta \in I,\ x_\alpha \in M_\alpha).$$

Nótese que si el conjunto de índices I es finito, la suma directa coincide con el producto directo. La notación en estos casos será

$$M_1 \times M_2 \times \cdots \times M_n, M_1 \oplus M_2 \oplus \cdots \oplus M_n.$$

Proposición 4.5. (Propiedad universal de la suma directa.) Para *cada* A*-módulo* N *y cada familia de homomorfismos* $\mathrm{f}_\alpha : \mathrm{M}_\alpha \to \mathrm{N}$ $(\alpha \in \mathrm{I})$ *existe un homomorfismo* $\mathrm{f}: \oplus \mathrm{M}_\alpha \to \mathrm{N}$ *único tal que* $\mathrm{fi}_\alpha = \mathrm{f}_\alpha$ *es decir, tal que hace conmutativos los diagramas*



La propiedad universal de la suma directa se expresa diciendo que para definir un homomorfismo desde una suma directa, basta definirla desde cada uno de los sumandos.

Corolario 4.6. *La propiedad universal caracteriza a la suma directa.*

Las demostraciones de 4.5 y 4.6 son parecidas a las correspondientes del producto y se dejan al lector, así como la de la siguiente propiedad bien conocida.

Proposición 4.7. *Sea* $\mathrm{M}_1, \ldots, \mathrm{M}_n$ *una familia de submódulos de un* A*-módulo* M. *Entonces se cumplen las condiciones*

1) $M_1 + \cdots + M_n = M$,
2) $M_k \cap (M_1 + \cdots + M_{k-1} + M_{k+1} + \cdots + M_n) = 0$, $(1 \leq k \leq n)$,

si y solamente si el homomorfismo de la suma directa $M_1 \oplus \cdots \oplus M_n \to M$ *que determinan las inclusiones* $M_i \to M$ *es un isomorfismo.*

Bajo las hipótesis de la proposición anterior, cada elemento x de M puede escribirse en forma única como

$$x = x_1 + \cdots + x_n \quad (x_k \in M_k).$$

Podemos entonces definir los A-endomorfismos

$$p_k : M \to M \qquad (1 \leq k \leq n),$$

haciendo $p_k(x) = x_k$. Estos endomorfismos tienen las tres propiedades siguientes:

1) $p_j p_k = 0$ si $j \neq k$,
2) $p_k p_k = p_k$,
3) $p_1 + \cdots + p_n = 1_M$.

Recíprocamente,

Proposición 4.8. *Si* $p_1, \ldots, p_n$ *es una familia de* A*-endomorfismos de* M *tales que cumplen las propiedades* (1), (2) y (3), *entonces* $M \cong M_1 \oplus \cdots \oplus M_n$ *con* $M_k = Im\ p_k$.

La demostración es muy simple.

Definición 4.9. *Se dice que la sucesión exacta de* A*-módulos*

$$0 \to M' \xrightarrow{f} M \underset{h}{\overset{g}{\rightleftarrows}} M'' \to 0 \qquad (1)$$

se escinde si existe un A*-homomorfismo* $h : M'' \to M$ *tal que* $gh = 1_{M''}$.

Obsérvese que en este caso existe también un A-homomorfismo k: $M \to M'$ tal que la sucesión $0 \to M'' \underset{h}{\to} M \underset{k}{\to} M' \to 0$ es exacta y la composición $kf = 1_{M'}$.

Por ejemplo, si $M = M' \oplus M''$ es una suma directa de A-módulos, la sucesión exacta

$$0 \to M' \xrightarrow{i'} M' \oplus M'' \xrightarrow{p''} M'' \to 0$$

(en donde i' es la inclusión y p'' la proyección respectivas) se escinde, pues, la inclusión $i'' : M'' \to M$ es un A-homomorfismo tal que $p''i'' = 1_{M''}$. Inversamente, es válida la

Proposición 4.10. *Si* (1) *es una sucesión exacta escindible, entonces los isomorfismos* $h: M'' \to M$, $f: M' \to M$ *inducen un isomorfismo* $M' \oplus M'' \to M$ *dado por* $(x, y) \mapsto f(x) + h(y)$.

Demostración. Si $f(x) + h(y) = 0$, se tiene que $0 = gf(x) + gh(y) = y$. Por tanto, $f(x) = 0$, de donde también $x = 0$. Sea ahora z un elemento de M. Tenemos que $z = z - hg(z) + hg(z)$. Pero $g(z - hg(z)) = g(z) - g(z) = 0$ y según la exactitud $z - hg(z) = f(x)$ para cierta $x \in M'$. Por tanto, $z = f(x) + h(y)$ con $y = g(z)$.

5. *Módulos libres*

Si A es, como antes, un anillo con 1 e I es un conjunto arbitrario, con $A^{(I)}$ se denota la suma directa de la familia de A-módulos A_α, $\alpha \in I$, con $A_\alpha = A$ considerado como A-módulo izquierdo.

Sea M un A-módulo izquierdo. A cada familia de elementos de M con índices en I

$$B = (b_\alpha)_{\alpha \in I} \quad (b_\alpha \in M)$$

se le asocia el A-homomorfismo

$$\theta_B: A^{(I)} \to M$$

definido por

$$\theta_B((a_\alpha)) = \sum a_\alpha b_\alpha$$

(la suma tiene sentido, pues casi toda a_α vale 0).

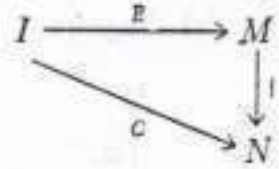
Definición 5.1. *La familia* B *es*

a) *linealmente independiente si* θ_B *es inyectiva,*
b) *una familia de generadores de* M *si* θ_B *es suprayectiva,*
c) *una base de* M *si* θ_B *es biyectiva.*

Si I es un conjunto finito, $I = \{1, 2, \ldots, n\}$, se escribe $A^{(I)} = A^n$. Obsérvese que M tiene una base con n elementos si y sólo si A^n es isomorfo a M.

Una propiedad fundamental que caracteriza las bases es la siguiente [la familia $B = (b_\alpha)_{\alpha \in I}$ es realmente una función $B: I \to M$; $B(\alpha) = b_\alpha$]:

Proposición 5.2. *Una familia* $B: I \to M$ *es una base del* A*-módulo* M *si y solamente si dado un* A*-módulo arbitrario* N *y una familia* $C: I \to N$ *existe un* A*-homomorfismo único* $f: M \to N$ *tal que* $fB = C$, *o sea, tal que el diagrama*



es conmutativo.

Se deja como ejercicio la demostración.

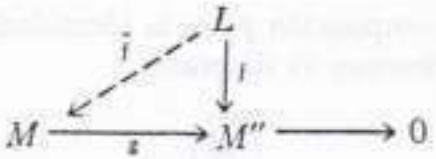
Definición 5.3. *Un* A*-módulo* L *es libre si y sólo si tiene una base.*

En particular el A-módulo $A^{(I)}$ es libre y la aplicación

$$I \to A^{(I)}$$

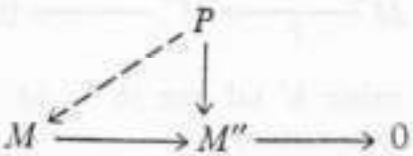
dada por la inclusión natural es una base que se llamará canónica.

Corolario 5.4. *Si* $M \xrightarrow{g} M'' \to 0$ *es una sucesión exacta,* L *es un módulo libre y* $f: L \to M''$ *un* A*-homomorfismo, entonces existe* $\bar{f}: L \to M$ *tal que* $\bar{f} = g\,f$*, es decir, tal que el diagrama*



es conmutativo.

Los módulos que satisfacen la propiedad del corolario anterior se llaman *proyectivos;* es decir, un A-módulo P es proyectivo si y sólo si para cualquier sucesión exacta $M \to M'' \to 0$ de A-módulos y cualquier A-homomorfismo $P \to M''$ *existe* un A-homomorfismo $P \to M$ tal que el diagrama



es conmutativo.

En particular, los módulos libres son proyectivos.

Proposición 5.5. *Todo* A*-módulo* M *es cociente de un* A*-módulo libre* L.

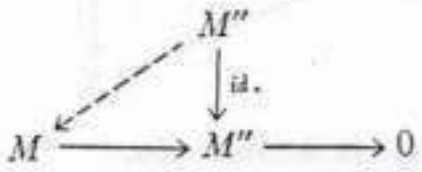
Demostración. Basta considerar $L = A^{(M)}$, el módulo libre con base M y la aplicación natural $L \to M$ que es un epimorfismo.

Proposición 5.6. *Si en una sucesión exacta de* A*-homomorfismos*

$$0 \to M' \to M \to M'' \to 0$$

M'' *es proyectivo, entonces la sucesión se escinde.*

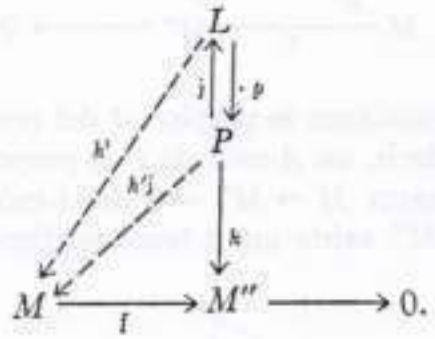
Demostración. En efecto, del diagrama



por ser M'' proyectivo, existe un homomorfismo $M'' \to M$ tal que $M'' \to M \to M''$ es la identidad (véase la definición 4.9).

Proposición 5.7. *Todo* A*-módulo proyectivo es sumando directo de un* A*-módulo libre e inversamente.*

Demostración. La parte directa es consecuencia de las dos proposiciones anteriores. Para la parte inversa observemos primero que si P es sumando directo de un módulo libre L, existen homomorfismos $P \xrightarrow{j} L \xrightarrow{p} P$ tales que su composición pj es la identidad. Sea $f: M \to M''$ un epimorfismo. Consideremos el diagrama



Por ser L proyectivo existe h' tal que $fh' = hp$. Entonces $h = hpj = f(h'j)$, de donde P es proyectivo.

Proposición 5.8. *Si* $\{P_\alpha\}$ *es una familia de módulos proyectivos, entonces su suma directa* $\bigoplus P_\alpha$ *es proyectivo.*

Demostración. Ya que cada P_α es sumando directo de un libre L_α entonces $P = \bigoplus P_\alpha$ será sumando directo de $L = \bigoplus L_\alpha$, que es libre.

6. Módulos noetherianos y artinianos

Definición 6.1. *Un* A*-módulo se llama noetheriano si toda cadena ascendente de submódulos*

$$M_1 \subset M_2 \subset \ldots \subset M_n \subset \ldots$$

es estacionaria (es decir, existe n_0 tal que para toda $n \geq n_0$, $M_n = M_{n_0}$).

Definición 6.2. *Un* A*-módulo se llama artiniano si toda cadena descendente de submódulos*

$$M_1 \supset M_2 \supset \ldots \supset M_n \supset \ldots$$

es estacionaria.

En particular, si el anillo A considerado como A-módulo izquierdo es noetheriano (resp. artiniano) A se llama anillo noetheriano (resp. artiniano) izquierdo.

Obsérvese que la propiedad de ser noetheriano y artiniano se hereda a submódulos y a módulos cociente.

Proposición 6.3. *Las tres condiciones siguientes son equivalentes:*

a) *El* A*-módulo* M *es noetheriano.*
b) *Todo submódulo de* M *es finitamente generable.*
c) *Todo conjunto no vacío de submódulos de* M *tiene elementos máximos.*

Proposición 6.4. *Las dos condiciones siguientes son equivalentes:*

a) *El* A*-módulo* M *es artiniano.*
b) *Todo conjunto no vacío de submódulos de* M *tiene elementos mínimos.*

Las demostraciones son bien conocidas y aquí se dejan como ejercicios.

Lema 6.5. *Si*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0,$$

es una sucesión exacta de A*-módulos tal que* M′ *y* M″ *son finitamente generables, entonces* M *lo es también.*

Demostración. Sean $x'_1, \ldots, x'_n$ y $x''_1, \ldots, x''_m$ familias de generadores de M' y M'' respectivamente. Entonces la familia $x_1, \ldots, x_n, y_1, \ldots, y_m$ formada con elementos de M tales que $x_i = f(x'_i), g(y_j) = x''_j$, es evidentemente una familia de generadores de M.

Proposición 6.6. *Si el anillo* A *es noetheriano* (izquierdo) *entonces todo* A*-módulo* (izquierdo) *finitamente generado es noetheriano.*

Demostración. Por inducción sobre el número de elementos con que se pueda generar un módulo. Si M puede generarse con un solo elemento, existe entonces un epimorfismo de A sobre M. Por consiguiente,

todo submódulo N de M es isomorfo a un cociente de algún ideal I de A, el cual es finitamente generable por serlo I. Supongamos ahora que $x_1, \ldots, x_m$ es una familia de generadores de M. Sea M' el submódulo de M generado por $x_2, \ldots, x_m$. Entonces M' y M/M' pueden generarse con menos de m elementos. Si N es un submódulo de M, se tiene la sucesión exacta

$$0 \to N' \to N \to N'' \to 0$$

con N' submódulo de M' y N'' submódulo de M''. De acuerdo con la hipótesis, N' y N'' son finitamente generables, lo cual, según el lema 6.5, implica que N lo es.

7. Series de composición

Definición 7.1. *Un A-módulo se llama irreducible o simple si es distinto de cero y sus únicos submódulos son él mismo y el módulo* 0.

Un módulo cociente M/N resulta entonces irreducible si y sólo si N es un submódulo máximo de M.

Proposición 7.2. *En un A-módulo finitamente generable todo submódulo propio está contenido en un submódulo máximo.*

Demostración. Esto resulta de que la familia de todos los submódulos propios de un A-módulo finitamente generable M es inductiva. En efecto, sea $M_1 \subset M_2 \subset \ldots \subset M_n \subset \ldots$ una familia de submódulos propios de M. Entonces $\cup_{i \in N} M_i$ es una submódulo *propio* pues, en caso contrario, si $(u_1, \ldots, u_r)$ es una familia de generadores de M, existiría $k \in N$ tal que $u_1, \ldots, u_r \in M_k$ y, por tanto, M_k sería igual a M, lo cual es falso.

Sea M un A-módulo. Una cadena de submódulos de M se llama *serie de composición de M* si es de la forma

$$M = M_0 \supset M_1 \supset \ldots \supset M_k = 0$$

y los cocientes

$$M_0/M_1, M_1/M_2, \ldots, M_{k-1}/M_k$$

(llamados también factores de la serie) son irreducibles; en particular, los factores de la serie son distintos de cero y, por tanto $M_i \neq M_{i+1}$ para $1 \leq i \leq k-1$. k se llama la *longitud de la serie de composición.*

Proposición 7.3. *Si un módulo es noetheriano y artiniano, entonces tiene series de composición.*

Demostración. Se construye, por inducción, una cadena descendente de submódulos: $M_0 = M$; M_{i+1} es un submódulo de M máximo en la

familia de los submódulos propios de M_i, el cual existe por ser M_i noetheriano. Esta cadena es finita por ser las continencias propias y M artiniano. Por ser M_{i+1} máximo en M_i, ésta es una serie de composición de M.

Proposición 7.4. *Si el* A*-módulo* M *tiene una serie de composición de longitud* k

$$M = M_0 \supset M_1 \supset \ldots \supset M_k = 0$$

y

$$N_1 \supset N_2 \supset \ldots \supset N_t, N_i \neq N_{i+1}\ (1 \leq i \leq t-1)$$

es una cadena arbitraria de submódulos de M, *entonces* $t \leq k+1$.

Demostración. Supongamos cierta la proposición para todos los A-módulos que posean series de composición de longitud menor que k y consideremos primero el caso en que $N_1 = M_0$. Si se tiene que $N_2 \subset M_1$, entonces, como M_1 tiene una serie de composición de longitud $k-1$ y $N_2 \supset \ldots \supset N_t$ es una cadena de submódulos de M_1, según la hipótesis de inducción se tiene que $t-1 \leq k$, o sea, $t \leq k+1$. Si $N_2 \not\subset M_1$, consideremos el A-módulo $M_1 \cap N_2$ que por ser submódulo de M_1 es noetheriano y artiniano y, según 7.3 tiene entonces series de composición. Sea, pues,

$$M_1 \cap N_2 = L_0 \supset L_1 \supset \ldots \supset L_s = 0$$

una serie de composición.

Si consideramos la cadena de submódulos de M_1

$$M_1 \supset M_1 \cap N_2 \supset L_1 \supset \ldots \supset L_s$$

nuevamente, según la hipótesis de inducción, se tiene que $s+2 \leq k$. Ya que $N_2 \not\subset M_1$, $M_1 + N_2 = M$, pues M_1 es un submódulo máximo en M. Entonces

$$M/M_1 = (M_1 + N_2)/M_1 \cong N_2/M_1 \cap N_2.$$

Por tanto, la cadena

$$N_2 \supset M_1 \cap N_2 \supset L_1 \supset \ldots \supset L_s = 0$$

es una serie de composición de N_2 y al considerar la cadena de submódulos de N_2

$$N_2 \supset N_3 \supset \ldots \supset N_t$$

se tiene, nuevamente por la inducción, que $t-1 \leq s+2$. Por tanto, $t-1 \leq s+2 \leq k$ y $t \leq k+1$.

Finalmente, al considerar el caso en que $N_1 \neq M$, se puede formar la cadena

$$M \supset N_1 \supset \ldots \supset N_t$$

y al reducirlo al caso anterior resulta $t + 1 \leq k + 1$, de donde $t \leq k + 1$ también.

Corolario 7.5. *Dos series de composición de un módulo tienen la misma longitud.*

Definición 7.6. *Un* A*-módulo* M *es de longitud finita si tiene una serie de composición. En este caso, a la longitud de la serie se le llama la longitud del módulo y se denota*

$$\text{long } M.$$

Otra consecuencia de la proposición anterior es que si un módulo tiene una serie de composición es noetheriano y artiniano, lo cual, junto con la proposición 7.3 puede enunciarse en la forma siguiente:

Teorema 7.7. *Un módulo tiene series de composición si y solamente si es noetheriano y artiniano.*

Definición 7.8. *Dos series de composición de un* A*-módulo* M

$$M = M_0 \supset M_1 \supset \ldots \supset M_k = 0, \tag{1}$$

$$M = N_0 \supset N_1 \supset \ldots \supset N_k = 0, \tag{2}$$

se llaman equivalentes si existe una permutación σ *del conjunto* $\{1, 2, \ldots, k\}$ *tal que*

$$N_i/N_{i+1} \cong M_{\sigma(i)}/M_{\sigma(i)+1}, \quad (1 \leq i \leq k-1).$$

Teorema 7.8. (Jordan-Hölder.) *Todas las series de composición de un* A*-modulo son equivalentes.*

Dmostración. Se hará por inducción sobre la longitud de las series de composición. Consideremos primero el caso en que $M_1 = N_1$. La inducción da aquí el resultado. Consideremos, pues, el caso $M_1 \neq N_1$. Se tiene, entonces, que $M_1 + N_1 = M$ y, por tanto, que

$$M_0/M_1 \cong N_1/M_1 \cap N_1, \tag{3}$$

$$N_0/N_1 \cong M_1/M_1 \cap N_1, \tag{4}$$

y estos cocientes son A-módulos irreducibles. Sea

$$M_1 \cap N_1 = L_0 \supset L_1 \supset \ldots, \supset L_t = 0$$

una serie de composición de $M_1 \cap N_1$. Formemos las dos siguiente series de composición.

$$M = M_0 \supset M_1 \supset M_1 \cap N_1 \supset L_1 \supset \ldots \supset L_t = 0, \tag{5}$$

$$M = N_0 \supset N_1 \supset M_1 \cap N_1 \supset L_1 \supset \ldots \supset L_t = 0. \tag{6}$$

Las series (1) y (4) son equivalentes, pues están dentro del primer caso ya demostrado. Asimismo (2) y (6) lo son. Además, las fórmulas (3) y (4) demuestran que las series (5) y (6) son equivalentes, de donde (1) y (2) lo son.

Proposición 7.9. *Si*

$$0 \to M'' \to M \xrightarrow{g} M' \to 0$$

es una sucesión exacta de módulos, entonces M *es de longitud finita si y sólo si* M′ *y* M″ *lo son. En este caso es válida la igualdad*

$$\text{long } M = \text{long } M' + \text{long } M''$$

Demostración. Si M es de longitud finita, de acuerdo con la proposición 7.7, M es artiniano y noetheriano. Entonces M' y M'' también lo son y, según la misma proposición, son de longitud finita. Inversamente, supongamos que

$$M' = M'_0 \supset M'_1 \supset \ldots \supset M'_h = 0,$$
$$M'' = M''_0 \supset M''_1 \supset \ldots \supset M''_k = 0$$

son series de composición de M' y M''. Entonces, usando el segundo teorema de isomorfismo es fácil comprobar que

$$M \supset g^{-1}(M''_1) \supset \ldots \supset g^{-1}(M''_k) \supset M'_1 \supset \ldots \supset M'_h = 0$$

es un serie de composición de M. Ésta es de longitud $h + k$.

Corolario 7.10. *Si*

$$M \supset M_1 \supset \ldots \supset M_k = 0$$

es una cadena de A*-módulos tal que* M_i/M_{i+1} *es de longitud finita para toda* i, *entonces* M *lo es y*

$$\text{long } M = \Sigma \text{ long } M_i/M_{i+1}$$

8. Módulos inescindibles

Definición 8.1. *Se dice que un* A*-módulo* M *es escindible si existe una sucesión exacta y escindible de* A*-módulos de la forma*

$$0 \to M' \to M \to M'' \to 0$$

con M′ *y* M″ *distintos de* 0.

Esto equivale a decir que M puede expresarse como una suma directa de submódulos propios

$$M = M_1 \oplus M_2 \qquad (M_1, M_2 \neq 0)$$

En caso contrario, diremos que M es *inescindible*. Todo módulo irreducible es inescindible, pero no inversamente. Por ejemplo los **Z**-módulos **Z** y $\mathbf{Z}_4$.

Proposición 8.2. *Todo módulo artiniano es isomorfo a una suma directa de un número finito de módulos inescindibles.*

Demostración. Sea C el conjunto de submódulos del A-módulo dado M para los cuales la proposición es falsa. Si C es no vacío existe en C un elemento mínimo, es decir, un submódulo mínimo M_0, con la propiedad de no ser suma directa de módulos inescindibles. M_0 es, por tanto, escindible. Sea $M_0 = M_1 \oplus M_2$, M_1, $M_2 \neq 0$. Entonces M_1, M_2 son submódulos propios de M_0 y, por tanto, no pueden estar en C. Luego M_1 y M_2 son sumas directas de un número finito de A-módulos inescindibles y, por consiguiente, M_0 también lo es, lo cual es una contradicción.

Lema 8.3. *Todo endomorfismo inyectivo de un* A*-módulo artiniano es un automorfismo.*

Demostración. Sea M el A-módulo artiniano y $\alpha: M \to M$ un monomorfismo. Entonces la cadena de submódulos de M

$$M \supset \operatorname{Im}\alpha \supset \operatorname{Im}\alpha^2 \supset \ldots \supset \operatorname{Im}\alpha^n \supset \ldots$$

es estacionaria. Sea n tal que

$$\operatorname{Im}\alpha^n = \operatorname{Im}\alpha^{n+1},$$

y sea x un elemento de M. Entonces, $\alpha^n x = \alpha^{n+1}$ y, de donde $\alpha^n(x - \alpha y) = 0$ $(y \in M)$. Como α es monomorfismo, también α^n lo es, de donde $x = \alpha y$.

Lema 8.4. *Todo endomorfismo suprayectivo de un* A*-módulo noetheriano es un automorfismo.*

Demostración. Sea M el A-módulo noetheriano y $\alpha: M \to M$ un epimorfismo. Entonces la cadena de submódulos de M

$$\operatorname{Ker}\alpha \subset \operatorname{Ker}\alpha^2 \subset \ldots \subset \operatorname{Ker}\alpha^n \subset \ldots$$

es estacionaria. Sea n tal que

$$\operatorname{Ker} \alpha^n = \operatorname{Ker} \alpha^{n+1}$$

y sea x un elemento de M tal que $\alpha x = 0$. Como α es epimorfismo, también α^n lo es. Existe entonces $y \in M$ tal que $x = \alpha^n y$. Por consiguiente, $\alpha^{n+1} y = 0$ y de la igualdad de los núcleos de α^n y α^{n+1} resulta que también $\alpha^n y = 0$, es decir $x = 0$ y α es inyectiva.

Corolario 8.5. *Si* M *es un* A*-módulo artiniano, noetheriano e inescindible y* α *un endomorfismo no nilpotente de* M, *entonces* α *es un automorfismo de* M.

Demostración. Como antes, la cadena de imágenes es estacionaria:

$$M \supset \operatorname{Im} \alpha \supset \ldots \supset \operatorname{Im} \alpha^n = \operatorname{Im} \alpha^{n+1} = N.$$

Entonces, $\alpha^n | N : N \to N$ es suprayectivo y como N es noetheriano, según el lema anterior $\alpha^n | N$ es un automorfismo de N. Esto implica que N es un sumando directo de M. Ya que α no es nilpotente, $N \neq 0$, de donde $N = M$, pues, de lo contrario, M sería escindible contra la hipótesis. Esto implica que $\operatorname{Im} \alpha = M$, lo que, nuevamente según el lema anterior, implica que α es un automorfismo de M.

Proposición 8.6. *Si* M *es un* A*-módulo noetheriano, artiniano e inescindible, y* α, β *son endomorfismos de* M *tales que* $1_M = \alpha + \beta$, *entonces al menos uno de los dos es un automorfismo de* M.

Como $\beta = 1 - \alpha$, β conmuta con α, de donde

$$1_M = (\alpha + \beta)^n = \sum \binom{n}{k} \alpha^k \beta^{n-k},$$

por lo que α y β no pueden ser, ambos, nilpotentes y entonces la proposición resulta del último corolario.

Teorema 8.7. (Krull-Schmidt.) *Si*

$$M \cong M_1 \oplus \cdots \oplus M_r \cong N_1 \oplus \cdots \oplus N_s$$

son dos descomposiciones de un A*-módulo artiniano y noetheriano en suma directa de* A*-módulos inescindibles, entonces* r = s *y existe una permutación* σ *del conjunto de índices* $\{1, \ldots, r\}$ *tal que*

$$M_i \cong N_{\sigma(i)}.$$

Demostración. Para los efectos de la demostración puede suponerse que se tiene una igualdad

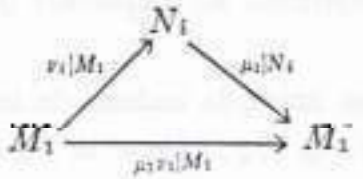
$$M_1 \oplus \cdots \oplus M_r = N_1 \oplus \cdots \oplus N_s = M.$$

Sean $\mu_1, \ldots, \mu_r, \nu_1, \ldots, \nu_s$ los endomorfismos asociados a las dos descomposiciones de M en suma directa (capítulo 1, sección 4, pág. 14).

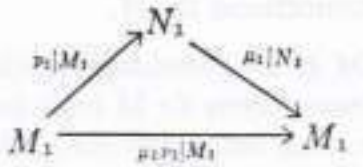
Tenemos entonces

$$\mu_1 + \cdots + \mu_r = 1, \quad \mu_i^2 = \mu_i, \quad \mu_i \mu_j = 0 \quad (i \neq j),$$
$$\nu_1 + \cdots + \nu_s = 1, \quad \nu_j^2 = \nu_j, \quad \nu_j \nu_k = 0 \quad (j \neq k),$$
$$M_i = \operatorname{Im} \mu_i \qquad N_j = \operatorname{Im} \nu_j.$$

Para $1 \leq i \leq s$ consideremos las composiciones



Como $\sum_{i=1}^{s} \mu_1 \nu_i = \mu_1$, $\sum_{i=1}^{s} \mu_1 \nu_i|M_1 = 1_{M_1}$, pues $\mu_1|M_1 = 1_{M_1}$.
De acuerdo con la proposición anterior, algún sumando es un automorfismo de M_1. Supongamos que éste es $\mu_1 \nu_1|M_1$.



Ya que N_1 es inescindible y M_1 no nulo, $\nu_1|M_1$ es un isomorfismo de M_1 en N_1.

Consideremos ahora el endomorfismo $\alpha: M \to M$ definido por

$$\alpha = \nu_1 \mu_1 + \mu_2 + \cdots + \mu_r.$$

Demostraremos que α es un automorfismo. Supongamos primero que $\alpha(x) = 0$ $(x \in M)$. Entonces

$$\nu_1 \mu_1(x) + \mu_2(x) + \cdots + \mu_r(x) = 0.$$

Y, por tanto,

$$\mu_1 \alpha(x) = \mu_1 \nu_1 \mu_1(x) = 0.$$

Pero como $\mu_1(x) \in M_1$ y en M_1 $\mu_1 \nu_1$ es un automorfismo, se tiene que $\mu_1(x) = 0$. Entonces

$$\mu_2(x) + \cdots + \mu_r(x) = 0,$$

de donde $\mu_i(x) = 0$ para $1 \leq i \leq r$, por lo que $x = 0$. Así pues, α es inyectivo y como M es artiniano, del lema 8.3 resulta que α es un automorfismo. Consideremos, entonces, el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M & \longrightarrow & M/M_1 & \longrightarrow & 0 \\ & & \cong\downarrow{\scriptstyle \nu_1} & & \cong\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha'} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & M & \longrightarrow & M/N_1 & \longrightarrow & 0 \end{array}$$

que es conmutativo ya que si $y \in M_1$, $y = \mu_1(x)$ y se tiene

$$\begin{aligned} \alpha y = \alpha\,\mu_1(x) &= \nu_1\,\mu_1\,\mu_1(x) + \mu_2\,\mu_2(x) + \cdots + \mu_r\,\mu_2(x) \\ &= \nu_1\mu_1(x) = \nu_1 y. \end{aligned}$$

Por tanto, existe un isomorfismo $\alpha' : M/M_1 \to M/N_1$. Entonces se tiene que

$$M_2 \oplus \cdots \oplus M_r \cong N_2 \oplus \cdots \oplus N_s$$

y, por inducción, queda probado el teorema.

9. Producto tensorial de módulos

En esta sección supondremos que el anillo A es conmutativo y con elemento unitario y trataremos únicamente el concepto de producto tensorial de módulos sobre anillos conmutativos. En los capítulos posteriores se utilizarán casi exclusivamente productos tensoriales de espacios vectoriales.

Definición 9.1. *El producto tensorial* $\mathrm{M} \otimes_A \mathrm{N}$ *de dos* A*-módulos* M *y* N *es el* A*-módulo cociente del* A*-módulo libre* $\mathrm{A}^{(\mathrm{M}\times\mathrm{N})}$ *con respecto al submódulo* R *generado por los elementos de la forma*

$$\begin{aligned} &(x + x', y) - (x, y) - (x', y), \\ &(x, y + y') - (x, y) - (x, y'), \\ &(ax, y) - a(x, y), \\ &(x, ay) - a(x, y), \qquad (x, x' \in M, y, y' \in N, a \in A). \end{aligned}$$

Se tiene, pues, la sucesión exacta de A-módulos

$$0 \to R \to A^{(M\times N)} \to M \otimes_A N \to 0.$$

La composición φ de las aplicaciones

$$\begin{array}{ccc} & A^{(M\times N)} & \\ \nearrow & & \searrow \\ M \times N & \xrightarrow[\varphi]{} & M \otimes_A N \end{array}$$

que se denota

$$\varphi(x, y) = x \otimes y$$

es bilineal en el sentido común, es decir, se tiene que

$$(x + x') \otimes y = x \otimes y + x' \otimes y,$$
$$x \otimes (y + y') = x \otimes y + x \otimes y',$$
$$a(x \otimes y) = ax \otimes y = x \otimes ay.$$

Además, $M \otimes_A N$ está generado por la imagen de φ, es decir, por los elementos de la forma $x \otimes y$.

Sea ahora Q un A-módulo y $f: M \times N \to Q$ una aplicación bilineal. Consideremos el diagrama

$$0 \to R \to L \xrightarrow{p} M \otimes_A N \to 0 \qquad (L = A^{(M \times N)})$$
$$\uparrow i \quad \searrow \quad \downarrow \bar{f}$$
$$M \times N \xrightarrow[f]{} Q$$

Por ser $M \times N$ una base del A-módulo libre L, existe un A-homomorfismo $f_1: L \to Q$ que extiende a f (proposición 5.2). Ahora, ya que f es bilineal, $f_1(R) = 0$ y, por tanto, existe un A-homomorfismo (proposición 2.3) $\bar{f}: M \otimes_A N \to Q$ tal que $\bar{f} p i = f$, de donde,

$$\bar{f} \varphi = f.$$

Además, éste es el único A-homomorfismo con la propiedad anterior. En efecto, sea $\bar{f}'$ tal que $\bar{f}' \varphi = f$. Entonces $\bar{f} p i = \bar{f}' p i$, de donde $\bar{f} p = \bar{f}' p$ (proposición 5.2) y entonces $\bar{f} = \bar{f}'$ (proposición 2.3).

Lo que acabamos de discutir puede resumirse en la forma siguiente. Si se tiene una función de la familia de generadores $x \otimes y$ de $M \otimes_A N$ en un A-módulo Q tal que

$$f((x + x') \otimes y) = f(x \otimes y) + f(x' \otimes y),$$
$$f(x \otimes (y + y')) = f(x \otimes y) + f(x \otimes y'),$$
$$af(x \otimes y) = f(ax \otimes y) = f(x \otimes ay),$$

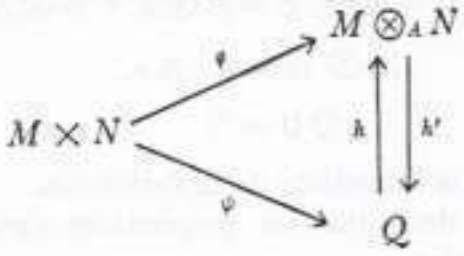
existirá un homomorfismo único $\bar{f}: M \otimes_A N \to Q$ que extiende a f. Podemos enunciar entonces la

Proposición 9.2. (Propiedad universal del producto tensorial.) *Si* Q *es un* A*-módulo y* $\mathrm{f}: \mathrm{M} \times \mathrm{N} \to \mathrm{Q}$ *es una función bilineal, existe entonces un* A*-homomorfismo* $\bar{\mathrm{f}}: \mathrm{M} \otimes_A \mathrm{N} \to \mathrm{Q}$ *único tal que* $\bar{\mathrm{f}} \varphi = \mathrm{f}$.

Esta propiedad caracteriza al producto tensorial:

Corolario 9.3. *Si* Q *es un* A*-módulo y* $\psi: \mathrm{M} \times \mathrm{N} \to \mathrm{Q}$ *una función bilineal con la propiedad universal de la proposición anterior, entonces existe un* A*-isomorfismo* $\mathrm{h}: \mathrm{M} \otimes_A \mathrm{N} \to \mathrm{Q}$ *tal que* $\mathrm{h} \varphi = \psi$.

Demostración. Según la hipótesis y la propiedad universal de $M \otimes_A N$ existen homomorfismos h, h'

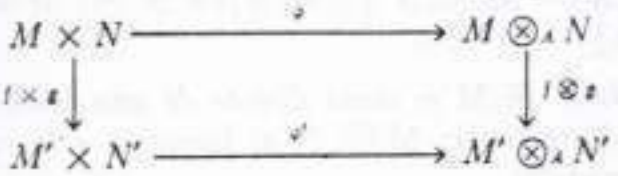


tales que $h'\varphi = \psi$, $h\psi = \varphi$. Entonces $hh'\varphi = \varphi$, $h'h\psi = \psi$. Pero también

$$1_{M\otimes_A N}\varphi = \varphi, \quad 1_Q\psi = \psi,$$

de donde, por la unicidad que se pide en la propiedad universal, $hh' = 1$, $h'h = 1$.

Sean $f: M \to M'$, $g: N \to N'$ homomorfismos de A-módulos. Consideremos el diagrama



Ya que la composición

$$M \times N \xrightarrow{f\times g} M' \times N' \xrightarrow{\varphi'} M' \otimes_A N'$$

es bilineal, según la propiedad universal del producto tensorial *existe un* A-*homomorfismo único* denotado

$$f \otimes g : M \otimes_A N \to M' \otimes_A N'$$

y que se llama producto tensorial de los A-*homomorfismos* f *y* g.

Este A-homomorfismo queda determinado por la fórmula

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$$

y de aquí se sigue la

Proposición 9.4. *Si*

$$M \xrightarrow{f} M' \xrightarrow{f'} M''$$

$$N \xrightarrow{g} N' \xrightarrow{g'} N''$$

son homomorfismos de A-*módulos entonces*

$$(f' \otimes g')(f \otimes g) = f'f \otimes g'g.$$

Otras propiedades del producto tensorial de A-homomorfismos son

$$(f_1 + f_2) \otimes g = f_1 \otimes g + f_2 \otimes g,$$

$$1_M \otimes 1_N = 1_{M \odot N},$$

$$f \otimes 0 = 0.$$

Éstas son consecuencia inmediata de la definición.

También es fácil demostrar las propiedades siguientes del producto tensorial de A-módulos.

Proposición 9.5. *Sean* L, M *y* N A*-módulos. Entonces se tienen los siguientes isomorfismos (naturales).*

$$A \otimes_A M \cong M, \quad M \otimes_A N \cong N \otimes_A M$$

$$L \otimes_A (M \otimes_A N) \cong (L \otimes_A M) \otimes_A N.$$

[La naturalidad de los isomorfismos significa, por ejemplo, que los functores $(M, N) \mapsto M \otimes_A N$ y $(M, N) \mapsto N \otimes_A M$ son naturalmente equivalentes.]

Proposición 9.6. *Si* M *es suma directa de una familia de submódulos* $M_1, \ldots, M_n$, *entonces* $M \otimes_A N$ *es isomorfo a la suma directa de la familia de módulos*

$$M_1 \otimes_A N, \ldots, M_n \otimes_A N.$$

Demostración. Según los comentarios anteriores a la proposición 4.8 existen endomorfismos $p_k : M \to M$ $(1 \leq k \leq n)$ tales que $\operatorname{Im} p_k = M_k$, $p_j p_k = 0$ $(j \neq k)$, $p_k p_k = p_k$ y $p_1 + \ldots + p_n = 1_M$. Consideremos ahora los endomorfismos

$$p_k \otimes 1_N : M \otimes N \to M \otimes N, \qquad (1 \leq k \leq n).$$

De acuerdo con la proposición 9.4 y las propiedades posteriores, se tiene que

$$(p_j \otimes 1)(p_k \otimes 1) = 0, \quad (j \neq k),$$

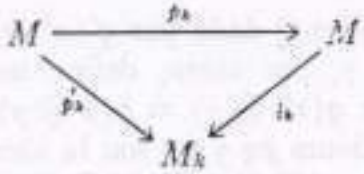
$$(p_k \otimes 1)(p_k \otimes 1) = p_k \otimes 1,$$

$$p_1 \otimes 1 + \ldots + p_n \otimes 1 = 1_{M \odot N}.$$

Por tanto, según proposición 4.8, $M \otimes_A N$ es la suma directa de los submódulos $\operatorname{Im}(p_k \otimes 1)$. Probaremos ahora que

$$\operatorname{Im}(p_k \otimes 1) \cong M_k \otimes N.$$

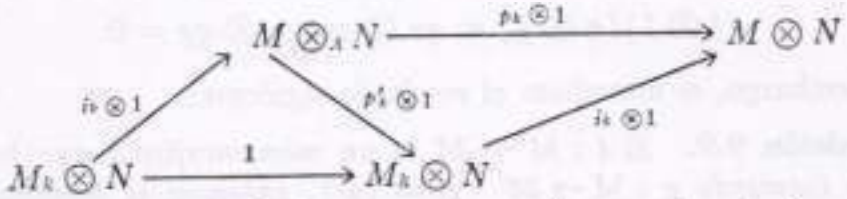
Para eso, consideremos la factorización de p_k



en donde i_k y p'_k están definidas de la manera natural. Se tendrá, entonces, ya que $p_k p_k = p_k$, que la composición

$$M_k \xrightarrow{i_k} M \xrightarrow{p'_k} M_k$$

es la identidad en M_k, por lo cual, el siguiente diagrama es conmutativo



Verificaremos que $(i_k \otimes 1)$ es un isomorfismo sobre la imagen de $p_k \otimes 1$. Ya que $(p'_k \otimes 1)(i_k \otimes 1) = 1$, $i_k \otimes 1$ es inyectivo, $p'_k \otimes 1$ es suprayectivo y, por tanto, $\mathrm{Im}(i_k \otimes 1) = \mathrm{Im}(p_k \otimes 1)$.

Corolario 9.7. *Si* V *y* V′ *son espacios vectoriales sobre* K *de dimensión* m *y* m′ *respectivamente, entonces la dimensión de* $V \otimes_K V'$ *es* mm′.

Proposición 9.8. *Si la sucesión de* A*-homomorfismos*

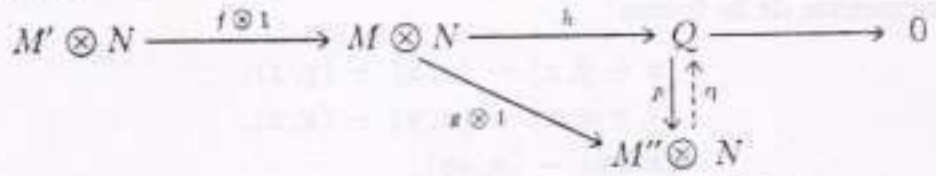
$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

es exacta y N *es un* A*-módulo, entonces la sucesión*

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0$$

es exacta.

Demostración. Si Q es el A-módulo cociente de $M \otimes N$ con respecto a la imagen de $f \otimes 1$ y h, el homomorfismo canónico se tiene el diagrama



con la sucesión superior exacta. Ya que $(g \otimes 1)(f \otimes 1) = 0$, existe un A-homomorfismo p tal que $ph = g \otimes 1$. Probaremos que p es un isomorfismo. Sea $(x'', y) \in M'' \times N$ y $x \in M$ tal que $g(x) = x''$. La

aplicación $q' : M'' \times N \to Q$ dada por $q'(x'', y) = h(x \otimes y)$ está bien definida y es bilineal y, por tanto, define un A-homomorfismo $q : M'' \otimes N \to Q$ tal que $q(x'' \otimes y) = h(x \otimes y)$. Se comprueba fácilmente que las composiciones pq y qp son la identidad.

Obsérvese que $i \otimes 1 : M'' \otimes N \to M \otimes N$ no es monomorfismo en general. Por ejemplo, si $f : \mathbf{Z} \to \mathbf{Z}$ es el monomorfismo dado por $f(n) = qn$ (q un entero positivo fijo) y G un grupo abeliano de orden q, el homomorfismo

$$f \otimes 1 : \mathbf{Z} \otimes_{\mathbf{Z}} G \to \mathbf{Z} \otimes_{\mathbf{Z}} G$$

es nulo. En efecto,

$$(f \otimes 1)(n \otimes g) = qn \otimes g = n \otimes qg = 0.$$

Sin embargo, es inmediato el resultado siguiente:

Proposición 9.9. *Si* $\mathrm{f} : \mathrm{M}' \to \mathrm{M}$ *es un monomorfismo que posee un inverso izquierdo* $\mathrm{g} : \mathrm{M} \to \mathrm{M}'$ ($\mathrm{gf} = 1_{\mathrm{M}'}$), *entonces el homomorfismo inducido* $\mathrm{f} \otimes 1 : \mathrm{M}' \otimes \mathrm{N} \to \mathrm{M} \otimes \mathrm{N}$ *es un monomorfismo (que posee inverso izquierdo).*

En particular, para espacios vectoriales, todo monomorfismo tiene inverso izquierdo y, por tanto, si

$$0 \to V' \to V \to V'' \to 0$$

es una sucesión exacta de espacios vectoriales sobre K y W es un espacio vectorial sobre K la sucesión inducida

$$0 \to V' \otimes_K W \to V \otimes_K W \to V'' \otimes_K W \to 0$$

es exacta.

Para finalizar la sección discutiremos en forma suscinta el concepto de producto tensorial para el caso no conmutativo.

Sea A un anillo con 1 (ahora no necesariamente conmutativo), M un A-módulo *derecho* y N un A-módulo *izquierdo*.

El producto tensorial $M \otimes_A N$ es el grupo abeliano cociente del grupo abeliano libre $L = \mathbf{Z}^{(M \times N)}$ con respecto al subgrupo R generado por los elementos de la forma

$$\begin{aligned} &(x + y, z) - (x, z) - (y, z), \\ &(x, y + z) - (x, y) - (x, z), \\ &(xa, y) - (x, ay). \end{aligned}$$

Se tiene la sucesión exacta de grupos abelianos

$$0 \to R \to L \to M \otimes_A N \to 0.$$

La composición φ: $M \times N \to L \to M \otimes_A N$ se llama aplicación canónica denotada por $\varphi(x, y) = x \otimes y$ y es una aplicación bilineal, es decir,

$$(x + x') \otimes y = x \otimes y + x' \otimes y$$
$$x \otimes (y + y') = x \otimes y + x \otimes y'.$$

Además, φ tiene la propiedad

$$xa \otimes y = x \otimes ay.$$

En caso de que el anillo sea conmutativo, al dotar al grupo abeliano $M \otimes_A N$ con la operación

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

este módulo coincide con el definido al principio de la sección.

Es evidente cómo muchas de las propiedades demostradas para el caso conmutativo pueden extenderse a este caso.

10. Matrices y transformaciones lineales

Sean K un campo y m, n dos enteros positivos. Denotaremos con $M(m \times n, K)$ al espacio vectorial sobre K cuyos elementos son las matrices de $m \times n$, es decir, las funciones

$$A : J_m \times J_n \to K$$

($J_m = \{1,2, \ldots, m\}$) con las operaciones ordinarias.

$$(A + B)(i, j) = A(i, j) + B(i, j),$$
$$(aA)(i, j) = aA(i, j),$$
$$(A, B \in M(m \times n, K), (i, j) \in J_m \times J_n, a \in K).$$

La multiplicación de matrices

$$(AB)(i, j) = \Sigma_k A(i, k)\, B(k, j)$$

define una aplicación bilineal de espacios vectoriales

$$M(k \times n, K) \times M(m \times k, K) \to M(m \times n, K),$$
$$(B, A) \mapsto AB.$$

En el caso particular en que $m = n$, $M(m \times m, K)$, denotado también $M(m, K)$ resulta ser, con la multiplicación mencionada, un álgebra sobre K.

A cada matriz $A \in M(n \times m, K)$ se le asocia una transformación lineal $U(A): K^m \to K^n$ (en donde, como de costumbre, $K^m =$

$K \oplus \ldots \oplus K$ es el espacio vectorial de dimensión m sobre K), dada por la fórmula usual

$$U(A)(x_1, \ldots, x_m) = (y_1, \ldots, y_n)$$

con

$$y_i = \Sigma_{j=1}^{m} A(i,j) x_j \quad (1 \leq i \leq n). \tag{1}$$

Recíprocamente, si V y V' son dos espacios vectoriales sobre K con bases $B = (b_1, \ldots, b_m)$ y $B' = (b'_1, \ldots, b'_n)$ respectivamente. Entonces a cada transformación lineal $f \in \mathrm{Hom}_K(V, V')$ se le asocia una matriz $A = F(f) \in M(n \times m, K)$ dada, como de costumbre, por

$$f(b_j) = \Sigma_{i=1}^{n} A(i,j) b'_i \quad (1 \leq j \leq m). \tag{2}$$

Lema 10.1. *Sean* $\mathrm{V}, \mathrm{V}', \mathrm{V}''$ *espacios vectoriales sobre* K *de dimensiones* m, n, q *respectivamente. Sean* $\mathrm{B} = (\mathrm{b}_1, \ldots, \mathrm{b}_m)$, $\mathrm{B}' = (\mathrm{b}'_1, \ldots, \mathrm{b}'_n)$, $\mathrm{B}'' = (\mathrm{b}''_1, \ldots, \mathrm{b}''_q)$ *bases de* $\mathrm{V}, \mathrm{V}', \mathrm{V}''$. *Si* $\mathrm{f} : \mathrm{V} \to \mathrm{V}'$ *y* $\mathrm{g} : \mathrm{V}' \to \mathrm{V}''$ *son transformaciones lineales y* F(f), F(g), F(gf) *son matrices asociadas a las transformaciones respectivas, entonces*

$$F(gf) = F(g)\,F(f).$$

Demostración.

$$(gf)(b_j) = g(f(b_j)) = g(\Sigma_{i=1}^{n} F(f)(i,j)\, b'_i) =$$
$$= \Sigma_{i=1}^{n} F(f)(i,j)\, g(b'_i) = \Sigma_{j=1}^{n} \Sigma_{k=1}^{q} F(f)(i,j)\, F(g)(k,i)\, b''_k =$$
$$= \Sigma_{k=1}^{q} (F(g)\,F(f))(k,j)\, b''_k = \Sigma_{k=1}^{q} F(gf)(k,j)\, b''_k.$$

Tenemos entonces dos aplicaciones

$$U : M(n \times m, K) \to \mathrm{Hom}_K(V, V')$$
$$F : \mathrm{Hom}_K(V, V') \to M(n \times m, K)$$

que son transformaciones lineales de espacios vectoriales sobre K.

Se comprueba directamente que estas aplicaciones son inversas la una de la otra, es decir, si $A \in M(n \times m, K)$, $FU(A) = A$ y si $f \in \mathrm{Hom}(K^m, K^n)$, se pueden elegir bases de V y V' de manera que $UF(f) = f$.

De lo anterior y el lema 10.1 se sigue la

Proposición 10.2. *Las transformaciones lineales*

$$U : M(n, K) \to \mathrm{End}_K(V) \qquad (n = \dim V)$$
$$F : \mathrm{End}_K(V) \to M(n, K)$$

son isomorfismos de K*-álgebras.*

Para finalizar esta sección daremos la definición de producto de Kronecker de matrices y su relación con el producto tensorial de transformaciones lineales.

Si f y g son transformaciones lineales entre espacios vectoriales con matrices A y B asociadas a cierta elección de bases, entonces al producto tensorial $f \otimes g$ se le puede asociar, eligiendo convenientemente la base, una matriz $A \otimes B$ llamada producto de Kronecker de las matrices A y B. Más precisamente:

Definición 10.3. *Si* A *y* A′ *son matrices de* n × m *y* n′ × m′ *respectivamente, entonces el producto de Kronecker* A ⊗ A′ *es la matriz de* nn′ × mm′ *definida por*

$$A \otimes A'((h\text{-}1)n + i, (k\text{-}1)\, m + j) = A(i, j)\, A'(h, k),$$

con $1 \leq \mathrm{i} \leq \mathrm{n}$, $1 \leq j \leq m$, $1 \leq h \leq n'$, $1 \leq \mathrm{k} \leq \mathrm{m}'$.

Gráficamente, $A \otimes A'$ es la matriz de bloques

$$A \otimes A' = \begin{pmatrix} A_{11} & \dots & A_{1m'} \\ \dots & \dots & \dots \\ A_{n'1} & \dots & A_{n'm'} \end{pmatrix}$$

en donde cada bloque es la matriz de $n \times m$ dada por

$$A_{hk} = A'(h, k)\, A.$$

Dicho de otra manera, $A \otimes A'$ es la matriz que se obtiene sustituyendo cada elemento de la matriz A' por la matriz que se obtiene multiplicando dicho elemento por la matriz A.

Sean $f : V \to W$, $g : V' \to W'$ y $f \otimes g : V \otimes_K V' \to W \otimes_K W'$ transformaciones lineales de espacios vectoriales sobre K y supongamos que

$$\begin{aligned} B &= (b_1, \dots, b_m) \text{ es una base de } V, \\ B' &= (b'_1, \dots, b'_{m'}) \text{ es una base de } V' \\ C &= (c_1, \dots, c_n) \text{ es una base de } W, \\ C' &= (c'_1, \dots, c'_n) \text{ es una base de } W', \end{aligned}$$

entonces las familias

$$\begin{aligned} B'' &= (b''_1, \dots, b''_{mm'}), \\ C'' &= (c''_1, \dots, c''_{nn'}) \end{aligned}$$

definidas por

$$\begin{aligned} b''_{(h-1)m+j} &= b_j \otimes \\ c''_{(h-1)n+i} &= c_i \otimes c'_h \end{aligned}$$

con $1 \leq i \leq n$, $1 \leq j \leq m$, $1 \leq h \leq n'$, $1 \leq k \leq m'$ son bases de $V \otimes_K V'$ y $W \otimes_K W'$ respectivamente. Esto es consecuencia de 10.2 ya que, evidentemente, son familias de generadores en número correcto.

Proposición 10.4. *Si* A *es la matriz de la transformación lineal* $f : V \to W$ *asociada a las bases* B, C, *y* A′ *es la matriz asociada a la transformación lineal* $g: V' \to W'$ *con respecto a las bases* B′, C′, *entonces la matriz asociada a la transformación lineal* $f \otimes g$ *con respecto a las bases* B″, C″ *es el producto de Kronecker* $A \otimes A'$ *de las matrices* A *y* A′.

Demostración. Como se recuerda, la matriz asociada a $f \otimes g$ con respecto a las bases B'', C'' se obtiene [sección 10, fórmula (2)] como sigue:

$$(f \otimes g)(b''_{(k-1)m+j}) = (f \otimes g)(b_j \otimes b'_k) =$$

$$= \sum_{i=1}^{n} A(i,j)\, c_i \otimes \sum_{h=1}^{n'} A'(h,k)\, c'_h =$$

$$= \sum_{i=1}^{n} \sum_{h=1}^{n'} A(i,j)\, A'(h,k)\, c_i \otimes c'_h =$$

$$= \sum A''\,((h\text{-}1)n + i,\, (k\text{-}1)m + j)\, c''_{(h-1)n+i}$$

Por tanto,

$$A''((h\text{-}1)n + i,\, (k\text{-}1)\, m + j) = A(i,j)\, A'(h,k),$$

de donde $A'' = A \otimes A'$.

CAPITULO 2

Representaciones de un grupo finito

1. Representaciones

Sea G un grupo finito y K un campo. Designaremos con $GL_K(V)$ al grupo de las unidades del anillo $\mathrm{End}_K(V)$ de todos los endomorfismos de un espacio vectorial V de dimensión finita n sobre K.

Definición 1.1. *Una representación de* G *por endomorfismos del espacio vectorial* V *es un homomorfismo*

$$R : G \to GL_K(V).$$

V *se llama el espacio de la representación y se dice que* n *es el grado de la representación.*

Si R *es un monomorfismo se dice que la representación es fiel.*

EJEMPLOS

a) El homomorfismo dado por $R(g) = 1$ para toda g de G se llama *representación trivial.*

b) Sea G un grupo cíclico de orden n y g un generador de G. El grupo multiplicativo $\mathbf{C}^*$ del campo $\mathbf{C}$ de los números complejos es el grupo de las unidades del anillo de los endomorfismos de $\mathbf{C}$ considerado como espacio vectorial de dimensión uno sobre $K = \mathbf{C}$.

Si z es una raíz n-ésima de la unidad, entonces el homomorfismo

$$R : G \to \mathbf{C}^*$$

dado por $R(g^k) = z^k$ es una representación de grado 1 de G. Esta representación es fiel si y sólo si z es una raíz primitiva de la unidad.

Recíprocamente, si R es una representación de G en $\mathbf{C}^*$ entonces $R(g)$ es una raíz n-ésima de la unidad, por lo cual, la correspondencia que asocia a cada R el elemento $R(g) \in \mathbf{C}^*$ es una biyección entre el conjunto de todas las representaciones de grado uno de G en $\mathbf{C}^*$ y el conjunto de las raíces n-ésimas de la unidad.

c) Si G es un subgrupo del grupo lineal $GL_K(V)$ entonces la inclusión $R: G \to GL_K(V)$ es una representación fiel de G por endomorfismos de V.

d) Sea $I = \{1, 2, \ldots, n\}$ y $B: I \to V$ una base del espacio vectorial V de dimensión n sobre K (sección 5, capítulo 1).

Sea G un subgrupo del grupo de las permutaciones del conjunto I. La aplicación dada por

$$R(g)(b_i) = b_{g(i)}$$

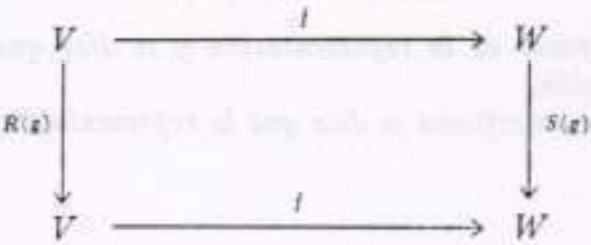
$(b \in G,\ b_i = B(i))$ define una representación fiel

$$R : G \to GL_K(V)$$

de G con espacio de representación V.

Obsérvese que esto permite considerar a todo grupo como subgrupo de un grupo lineal.

Definición 1.2. *Dos representaciones* R *y* S *de un grupo* G *con espacios de representación* V *y* W *se llaman equivalentes si existe un isomorfismo* $f: V \to W$ *tal que para cada* $g \in G$ *el diagrama*



sea conmutativo (V y W son espacios vectoriales sobre el mismo campo K).

Sea $GL(n, K)$ el grupo de las unidades del álgebra $M(n, K)$ de las matrices cuadradas de orden n con elementos en el campo K.

Definición 1.3. *Una representación del grupo* G *por matrices de orden* n, *sobre* K, *es un homomorfismo*

$$R : G \to GL(n, K)$$

Definición 1.4. *Dos representaciones* R *y* S *de un grupo* G *por matrices de orden* n *sobre el campo* K, *son equivalentes si existe una matriz* A *en* GL (n, K) *tal que para toda* g *en* G *se tenga*

$$R(g) = A^{-1} S(g) A$$

Obsérvese que dos representaciones de grado uno son equivalentes si y solamente si son iguales, pues en este caso el grupo de endomorfismos es conmutativo.

EJEMPLOS

e) A la representación del ejemplo *(d)* le corresponde, por medio de la misma base B, la representación matricial

$$R : G \to GL(n, K)$$

siguiente:

$$(R(g))(i, j) = E(g^{-1}(i), j) = \begin{cases} 1 & \text{si } i = g(j) \\ 0 & \text{si } i \neq g(j), \end{cases}$$

es decir, $R(g)$ es la matriz que se obtiene de la matriz idéntica E aplicando a sus renglones la permutación g^{-1}.

f) Sea G un grupo cíclico de orden 3 y g un generador de G. Si a g le asociamos

$$R(g) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

obtenemos una representación de grado 3 de G. Si a g le asociamos

$$S(g) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$$

en donde ω es una raíz cúbica primitiva de la unidad, obtenemos otra representación de grado 3 de G (sobre $K = \mathbf{C}$, por ejemplo). Estas dos representaciones son equivalentes puesto que

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}^{-1}$$

(La matriz

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_1 & \omega_1^2 \\ 1 & \omega_2 & \omega_2^2 \end{pmatrix}$$

es no singular, pues su determinante es de Van der Monde, con 1, ω_1, ω_2 las raíces cúbicas de la unidad.)

g) El ejemplo anterior se generaliza fácilmente a un grupo cíclico G de orden n, si a su generador g le asociamos las matrices

$$R(g) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

$$S(g) = \begin{pmatrix} z_1 & 0 & \dots & 0 \\ 0 & z_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & z_n \end{pmatrix}$$

en donde $z_1, z_2, \dots, z_n$ son las raíces n-ésimas de la unidad. La equivalencia se encuentra usando la matriz de Van der Monde.

$$\begin{pmatrix} 1 & z_1 & z_1^2 & \dots & z_1^{n-1} \\ 1 & z_2 & z_2^2 & \dots & z_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & z_n & z_n^2 & \dots & z_n^{n-1} \end{pmatrix}$$

EJERCICIO

Pruebe que si G es un grupo cíclico de orden 3, g un generador de G, A una matriz de 3×3 sobre los complejos, tal que $A^3 = 1$, entonces la representación $R: G \to GL(3, \mathbf{C})$ definida por $R(g) = A$ es equivalente a una del tipo

$$S(g) = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$$

en donde $a, b, c \in \{1, \omega, \omega^2\}$.

2. Suma y producto de representaciones matriciales

Se definirán a continuación las operaciones de suma y producto de representaciones de un grupo finito G por matrices sobre el campo K.

Sean

$$R: G \to GL(m, K)$$
$$S: G \to GL(n, K)$$

dos representaciones. Su suma

$$R \oplus S: G \to GL(m+n, K)$$

se define mediante la relación

$$(R \oplus S)\,(g)\,(i,j) = \begin{cases} R(g)\,(i,j) & \text{si} \quad 1 \leq i, j \leq m \\ S(g)\,(i,j) & \text{si} \quad m+1 \leq i, j \leq m+n \\ 0 & \text{en los casos restantes;} \end{cases}$$

o sea

$$(R \oplus S)\,(g) = \begin{bmatrix} R(g) & 0 \\ 0 & S(g) \end{bmatrix}.$$

El producto $R \otimes S$ se define como la representación

$$R \otimes S: G \to GL\,(mn, K)$$

cuya matriz $(R \otimes S)\,(g)$ es el producto de Kronecker de las matrices $R(g)$ y $S(g)$

$$(R \otimes S)(g) = R(g) \otimes S(g).$$

Explícitamente si $1 \leq \alpha, \beta \leq mn$, se puede escribir en forma única

$$\alpha = hm + i, \qquad 0 \leq h,\ k \leq n-1,$$
$$\beta = km + j, \qquad 1 \leq i,\ j \leq m,$$

y entonces se tiene que

$$(R(g) \otimes S(g))\,(\alpha, \beta) = R(g)\,(i,j)\ S(g)\,(h+1, k+1).$$

En otras palabras,

$$R(g) \otimes S(g) = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{bmatrix}$$

siendo $A_{hk} = S(g)\,(h,k)\ R(g)$.

Desde luego, debe comprobarse que $(R \oplus S)(g)$ y $(R \otimes S)(g)$ están en los grupos lineales correspondientes, es decir, que estas matrices son no singulares. Para ello se usarán las dos fórmulas básicas:

$$(A \oplus B)(C \oplus D) = AC \oplus BD,$$
$$(A \otimes B)(C \otimes D) = AC \otimes BD,$$

en donde $A, C \in M(m, K)$, $B, D \in M(n, K)$.

Éstas son consecuencias de las definiciones de suma y producto tensorial del homomorfismos (véase la proposición 9.9, capítulo 1). Sin embargo, daremos demostraciones directas.

$$(A \oplus B)(C \oplus D)(i,j) = \sum_{k=1}^{m+n} (A \oplus B)(i,k)(A \oplus B)(k,j) =$$

$$= \begin{cases} \sum\limits_k A(i,k)\, C(k,j) & 1 \le i,j,k \le m \\ 0 & 1 \le i,j \le m,\ m \le k-1 \\ \sum\limits_k B(i,k)\, C(k,j) & m+1 \le i,j,k \le m+n \\ 0 & m+1 \le i,j \le m+n,\ k \le m \\ 0 & \text{en los demás casos} \end{cases}$$

$$= \begin{cases} AC(i,j) & 1 \le i,j \le m \\ BD(i,j) & m+1 \le i,j \le m+n \\ 0 & \text{en los casos restantes} \end{cases}$$

$= (AC \oplus BD)(i,j)$, lo cual prueba la primera fórmula.

Para demostrar la segunda, sean α, β como antes. Entonces

$$(A \otimes B)(C \otimes D)(\alpha, \beta) =$$
$$= \sum (A \otimes B)(\alpha, (s-1)m + r)(C \otimes D)((s-1)m + r, \beta)$$
$$(1 \le (s-1)m + r \le mn,\ 1 \le s,\ r \le n)$$
$$= \sum_{r,s} A(i,r)\, B(h+1,s)\, C(r,j)\, D(s+1, k+1)$$
$$= (AC)(i,j)(BD)(h+1, k+1)$$
$$= ((AC) \otimes (BD))(\alpha, \beta), \text{ lo cual prueba la segunda.}$$

Es inmediato que si I_n denota la matriz unitaria de $n \times n$ se tiene

$$I_m \oplus I_n = I_{m+n}$$
$$I_m \otimes I_n = I_{mn}.$$

Por tanto, si A y B son matrices invertibles, $A \oplus B$ y $A \otimes B$ lo son también, pues

$$(A \oplus B)(A^{-1} \oplus B^{-1}) = I_m \oplus I_n = I_{m+n}$$
$$(A \otimes B)(A^{-1} \otimes B^{-1}) = I_m \otimes I_n = I_{mn}$$

y los inversos son, respectivamente, $A^{-1} \oplus B^{-1}$ y $A^{-1} \otimes B^{-1}$.

Con esto queda probado que $R \oplus S$ y $R \otimes S$ son efectivamente representaciones.

Las dos operaciones que acabamos de definir son compatibles con la relación de equivalencia de representaciones. En efecto, si R y R' son representaciones equivalentes y S y S' también, para toda g de G se tiene

$$R'(g) = A\,R(g)A^{-1}, \qquad S'(g) = B\,S(g)B^{-1},$$

con A, B matrices invertibles. Entonces,

$$R'(g) \oplus S'(g) = (A\,R(g)\,A^{-1}) \oplus (B\,S(g)\,B^{-1}) = \\ = (A \oplus B)(R(g) \oplus S(g))(A \oplus B)^{-1}$$

Por tanto, $R \oplus S$ y $R' \oplus S'$ son equivalentes. Para el producto, la demostración es la misma.

En el conjunto de clases de equivalencia de representaciones de G por matrices, las operaciones definidas tienen las siguientes propiedades:

La suma es asociativa y conmutativa, hay unitario para el producto, éste es asociativo y las dos leyes distributivas del producto sobre la suma son válidas.

La asociatividad es válida para la suma de representaciones. La conmutatividad resulta de la fórmula de "multiplicación por bloques"

$$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}^{-1} = \begin{pmatrix} B & 0 \\ 0 & A \end{pmatrix}.$$

El elemento unitario para la multiplicación es la representación dada por la matriz de 1×1, (1).

3. Algebra de un grupo finito

Extenderemos primero el concepto de módulo sobre un anillo al de módulo sobre un álgebra.

Sea K un anillo conmutativo (con 1); como se sabe, una K-álgebra consta de un anillo A (con 1) y una estructura de K-módulo en A con la condición adicional

$$t(ab) = (ta)b = a(tb) \qquad (t \in K,\ a, b \in A)$$

Dicho de otra manera, una K-álgebra consta de un anillo A y un homomorfismo de anillos (con 1) de K en el centro de A.

Definición 3.1. *Un* K-*módulo* M *se llama módulo izquierdo sobre* una K-*álgebra* A *si* M *es un* A-*módulo izquierdo y*

$$t(ax) = (ta)x = a(tx) \qquad (t \in K,\ a \in A,\ x \in M).$$

EJEMPLOS

a) Todo anillo A (con 1) es un álgebra sobre $\mathbf{Z}$.

b) Si V es un espacio vectorial sobre un campo K, $\mathrm{End}_K(V)$ es un álgebra sobre K.

c) $M(n, K)$ es un K-álgebra.

d) Si K es un subcampo de un campo L, L es un K-álgebra.

e) Las únicas álgebras (asociativas) con división sobre $\mathbf{R}$ son $\mathbf{R}$, $\mathbf{C}$ y los cuaternios.

f) Todo módulo M sobre un anillo A es un módulo sobre el anillo $\mathbf{Z}$ de los enteros y un módulo sobre la $\mathbf{Z}$-álgebra A.

g) Un espacio vectorial V sobre un campo K es un módulo sobre la K-álgebra $\mathrm{End}_K(V)$.

h) Toda K-álgebra A es un módulo sobre la K-álgebra A.

Analizaremos ahora un tipo especial de álgebras asociadas a grupos finitos.

Definición 3.2. *El álgebra de un grupo finito* G *sobre un anillo conmutativo (con* 1) K, *denotada* KG *es la* K-*álgebra cuyos elementos son las aplicaciones*

$$u : G \to K$$

con las operaciones

$$(u + v)(g) = u(g) + v(g),$$
$$(u\,v)(g) = \sum_{g'g''=g} u(g')\,v(g''),$$
$$(tu)(g) = tu(g), \qquad (t \in K,\ u, v \in KG,\ g, g', g'' \in G).$$

Obsérvese que KG es, como K-módulo, el módulo libre con base G, denotado por K^G y definido en la sección 5 del capítulo 1.

Es muy frecuente la siguiente notación: los elementos de KG se escriben como "sumas formales"

$$u = t_1 g_1 + \ldots + t_n g_n$$

con $G = \{g_1, \ldots, g_n\}$, $t_i = u(g_i)$. Con esta notación las operaciones son

$$(t_1g_1 + \ldots + t_ng_n) + (s_1g_1 + \ldots + s_ng_n) = (t_1 + s_1)g_1 + \ldots + (t_n + s_n)g_n$$

$$t(t_1g_1 + \ldots + t_ng_n) = tt_1g_1 + \ldots + tt_ng_n$$

$$(t_1g_1 + \ldots + t_ng_n)(s_1g_1 + \ldots + s_ng_n) = \sum_{i,j} t_is_j\, g_ig_j.$$

OBSERVACIÓN

Si G y G' son grupos no isomorfos, las álgebras KG y KG' pueden ser isomorfas. Por ejemplo, si G es un grupo abeliano de orden n y $\mathbf{C}$ el campo de los números complejos, entonces

$$\mathbf{C}G = \mathbf{C} \times \cdots \times \mathbf{C}, \quad (n \text{ factores})$$

producto directo de campos. Es decir, en $\mathbf{C} \times \cdots \times \mathbf{C}$ las operaciones son

$$(z_1, \ldots, z_n) + (z'_1, \ldots, z'_n) = (z_1 + z'_1, \ldots, z_n + z'_n)$$
$$(z_1, \ldots, z_n) + (z'_1, \ldots, z'_n) = (z_1 z'_1, \ldots, z_n z_n)$$

(La demostración de este resultado se dará en el capítulo 4.) Por consiguiente, todos los grupos abelianos del mismo orden tienen álgebras de grupo, sobre los complejos, isomorfas.

4. Representaciones de un grupo y módulos sobre el álgebra del grupo

El propósito de esta sección es establecer la equivalencia entre los conceptos de representación de un grupo y de módulos sobre el álgebra de dicho grupo. Para ello, cuando se hable de un álgebra de grupo KG en lo sucesivo se entenderá el álgebra definida anteriormente junto con la inclusión $G \subset KG$.

Consideremos un A-módulo izquierdo M y el anillo $\mathrm{End}_{\mathbf{Z}}(M)$ de $\mathbf{Z}$-endomorfismos ($\mathbf{Z}$ anillo de los enteros) del grupo abeliano M. Si $a \in A$, la multiplicación por a

$$x \mapsto ax \qquad (x \in M)$$

es un $\mathbf{Z}$-endomorfismo de M que denotaremos por $L(a)$. Se tiene entonces una aplicación

$$L: A \to \mathrm{End}_{\mathbf{Z}}(M).$$

L resulta ser un homomorfismo de anillos (con 1):

$$L(a + b)(x) = (a + b)x = ax + bx = L(a)(x) + L(b)(x) = (L(a) + L(b))(x),$$

$$L(ab)(x) = abx = a(bx) = L(a)(bx) = L(a)(L(b)(x))$$
$$= (L(a)L(b))(x),$$
$$L(1)(x) = 1 \cdot x = x.$$

Recíprocamente, si M es un grupo abeliano y se tiene un homomorfismo de anillos (con 1)

$$L: A \to \mathrm{End}_{\mathbb{Z}}(M),$$

podemos definir una operación

$$A \times M \to M$$

mediante $(a, x) \mapsto L(a)(x)$ (denotada $(a, x) \mapsto ax$) con la cual M resulta un A-módulo. En efecto,

$$a(x + y) = L(a)(x + y) = L(a)(x) + L(a)(y) = ax + ay,$$
$$(a + b)x = L(a + b)(x) = (L(a) + L(b))(x) =$$
$$= L(a)(x) + L(b)(x) = ax + bx,$$
$$(ab)x = L(ab)(x) = (L(a)L(b))(x) =$$
$$= L(a)(L(b)(x)) = a(bx),$$
$$1x = L(1)(x) = x.$$

Lo anterior podemos resumirlo dando la siguiente definición de A-módulo, equivalente a la de la sección 1 del capítulo 1.

Definición 4.1. *Un* A*-módulo izquierdo* M *es un grupo abeliano* M *junto con un homomorfismo del anillo* A *en el anillo de los endomorfismos del grupo* M.

Consideremos ahora el caso en que el anillo A es un álgebra sobre un campo K y M un K-módulo que es también módulo sobre el álgebra A. Entonces la imagen del homomorfismo

$$L: A \to \mathrm{End}_{\mathbb{Z}}(M)$$

está contenida en la K-álgebra $\mathrm{End}_K(M) \subset \mathrm{End}_{\mathbb{Z}} M$ y

$$L: A \to \mathrm{End}_K(M)$$

es un homomorfismo de K-álgebras. Al homomorfismo L se le llama representación del álgebra A por endomorfismos de M.

Recíprocamente, si M es un espacio vectorial sobre K, A una K-álgebra y $L: A \to \mathrm{End}_K(M)$ un homomorfismo de K-álgebras, entonces L determina en M una estructura de módulo sobre la K-álgebra A.

Para demostrar estas dos últimas afirmaciones, basta comprobar que, en primer lugar, el homomorfismo L tiene la propiedad adicional

$$L(ta) = tL(a), \qquad (t \in K,\ a \in A)$$

y, en segundo lugar, que si L es homomorfismo de K-álgebras, entonces

$$t(ax) = a(tx), \qquad (t \in K,\ a \in A,\ x \in M).$$

Las comprobaciones son directas:

$$L(ta)(x) = (ta)x = t(ax) = (tL(a))(x),$$
$$t(ax) = t(L(a)(x)) = L(a)(tx) = a(tx).$$

Como antes, esto puede resumirse diciendo que:

Definición 4.2. *Un módulo izquierdo* M *sobre una* K*-álgebra* A *es un espacio vectorial* M *sobre* K *junto con un homomorfismo de* K*-álgebras* $\mathrm{L}:\mathrm{A} \to \mathrm{End}_{\mathrm{K}}(\mathrm{M})$.

Nota. Todo lo anterior es válido si en lugar de un campo K se toma un anillo conmutativo con 1.

Sea ahora G un grupo finito y KG su álgebra de grupo sobre el campo K.

Proposición 4.3. *Cada homomorfismo*

$$R:G \to U(A)$$

de G *en el grupo de las unidades* U(A) *de una* K*-álgebra* A *se puede extender, en forma única, a un homomorfismo de* K*-álgebras*

$$\overline{R}:KG \to A.$$

Demostración. Ya que G es una base de la K-álgebra KG, R tiene una extensión única a una transformación lineal de espacios vectoriales

$$\overline{R}:KG \to A.$$

Además, ya que $R(gg') = R(g)R(g')$ se verifica directamente que $\overline{R}(uv) = \overline{R}(u)\overline{R}(v)$, $(u, v \in KG)$.

Para el caso de representaciones se da la siguiente

Definición 4.4. *El álgebra envolvente de una representación* $\mathrm{R}:\mathrm{G} \to \mathrm{GL}_{\mathrm{K}}(\mathrm{V})$ *es la subálgebra* Im $\overline{\mathrm{R}}$, *en donde* $\overline{\mathrm{R}}:\mathrm{KG} \to \mathrm{End}_{\mathrm{K}}(\mathrm{V})$ *es la extensión del homomorfismo* R *mencionado en* 4.3.

Haremos corresponder ahora a cada representación de G una estructura de KG-módulo.

De acuerdo con la proposición 4.3, toda representación $R:G \to GL_K(V)$ puede extenderse a un homomorfismo de K-álgebras $\overline{R}:KG \to \mathrm{End}_K(V)$. Por consiguiente, de acuerdo con la nueva definición de módulos sobre K-álgebras, V resulta ser un módulo sobre la K-álgebra KG.

Recíprocamente, si se tiene una estructura de KG-módulo en un espacio vectorial V sobre K, nuevamente, por lo anterior, tendremos un homomorfismo de K-álgebras

$$\overline{R}:KG \to \mathrm{End}_K(V).$$

La restricción

$$R:G \to \mathrm{End}_K(V)$$

necesariamente tiene su imagen contenida en el grupo de las unidades, $GL_K(V)$ de $\mathrm{End}_K(V)$ y define, pues, una representación

$$R:G \to GL_K(V)$$

En otras palabras, el concepto de representación de un grupo G por endomorfismos coincide con el de módulo sobre el álgebra de grupo KG.

Resumiendo lo anterior y para uniformar el lenguaje usaremos las frases siguientes:

Si $R:G \to GL_K(V)$ es una representación de G,

"*el* KG-*módulo correspondiente a* R"

es el grupo abeliano V con la operación

$$gx = R(g)(x).$$

Si V es un KG-módulo,

"*la representación asociada a* V"

es

$$R:G \to GL_K(V)$$

dada por

$$R(g)(x) = gx.$$

Analizaremos ahora algunos conceptos relativos a representaciones desde el punto de vista de KG-módulos y recíprocamente.

Como en lo sucesivo se utilizarán representaciones matriciales, es conveniente hacer las siguientes convenciones:

Si $R: G \to GL_K(V)$ es una representación y $B = (b_1, \ldots, b_n)$ una base de V sobre K,

"la representación matricial asociada a R *con respecto a la base* B"

es

$$R: G \to GL(n, K)$$

definida por

$$R(g)(b_j) = \sum_{i=1}^{n} R(g)(i,j) b_i \quad (1 \leq j \leq n)$$

Las frases anteriormente definidas podrán combinarse y así hablar, por ejemplo, de *"la representación matricial asociada a un* KG*-módulo, con respecto a una base"*.

Proposición 4.5. *Dos representaciones de un grupo* G *por endomorfismos son equivalentes si y sólo si los* KG*-módulos correspondientes son isomorfos.*

Demostración. Sean

$$R: G \to GL_K(V),$$
$$R: G \to GL_K(W)$$

dos representaciones equivalentes. Existe entonces un isomorfismo de espacios vectoriales sobre K

$$\alpha: V \to W$$

tal que para todo elemento g de G el siguiente diagrama es conmutativo.

$$\begin{array}{ccc} V & \xrightarrow{\alpha} & W \\ {\scriptstyle R(g)}\downarrow & & \downarrow{\scriptstyle S(g)} \\ V & \xrightarrow[\alpha]{} & W \end{array}$$

De aquí se concluye que α es un KG-isomorfismo, pues si $u = \sum t_i g_i$ y $x \in V$,

$$\alpha(ux) = \alpha(\overline{R}(u)(x)) = \alpha(\sum t_i R(g_i)(x)) =$$
$$= \sum t_i \alpha(R(g_i)(x)) = \sum t_i S(g_i)(\alpha(x)) =$$

$$= \overline{S}(\sum t_i g_i)(\alpha(x)) = \overline{S}(u)(\alpha(x)) =$$
$$= u\,\alpha(x).$$

Recíprocamente, sea $\alpha: V \to W$ un isomorfismo de dos KG-módulos. La representación $R: G \to GL_K(V)$ asociada al KG-módulo V está definida por

$$R(g)(x) = gx, \quad (g \in G,\ x \in V)$$

y, análogamente, la asociada al KG-módulo W es

$$S(g)(y) = gy, \quad (g \in G,\ y \in W).$$

Pero, para todo elemento g de G

$$\alpha(gx) = g\alpha(x)$$

o, lo que es lo mismo, el diagrama

$$\begin{array}{ccc} V & \xrightarrow{\alpha} & W \\ {\scriptstyle R(g)}\downarrow & & \downarrow{\scriptstyle S(g)} \\ V & \xrightarrow{\alpha} & W \end{array}$$

es conmutativo para toda g y como α es evidentemente un isomorfismo de espacios vectoriales sobre K, las representaciones R y S son equivalentes.

Definición 4.6. *La suma* $\mathrm{R} \oplus \mathrm{S}$ *de las representaciones*

$$R: G \to GL_K(V),$$
$$S: G \to GL_K(W),$$

es la representación asociada al KG*-módulo* $\mathrm{V} \oplus \mathrm{W}$, *suma directa de los* KG*-módulos* V *y* W *correspondientes a las representaciones* R *y* S *respectivamente.*

Dicho de otra manera, $R \oplus S$ es la representación

$$R \oplus S: G \to GL_K(\mathrm{V} \oplus W),$$
$$(R \oplus S)(g)(x, y) = (R(g)(x),\ S(g)(y)), \quad (g \in G,\ x \in V,\ y \in W).$$

Para definir en forma análoga el concepto de producto de representaciones necesitaremos un resultado preliminar:

Lema 4.7. *Si* V *y* W *son dos* KG*-módulos, entonces en* $\mathrm{V} \otimes_K \mathrm{W}$ *existe una estructura de* KG*-módulo, única, tal que*

$$g(x \otimes y) = gx \otimes gy, \quad (g \in G,\ x \in V,\ y \in W).$$

Demostración. Ya que la aplicación $(x, y) \mapsto gx \otimes gy$ es bilineal, se tiene una transformación lineal

$$L(g): V \otimes_K W \to V \otimes_K W$$

tal que

$$L(g)(x \otimes y) = gx \otimes gy.$$

Lo anterior define una función

$$L: G \to \mathrm{End}_K(V \otimes_K W)$$

dada por $g \mapsto L(g)$ que es, evidentemente, un homomorfismo de G en el grupo de las unidades de $\mathrm{End}_K(V \otimes_K W)$, por lo que, según la proposición 4.3, L se extiende a un homomorfismo de K-álgebras

$$L: KG \to \mathrm{End}_K(V \otimes_K W).$$

Esto determina una estructura de KG-módulo en $V \otimes_K W$, en la cual $g(x \otimes y) = gx \otimes gy$. Finalmente, si se tiene otra estructura de KG-módulo en $V \otimes_K W$

$$L': KG \to \mathrm{End}_K(V \otimes_K W)$$

tal que $L'(g)\ (x \otimes y) = gx \otimes gy$, L' coincide con L en G y, por tanto, según la misma proposición mencionada antes, $L' = L$.

Observación

La fórmula

$$u(x \otimes y) = ux \otimes uy \qquad (u \in KG)$$

no define una estructura de KG-módulo en $V \otimes_K W$, pues

$$(u + v)\ (x \otimes y) = (u + v)\, x \otimes (u + v)y =$$
$$ux \otimes uy + ux \otimes vy + vx \otimes uy + vx \otimes vy \neq$$
$$ux \otimes uy + vx \otimes vy$$

en general.

Definición 4.8. *El producto* R ⊗ S *de las representaciones*

$$R: G \to GL_K(V)$$
$$S: G \to GL_K(W)$$

es la representación asociada al KG*-módulo* V $\otimes_K$ W, *producto tensorial de los espacios vectoriales* V *y* W *con la estructura de* KG*-módulo determinada por*

$$g(x \otimes y) = gx \otimes gy, \quad (g \in G,\ x \in V,\ y \in W).$$

Estas dos definiciones de suma y producto de representaciones coinciden con las de suma y producto de representaciones matriciales de la sección 2 al interpretar estas últimas como representaciones por endomorfismos.

Definición 4.9. *Una representación de un grupo* G

$$R: G \to GL_K(V)$$

es irreducible si el KG*-módulo correspondiente es irreducible.*

Dicho en otras palabras, R es irreducible si para todo subespacio propio W de V existe g en G tal que $R(g)(W) \not\subset W$.

EJEMPLOS

a) Toda representación de grado 1 es irreducible.

b) Si $\mathbf{C}$ es el campo de los números complejos y G un grupo abeliano, una representación $R: G \to GL_C(V)$ es irreducible si y sólo si es de grado 1. Esto se demostrará en el capítulo 4.

El siguiente lema relaciona el álgebra de los KG-endomorfismos del módulo correspondiente a una representación con su álgebra envolvente.

Lema 4.10. *Si* $\mathrm{R}: \mathrm{G} \to \mathrm{GL}_K(\mathrm{V})$ *es una representación, entonces el conmutador del álgebra envolvente de* R *en* $\mathrm{End}_K(\mathrm{V})$ *coincide con el álgebra de los* KG*-endomorfismos del* KG*-módulo correspondiente a la representación* R.

Demostración. Sea f un elemento del conmutador, es decir, $fR(g) = R(g)f$ para toda $g \in G$. Entonces

$$f(gx) = f(R(g)(x)) = R(g)(f(x)) = gf(x),$$

de donde, f es un KG-endomorfismo. Recíprocamente, si f es un KG-endomorfismo, la misma fórmula prueba que $fR(g) = R(g)f$ para toda g de G.

Proposición 4.11. (Schur.) *El conmutador del álgebra envolvente de una representación irreducible es un álgebra con división.*

Demostración. Como V es un KG-módulo irreducible, todo KG-endomorfismo no nulo es isomorfismo. Por tanto, $\mathrm{End}_{KG}(V)$ es un álgebra con división, la cual, de acuerdo con el lema anterior, es igual al conmutador del álgebra envolvente de la representación.

5. Restricción de una representación y representaciones inducidas

En esta sección se discutirán algunas relaciones entre las representaciones de un grupo finito G y las de sus subgrupos.

Definición 5.1. *Si* H *es un subgrupo de* G *y*

$$R:G \to GL_K(V)$$

una representación de G, *la restricción de* R *a* H, *denotada* res(R) *es la representación de* H

$$H \xrightarrow{i} G \xrightarrow{R} GL_K(V),$$

en donde i *es el homomorfismo inclusión.*

Definición 5.2. *Si* H *es un subgrupo de* G *y*

$$S:H \to GL_K(V)$$

una representación de H, *la representación inducida en* G *por* S, *denotada* ind(S), *es la representación asociada al* KG-*módulo* $KG \otimes_{KH} V$.

Obsérvese que para trasladar estas definiciones al lenguaje de las representaciones matriciales en el primer caso, basta sustituir en la definición 5.1 $GL_K(V)$ por $GL(n, K)$. El segundo caso es algo más elaborado y la definición de la representación de G inducida por una representación $S:H \to GL(n, K)$ se dará en términos de una descomposición arbitraria de G en clases izquierdas

$$G = g_1 H \cup \ldots \cup g_r H, \qquad r = [G:H].$$

Será consecuencia de la equivalencia de las dos definiciones 5.2 y 5.3 que cualquier otra descomposición determina una representación equivalente.

Sea g un elemento de G y σ la permutación del conjunto $\{1, 2, \ldots, r\}$ determinada por la multiplicación

$$gg_j = g_{\sigma(j)} h_j, \qquad (h_j \in H,\ 1 \leq j \leq r).$$

Sea

$$S:H \to GL(n, K)$$

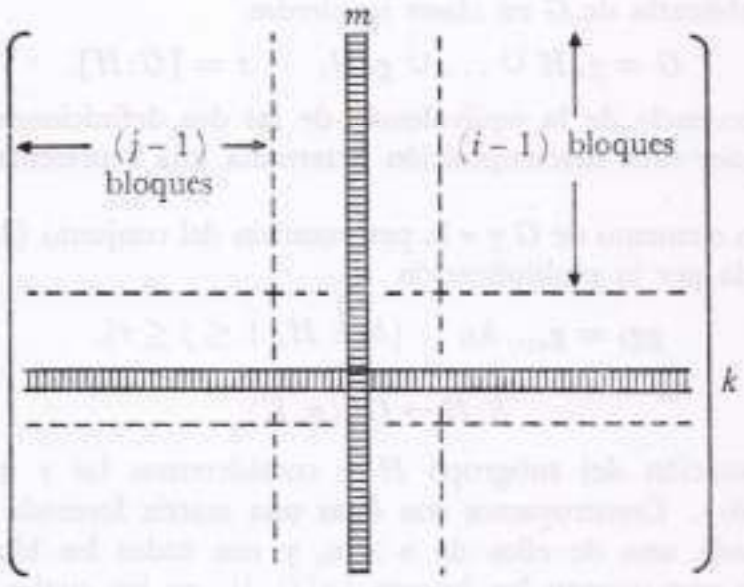
la representación del subgrupo H y consideremos las r matrices de $n \times n$, $S(h_j)$. Construyamos con éstas una matriz formada con $r \times r$ bloques, cada uno de ellos de $n \times n$, y con todos los bloques cero, excepto los que ocupan los lugares $(\sigma(j), j)$, en los cuales colocamos las matrices $S(h_j)$:

$$R(g) = \begin{array}{c} \begin{array}{ccc} & j & \end{array} \\ \left[\begin{array}{c:c:c} & 0 & \\ \hdashline 0 & S(h_j) & 0 \\ \hdashline & 0 & \end{array}\right] \end{array} \begin{array}{l} \\ \\ \left.\begin{array}{c} \\ \\ \end{array}\right\} \sigma(j) \\ \\ \end{array}$$

Escrita de otra manera, esta matriz es:

$$R(g)((i-1)\,n+k,\,(j-1)\,n+m) = \begin{cases} 0 \text{ si } i \neq \sigma(j) \\ S(h_j)(k,m) \text{ si } i = \sigma(j) \end{cases}$$

con $1 \leq i,\ j \leq r;\ 1 \leq k,\ m \leq n.$



Definición 5.3. *Si* H *es un subgrupo de índice* τ *del grupo* G *y*

$$S:H \to GL(n,K)$$

es una representación matricial de H, *la representación* $\mathrm{ind}(S) = R$ *inducida en* G *por* S *es la representación*

$$R:G \to GL(nr,K)$$

dada por

$$R(g)((i-1)\,n+k,(j-1)\,n+m) = \begin{cases} 0 \text{ si } i \neq \sigma(j) \\ S(h_j)(k,m) \text{ si } i = \sigma(j) \end{cases}$$

con $1 \leq i, j \leq r$; $1 \leq k, m \leq n$.

Para demostrar la equivalencia de las definiciones 5.2 y 5.3 de representación inducida usaremos el siguiente resultado:

Lema 5.4. *Si* $G = g_1H \cup \ldots \cup g_rH$ *es una partición de* G *en clases izquierdas, entonces la familia*

$$g_1 \otimes e_1, \ldots, g_1 \otimes e_n, \ldots, g_r \otimes e_1, \ldots, g_r \otimes e_n$$

es una base del espacio vectorial sobre K, $KG \otimes_{KH} K^n$.

Demostración. Sea Kg_iH el K-subespacio vectorial de KG generado por el conjunto g_iH $(1 \leq i \leq r)$. Entonces

$$KG = Kg_1H \oplus \ldots \oplus Kg_rH$$

es suma directa de espacios vectoriales sobre K. Pero Kg_iH es un KH-submódulo derecho de KG y, por tanto, la descomposición anterior es en suma directa de KH-submódulos derechos de KG. Por consiguiente (capítulo 1, sección 9)

$$KG \otimes_{KH} K^n \cong Kg_1H \otimes_{KH} K^n \oplus \ldots \oplus Kg_rH \otimes_{KH} K^n$$

y como, evidentemente, Kg_iH y KH son isomorfos como KH-módulos derechos, $Kg_iH \otimes_{KH} K^n \cong K^n$ (capítulo 1, sección 9), por lo cual

$$KG \otimes_{KH} K^n \cong K^n \oplus \ldots \oplus K^n, \ (r \text{ sumandos})$$

de donde, la dimensión, como espacio vectorial sobre K, es rn. Así pues, bastará probar que los rn elementos $g_i \otimes e_j$ generan a dicho espacio vectorial. En efecto, los elementos de la forma $g \otimes e_j$ generan a $KG \otimes_{KH} K^n$ sobre K y cada g se escribe en la forma $g = g_jh$ con $h \in H$. Entonces

$$g \otimes e_j = g_jh \otimes e_j = g_j \otimes he_j = g_j \otimes \sum t_k e_k = \sum t_k g_j \otimes e_k.$$

Proposición 5.5. *Si* $S:H \to GL(n,K)$ *es una representación de* H, *entonces la representación matricial de* G *asociada al* KG-*módulo* $KG \otimes_{KH} K^n$ *con respecto a la base*

$$b_{(i-1)n+k} = g_i \otimes e_k$$

es la representación inducida en G *por* S, *según la definición* 5.3.

Demostración. Basta ver que la matriz asociada a la transformación lineal

$$R(g)(u) = gu \qquad (u \in KG \otimes_{KH} K^n)$$

con respecto a la base mencionada es igual a la matriz de dicha definición. Se tiene, por un lado,

$$\begin{aligned} R(g)(b_{(j-1)n+m}) &= R(g)(g_j \otimes e_m) = gg_j \otimes e_m = \\ &= g_{\sigma(j)} h_j \otimes e_m = g_{\sigma(j)} \otimes h_j e_m = g_{\sigma(j)} \otimes S(\overline{h_j})(e_m) = \\ &= g_{\sigma(j)} \otimes \textstyle\sum_{k=1}^{n} S(h_j)(k,m)\, e_k = \\ &= \textstyle\sum_{k=1}^{n} S(h_j)(k,m)\, g_{\sigma(j)} \otimes e_k = \sum_{k=1}^{n} S(h_j)(k,m)\, b_{(\sigma(j)-1)n+k} \end{aligned}$$

Por otro lado,

$$\begin{aligned} &R(g)(b_{(j-1)n+m}) = \\ &= \textstyle\sum_{k=1}^{n} R(g)((i-1)\,n+k, (j-1)\,n+m)\, b_{(i-1)n+k} \end{aligned}$$

Igualando, obtenemos,

$$R(g)((i-1)\,n+k, (j-1)\,n+m) = \begin{cases} 0 \text{ si } i \neq \sigma(j) \\ S(h_j)(k,m) \text{ si } i = \sigma(j). \end{cases}$$

La interpretación de representaciones como KG-módulos permite dar una definición muy simple del concepto de representación regular.

Definición 5.6. *La representación asociada al* KG-*módulo (izquierdo)* KG *se llama la representación regular (izquierda) de* G.

Explícitamente, la representación regular de G es el homomorfismo

$$R: G \to GL_K(KG)$$

definido por $R(g)(g') = gg'$.

Evidentemente, la representación regular es fiel.

EJERCICIO

Descríbase la representación regular matricial. (Tómese como base a los elementos de G.)

CAPITULO 3

Módulos semisimples

1. Módulos semisimples

Definición 1.1. *Un* A*-módulo* M *se llama semisimple si* M *es suma directa de submódulos simples de* M.

Proposición 1.2. *Sea* M *un* A*-módulo. Las tres condiciones siguientes son equivalentes:*

1) M *es semisimple.*
2) M *es suma de submódulos simples.*
3) *Todo submódulo de* M *es sumando directo de* M.

Demostración. Desde luego (1) implica (2). Supongamos ahora que (2) es válida y sea

$M = \Sigma_{\alpha \in S} M_\alpha$ (M_α submódulo simple).

Sea M' un submódulo de M. Probaremos que M' es un sumando directo de M. Sea $\mathcal{L} = \{L \subset S | M' + \Sigma_{\alpha \in L} M_\alpha$ es una suma directa$\}$. La familia $\mathcal{L}$ es inductiva. Sea L_0 un máximo en $\mathcal{L}$ y

$$M' \oplus \bigoplus_{\alpha \in L_0} M_\alpha = M''.$$

Si $\beta \notin L_0$, $M_\beta \cap M'' \neq 0$, pues, de lo contrario, L_0 no sería máximo. Entonces, por ser M_β simple, $M_\beta \cap M'' = M_\beta$, es decir, $M_\beta \subset M''$. Por tanto, $M_\alpha \subset M''$ para toda $\alpha \in S$, de donde $M \subset M''$ y $M = M''$, o sea, M es suma directa de M' y otro submódulo de M. Finalmente, para probar que (3) implica (1) basta demostrar que todo submódulo

distinto de cero de M contiene un submódulo simple, ya que entonces la suma de todos los submódulos simples de M será un sumando directo y su complemento (como sumando directo) será forzosamente cero. Lo anterior es consecuencia de que todo submódulo contiene submódulos finitamente generados no nulos y éstos contienen submódulos máximos. Los complementos, como sumandos directos de estos máximos, son submódulos simples.

El siguiente resultado es inmediato:

Proposición 1.2. *Todo submódulo y todo módulo cociente de un módulo semisimple es semisimple. La suma directa de módulos semisimples es semisimple.*

Proposición 1.3. *Si* M *es un* A*-módulo semisimple y finitamente generable, entonces* M *es suma directa de un número finito de* A*-módulos simples. En particular,* M *es artiniano y noetheriano.*

Demostración. Sea $M = \sum_{\alpha \in L} M_\alpha$, M_α simples y $(u_1, \ldots, u_r)$ una familia de generadores de M. Entonces existe un subconjunto finito $L' \subset L$ tal que $u_i \in \sum_{\alpha \in L'} M_\alpha$ $(1 \leq i \leq r)$. Por consiguiente $M = \sum_{\alpha \in L'} M_\alpha$

Definición 1.4. *Se dice que un anillo* A *con* 1 *es semisimple si considerado como* A*-módulo izquierdo lo es.*

De lo anterior se sigue:

Proposición 1.5. *Los anillos semisimples son suma directa de un número finito de ideales mínimos izquierdos. En particular, son artinianos y noetherianos.*

Proposición 1.6. *Un anillo* A *es semisimple si y sólo si todo* A*-módulo es semisimple.*

Demostración. Si todo A-módulo es semisimple, A, en particular, es semisimple. Supongamos ahora que A es un anillo semisimple. Ya que la suma directa y el cociente de módulos semisimples es semisimple, basta observar que cualquier módulo M es el cociente de un A-módulo libre (véase la proposición 5.5 del capítulo 1).

Proposición 1.7. *Si* A *es un anillo semisimple, todo* A*-módulo simple* M *es isomorfo a un ideal izquierdo mínimo de* A.

Demostración. Sea $u \neq 0$ un elemento de M. Sea I el núcleo del A-homomorfismo suprayectivo $A \to M$ dado por $a \mapsto au$. Por ser A semisimple el ideal izquierdo I es un sumando directo de A. Existe entonces un ideal izquierdo J tal que $I \oplus J = A$, de donde, $J \cong A/I \cong M$. (J es mínimo por ser M simple.)

Corolario 1.8. *Todo módulo* M *sobre un anillo semisimple* A *es isomorfo a una suma directa de ideales izquierdos mínimos de* A. *En particular, si* M *es finitamente generado, es suma directa de un número finito de tales ideales.*

Proposición 1.9. *Si* A *es un anillo semisimple y* M *un* A*-módulo de tipo finito tal que*

$$M \cong A_1 \oplus \ldots \oplus A_r,$$

con A_i *ideal izquierdo mínimo de* A *y si* N *es un* A*-submódulo simple de* M, *entonces* N *es isomorfo a alguno de los* A_i.

En particular, dada una descomposición del anillo semisimple A en ideales izquierdos mínimos

$$A = A_1 \oplus \ldots \oplus A_r,$$

todo ideal izquierdo mínimo de A es isomorfo a uno de dichos ideales A_i.

Demostración. Ya que existe una descomposición de M en submódulos simples en la cual figura N, la proposición se sigue del teorema de Krull-Schmidt (teorema 8.7, capítulo 1).

Otra caracterización de los anillos semisimples se da la siguiente:

Proposición 1.10. *Una condición necesaria y suficiente para que un anillo* A *sea semisimple es que todo* A*-módulo sea proyectivo.*

Demostración. Supongamos primero que A es un anillo semisimple y sea M un A-módulo. Sabemos que M es cociente de un A-módulo libre L:

$$0 \to M' \to L \to M \to 0;$$

pero M' es sumando directo de L por ser A semisimple, es decir, $L = M' \oplus M''$ y entonces $M \cong M''$. Así pues, M resulta sumando directo de un módulo libre y, por consiguiente, M es proyectivo.

Inversamente, supongamos ahora que todo módulo sobre el anillo A es proyectivo. En particular, todo módulo cociente de A es un A-módulo proyectivo. Sea I un ideal izquierdo de A. Entonces la sucesión exacta

$$0 \to I \to A \to A/I \to 0$$

de A-módulos determinada por el homomorfismo canónico $A \to A/I$ se escinde (capítulo 1, proposición 5.6). Por tanto, I es sumando directo de A y A es un anillo semisimple.

2. Radical de un módulo

Definición 2.1. *El radical* R(M) *de un* A*-módulo* M *es la intersección de todos los submódulos máximos de* M.

En particular, si M no tiene submódulos máximos su radical es M. Si M es de tipo finito, entonces M tiene submódulos máximos (véase el capítulo 1, proposición 7.2) y el radical $R(M) \neq M$.

El radical $R(A)$ de un anillo A (con 1), es el radical de A considerado como A-módulo izquierdo.

Proposición 2.2. *El radical de un anillo es un ideal bilateral.*

Demostración. Sea $a \in R(A)$. Demostraremos primero que $a \in \text{an}(A/I)$ para todo ideal máximo I de A. [El anulador $\text{an}(M)$ de un A-módulo M es el ideal de A formado con todos los elementos $a \in A$ tales que $au = 0$ para toda $u \in M$.] Sea $u \in A/I$. Consideremos el A-homomorfismo $A \to A/I$ dado por $b \mapsto bu$ $(b \in A)$. El núcleo J de este homomorfismo es un ideal máximo J. Como $a \in R(A)$, $a \in J$, de donde $au = 0$, es decir, $a \in \text{an}(A/I)$. Supongamos ahora que c es un elemento arbitrario de A. Sea $\bar{c} \in A/I$ la clase de c módulo I. Por lo anterior $a\bar{c} = 0$, es decir $ac \in I$, de donde $ac \in R(A)$ con lo que queda probada la proposición.

Proposición 2.3. *Si* M *es un* A*-módulo, se tiene que*

$$R(A)M \subset R(M).$$

Demostración. Sea $a \in R(A)$, $u \in M$ y N un submódulo máximo de M. Si $u \in N$, $au \in N$; si $u \notin N$, sea $\bar{u} \in M/N$ la clase de u y consideremos el homomorfismo $\varphi: A \to M/N$ definido por $\varphi(b) = b\bar{u}$. φ es epimorfismo y su núcleo es un ideal máximo de J de A. Como $a \in R(A)$, $a \in J$ y entonces $a\bar{u} = 0$, es decir, $au \in N$. Por tanto, $au \in R(M)$.

Proposición 2.4. (Lema de Nakayama.) *Si* N *es un submódulo de un* A*-módulo* M *de tipo finito tal que*

$$N + IM = M,$$

con $\text{I} \subset \text{R(A)}$, *entonces* $\text{N} = \text{M}$.

Demostración. Si $N \neq M$, por ser M de tipo finito N está contenido en un submódulo máximo M' de M. Entonces $N + IM = M' + R(A)M = M$ y según la proposición anterior se tiene que $M' \supset R(A)M$, de donde $M' = M$ lo cual es una contradicción.

Proposición 2.5. *Todo ideal izquierdo de un anillo* A *que no esté contenido en el radical de* A *tiene elementos no nilpotentes.*

Demostración. Sea I un ideal izquierdo de A tal que $I \not\subset R(A)$. Existe entonces un ideal izquierdo máximo M tal que $I \not\subset M$. Entonces $I + M = A$ y $1 = a + b$, $a \in I$, $b \in M$. Se tiene que

$$ab = a(1 - a) = (1 - a)\, a = ba,$$

de donde, para toda n

$$1 = (a + b)^n = \sum \binom{n}{r} a^r b^{n-r}.$$

Si a fuera nilpotente, para alguna n, $a^n = 0$ y se tendría que $1 = cb \in M$, lo cual no es posible.

La proposición siguiente da otra caracterización de los anillos semisimples.

Proposición 2.6. *Un anillo es semisimple si y sólo si es artiniano y su radical es cero.*

Demostración. Supongamos primero que A es un anillo semisimple. La proposición 1.5 indica que A es artiniano. Para demostrar que su radical es cero, consideremos un elemento $a \neq 0$ de A. Como A es semisimple se tiene

$$A = A_1 \oplus \ldots \oplus A_n,$$

suma directa de ideales izquierdos mínimos. Entonces

$$a = a_1 + \ldots + a_n, \ (a_i \in A_i)$$

y podemos suponer $a_1 \neq 0$. Por tanto, $a \notin A_2 \oplus \ldots \oplus A_n$ que es un ideal máximo, de donde a no pertenece al radical de A.

Supongamos ahora que A es artiniano y sin radical. Demostraremos que todo ideal izquierdo I de A es un sumando directo de A. Consideremos el conjunto de ideales izquierdos L de A tales que $I + L = A$. El conjunto es no vacío ya que $I + A = A$. Sea L un mínimo de este conjunto. Bastará probar que $I \cap L = 0$. Supongamos, pues, $I \cap L \neq 0$ y sea I_0 un ideal izquierdo mínimo $(\neq 0)$ contenido en $I \cap L$. Ya que $R(A) = 0$, existe un ideal izquierdo máximo M tal que $I_0 \not\subset M$. Entonces $A = I_0 \oplus M$ y $L = I_0 \oplus M \cap L$. Sea $L' = M \cap L$. Entonces $L' \subset L$ y $L' \neq L$. Pero

$$A = I + L = I + I_0 + L' = I + L'$$

contra la hipótesis de que L es mínimo.

Corolario 2.7. *Si* A *es un anillo de Artin entonces* A/R(A) *es un anillo semisimple.*

Demostración. Se sigue de que

$$R(A/R(A)) = 0.$$

Un ideal izquierdo N de A se llama *nilpotente* si existe un entero positivo r tal que $N^r = 0$, es decir, si para cada familia $a_1, a_2, \ldots, a_r$ de elementos de N se tiene que $a_1 a_2 \ldots a_r = 0$.

En un ideal izquierdo nilpotente, todos los elementos son nilpotentes, pero no inversamente. Un ideal izquierdo en el que todos los elementos son nilpotentes se llama *nilideal*.

Si A no es conmutativo, no todo elemento nilpotente está contenido en un ideal izquierdo nilpotente.

Sea J el ideal izquierdo suma de todos los ideales nilpotentes izquierdos del anillo A.

Proposición 2.8. *Todo nilideal izquierdo de* A *está contenido en el radical* R(A) *de* A. *En particular*

$$J \subset R(A).$$

Este resultado es consecuencia de la proposición 2.5.

Proposición 2.9. *El radical de un anillo artiniano* A *es un ideal nilpotente.*

Demostración. Por ser A artiniano, si $R = R(A)$ se tiene

$$R \supset R^2 \supset \ldots \supset R^n = R^{n+1} = I.$$

Supongamos que R no es nilpotente. Entonces $I \neq 0$ e $I^2 = I$. Sea $\mathcal{L}$ el conjunto de todos los ideales izquierdos L de A tales que $IL \neq 0$ e $IL \subset I$; $\mathcal{L}$ no es vacío, pues $I \in \mathcal{L}$. Sea L un mínimo del conjunto $\mathcal{L}$. Como $IL \subset L$,

$$I\,I\,L = IL \neq 0,$$
$$I\,I\,L = IL \subset I$$

y por ser L mínimo en $\mathcal{L}$ se tiene que $IL = L$. Sea $ab \in IL$, $ab \neq 0$, $a \in I$, $b \in L$. Entonces

$$Ab \subset L,\ IAb \neq 0,\ IAb \subset IL \subset I$$

y, por consiguiente, $L = Ab$. Aplicando ahora el lema de Nakayama tenemos, de

$$L = 0 + IL = 0 + RL = L$$

que $L = 0$, lo cual es falso.

Corolario 2.10. *En un anillo de Artin el radical es la suma de todos los ideales izquierdos nilpotentes (o derechos).*

Resulta de las proposiciones 2.9. y 2.10.

Teorema 2.11. *Todo anillo artiniano es noetheriano.*

Demostración. Sea R el radical del anillo artiniano A. Consideremos la cadena

$$A = R^0 \supset R \supset R^2 \supset \ldots \supset R^n = 0.$$

Entonces los A-módulos R^i/R^{i+1} son también A/R-módulos $(0 \leq i \leq n-1)$ y sus A/R-submódulos coinciden con sus A-submódulos. Pero R^i/R^{i+1} es un A-módulo artiniano y, por lo anterior, es un A/R-módulo artiniano. Como A/R es semisimple (proposición 2.7) R_i/R_{i+1} es noetheriano como A/R-módulo y, por consiguiente, como A-módulo, de donde, de acuerdo con el teorema 7.7 del capítulo 1, R_i/R_{i+1} tendrá longitud finita como A-módulo. Aplicando ahora el corolario 7.10 del capítulo 1 se tiene el resultado deseado.

3. Anillos simples

Definición 3.1. *Un anillo artiniano se llama simple si no tiene ideales bilaterales propios.*

Un anillo simple A no siempre es un A-módulo simple. Más adelante se verán ejemplos de anillos simples que, considerados como módulos izquierdos no lo son.

Ya que el radical de un anillo es un ideal bilateral se tiene que

Proposición 3.2. *Todo anillo simple es semisimple.*

Para la discusión de las siguientes propiedades de los anillos semisimples nos será útil el resultado sobre descomposición en suma directa que damos a continuación.

Lema 3.3. *Si*

$$A = A_1 \oplus \ldots \oplus A_n$$

es una descomposición del anillo A *en suma directa de ideales izquierdos y*

$$1 = e_1 + \ldots + e_n, e_i \in A_i$$

entonces

$$e_i^2 = e_i,\ e_i e_j = 0 (i \neq j)\ \text{y}\ A_i = Ae_i.$$

Demostración. Veremos primero que $e_1 e_2 = 0$. En efecto

$$e_1(e_2 + \ldots + e_n) = e_1(1 - e_1) = (1 - e_1)e_1$$
$$\in A_1 \cap (A_2 + \ldots + A_n) = 0,$$

de donde

$$e_1 e_2 = -e_1(e_1 + \ldots + e_n) \in A_2 \cap (A_2 + \ldots + A_n) = 0.$$

En forma análoga, se ve que si $i \neq j$, $e_i e_j = 0$.

Entonces

$$1 = (e_1 + \ldots + e_n)^2 = e_1^2 + \ldots + e_n^2,$$

de donde $e_i = e_i^2$. Finalmente, si $a \in A_i$,

$$a = a\,1 = ae_1 + \ldots + ae_i + \ldots + ae_n$$

y por la unicidad de la descomposición se tiene que

$$a = ae_i.$$

Corolario 3.4. *En un anillo semisimple todo ideal izquierdo es principal y posee un generador idempotente.*

Demostración. Como todo ideal de A es sumando directo, el resultado se sigue del lema anterior.

Sean ahora I, I' dos ideales izquierdos de un anillo semisimple A. De acuerdo con el corolario anterior podemos escribir

$$I = A\,e,\ e^2 = e.$$

Consideremos la aplicación

$$G: eI' \to \mathrm{Hom}_A(I, I')$$

definida por la multiplicación a la derecha con elementos de eI', es decir,

$$G(ea')(a) = aea', \qquad a' \in I', a \in I.$$

$G(ea')$ es un homomorfismo de A-módulos. Con esta notación tenemos el siguiente resultado

Proposición 3.5. *La aplicación* G *es biyectiva y el diagrama*

$$\begin{array}{ccc} I \times eI' & \longrightarrow & I' \\ {\scriptstyle 1\times G}\downarrow & \nearrow & \\ I \times \mathrm{Hom}_A(I, I') & & \end{array}$$

es conmutativo.

Demostración. Que el diagrama sea conmutativo se sigue de las definiciones. Sean ea', $ea'' \in eI'$ $(a', a'' \in I')$ y supongamos que $G(ea') = G(ea'')$. Entonces para toda $a \in I$, $ae\,a' = ae\,a''$; en particular, si $a = e$ se tiene que $ea' = ea''$. Por tanto, G es inyectiva. Sea ahora $f: I \to I'$ un A-homomorfismo y $f(e) = a'$, $a' \in I'$. Entonces

$$f(ae) = af(e) = aa' = aea',$$

y, por tanto, G es suprayectiva.

De la proposición anterior resulta que II' es el ideal generado por $f(I)$ cuando f recorre $\mathrm{Hom}_A(I, I')$.

Corolario 3.6. *Si los ideales* I *e* I′ *son, además, mínimos, entonces* $\mathrm{II}' = \mathrm{I}'$ *si y solamente si* I *es isomorfo a* I′ *como* A*-módulos.*

Sea A un anillo semisimple y

$$A = I_{11} \oplus \ldots \oplus I_{1s_1} \oplus \ldots \oplus I_{t1} \oplus \ldots \oplus I_{ts_t}$$

una descomposición de A como suma directa de ideales izquierdos mínimos (véase el corolario 1.8) tal que

$$I_{ij} \cong I_{ik} \; ; \; I_{ij} \cong I_{hk} \quad (i \neq h)$$

(isomorfismos como A-módulo). Sean

$$A_1 = I_{11} \oplus \ldots \oplus I_{1s_1}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$A_t = I_{t1} \oplus \ldots \oplus I_{ts_t}.$$

Teorema 3.7. *Si* A *es un anillo semisimple y* $\mathrm{A}_1, \ldots, \mathrm{A}_t$ *son los ideales izquierdos de* A *arriba definidos se tiene:*

1) *Cada* A_i *es un ideal bilateral de* A.
2) *Cada* A_i *es un anillo simple.*
3) $\mathrm{A} = \mathrm{A}_1 \times \cdots \times \mathrm{A}_t$ (*producto directo de anillos*).

Demostración.

1) Para probar que A_i es bilateral basta ver que $A_i I_{jk} \subset A_i$ para todo I_{jk} de la descomposición. Pero según el corolario 3.6 se tiene entonces

$$A_i I_{ik} \subset A_i,$$
$$A_i I_{jk} = 0 \quad (i \neq j).$$

2) Observemos primero que cada A_i es un anillo con elemento unitario. En efecto, sea $1 = e_1 + \ldots + e_t$ $(e_i \in A_i)$. De acuerdo con el lema 3.3, $A_i = Ae_i$ y, también, por ser ideal derecho $A_i = e_i A$, de donde $A_i = e_i A e_i$ y e_i es, pues, el elemento unitario de A_i.

Ya que $A_i A_j \subset A_i \cap A_j$ por ser ideales bilaterales se tiene que $A_i A_j = 0$ si $i \neq j$. Por lo tanto, si I es un ideal izquierdo del anillo A_i entonces

$$AI = (A_1 \oplus \ldots \oplus A_t)\, I = A_i I \subset I,$$

es decir, I es un ideal izquierdo de A. Por tanto, el conjunto de ideales izquierdos del anillo A_i coincide con el conjunto de ideales izquierdos

de A contenidos en A_i. Esto implica, en particular, que los anillos A_i son artinianos.

Sea ahora I un ideal izquierdo propio de A_i. Ya que A_i es semisimple como A-módulo e I es un A-submódulo de A_i, por lo antes dicho,

$$A_i = I \oplus I'$$

con I' un ideal izquierdo propio de A_i. Sean I_0 e I'_0 ideales izquierdos mínimos de A contenidos en I e I' respectivamente. Ya que todos los ideales izquierdos mínimos de A_i son isomorfos (véase la proposición 1.9), según el corolario 3.4, $I_0 I'_0 = I'_0 \subset I$, por lo cual I no es un ideal bilateral de A_i y A_i resulta un anillo simple.

3) Por construcción, $A = A_1 \oplus \ldots \oplus A_t$, suma directa de A-módulos. Para probar que esta descomposición es un producto directo de anillos, $A = A_1 \times \ldots \times A_t$ basta ver que si $a = a_1 + \ldots + a_t$, $b = b_1 + \cdots + b_t$ $(a_i, b_i \in A_i)$ entonces $ab = a_1 b_1 + \cdots + a_t b_t$. Pero esto es consecuencia de que si $i \neq j$, $A_i A_j = 0$.

Corolario 3.8. *Un anillo es simple si y solamente si* A *tiene una descomposición en suma directa de ideales izquierdos mínimos en la cual todos ellos sean isomorfos entre sí* (como A-módulos).

Demostración. Supongamos que en alguna descomposición de A en ideales izquierdos mínimos hay ideales no isomorfos. Entonces, en cualquier descomposición tal ocurre lo mismo y, según la proposición anterior, existen ideales bilaterales propios de A, por lo cual A no es simple. La otra parte del corolario es consecuencia inmediata de la misma proposición, ya que A es semisimple de acuerdo con 3.7.

Observación

Es esencial que el isomorfismo mencionado en el corolario anterior sea de A-módulos como se observa en el ejemplo siguiente. Sea K un campo y $A = K \times K$ producto directo de anillos. A es un anillo semisimple, pero no simple, ya que evidentemente tiene ideales bilaterales propios. En la descomposición de A en ideales mínimos $A = K_1 \times K_2$, en donde

$$K_1 = \{(x, 0) \mid x \in K\},$$
$$K_2 = \{(0, y) \mid y \in K\},$$

K_1 es isomorfo a K_2 $(\cong K)$ como anillos, pero el ideal K_1 no es isomorfo al ideal K_2.

Corolario 3.9. *Un anillo es semisimple si y solamente si es producto directo de anillos simples en número finito.*

Demostración. En un sentido está probado en la última proposición. Ahora, si $A = A_1 \times \ldots \times A_t$ es un producto directo de anillos simples, cada A_i es semisimple por ser simple, de donde, es suma directa de ideales izquierdos mínimos de A_i. Pero éstos son también ideales izquierdos mínimos de A.

En el caso de que el anillo semisimple sea conmutativo se desprende del corolario anterior el siguiente resultado.

Proposición 3.10. *Un anillo conmutativo es simple si y sólo si es un campo y es semisimple si y sólo si es producto directo de un número finito de campos.*

4. Estructura de los anillos simples

Como se indica en el título, en esta sección se analizará la estructura de los anillos simples. Primero se demostrará que el anillo de los endomorfismos de un espacio vectorial sobre un anillo con división es simple. Después se demostrará un teorema de Wedderburn, el cual asegura que todo anillo simple es de esta forma.

Observemos primero que la teoría desarrollada en el capítulo 1 para espacios vectoriales se puede extender a módulos sobre anillos con división, que también llamaremos espacios vectoriales.

Teorema 4.1. *Si* M *es un espacio vectorial de dimensión finita, sobre un anillo con división* A, *entonces el anillo de los* A*-endomorfismos de* M *es simple.*

Demostración. Ya que el anillo $\mathrm{End}_A M$ es isomorfo al anillo $M_n(A)$ de matrices de $n \times n$, con $n = \dim_A M$ (véase la sección 10 del capítulo 1) demostraremos que $M(n, A)$ es un anillo simple. Sean $A_1, \ldots, A_n$ los ideales izquierdos de $M(n, A)$ definidos como sigue: una matriz

$$u : J_n \times J_n \to A \quad (J_n = \{1, 2, \cdots, n\})$$

pertenece a A_i si y sólo si $u(h, k) = 0$ para toda $k \neq i$. O sea, A_i consta de aquellas matrices cuyas columnas distintas de la columna i son todas nulas. El conjunto A_i es efectivamente un ideal izquierdo de A: si $v \in A$, $u \in A_i$,

$$(vu)(h, k) = \sum_{r=1}^{n} v(h, r)\, u(r, k) = 0 \quad (k \neq i)$$

ya que $u(r, k) = 0$ para toda r cuando $k \neq i$. Es claro que

$$M_n(A) = A_1 \oplus \cdots \oplus A_n.$$

Por otra parte, la aplicación

$$f: A_i \to A_j$$

definida por

$$f(u)(h,k) = \begin{cases} u(h,i) & \text{si} \quad k = j \\ 0 & \text{si} \quad k \neq j \end{cases}$$

es un isomorfismo de A-módulos. En efecto,

$$f(vu)(h,k) = \begin{cases} (vu)(h,i) & \text{si} \quad k = j \\ 0 & \text{si} \quad k \neq j. \end{cases}$$

Se tiene, pues, en el primer caso,

$$f(vu)(h,j) = \sum_{r=1}^{n} v(h,r)u(r,i)$$

$$vf(u)(h,j) = \sum_{r=1}^{n} v(h,r)f(u)(r,i) =$$

$$= \sum_{r=1}^{n} v(h,r)u(r,i).$$

En el segundo caso, es decir, cuando $k \neq j$,

$$(vf(u))(h,k) = \sum_{r=1}^{n} v(h,r)f(u)(r,k) = 0,$$

o sea, en ambos casos, $f(vu) = vf(u)$.

Resumiendo, $M(n,A)$ es suma directa de un número finito de ideales izquierdos todos isomorfos entre sí. De acuerdo con la proposición 3.8, bastará, pues, demostrar que dichos ideales son mínimos. Para ello consideremos dos elementos $u, w \in A_1$, $u \neq 0$ por ejemplo. Existe $v \in A$ tal que $vu = w$ pues si, por ejemplo, $u(i,1) \neq 0$, puede tomarse v como sigue:

$$v(h,k) = 0 \quad \text{si} \quad k \neq i,$$

$$v(h,i) = \frac{w(h,1)}{u(i,1)},$$

con lo que queda probado que A_1 es mínimo y con ello el teorema.

OBSERVACIÓN

El anillo A construido anteriormente no tiene ideales bilaterales propios, pero, en general, sí tiene ideales izquierdos propios; es decir, que A es simple como anillo, pero como A-módulo izquierdo no lo es.

Sea ahora A un anillo y P un ideal izquierdo de A. Sea $B = \mathrm{End}_A(P)$. En forma natural P es un B-módulo izquierdo y así podemos considerar el anillo $C = \mathrm{End}_B(P)$ de B-endomorfismos de P. La aplicación

$$L: A \to C$$

definida por la multiplicación izquierda

$$L(a)(x) = ax \qquad (a \in A,\ x \in P)$$

(evidentemente $L(a) \in C$) es un homomorfismo de anillos. Con esta notación, tenemos el siguiente resultado.

Teorema 4.2.[1] *Si* A *es un anillo simple, entonces* L:A→C *es un isomorfismo.*

Demostración. Sea $b_a: P \to P$ la aplicación definida con $b_a(x) = xa$ $(x, a \in P)$. b_a es un A-endomorfismo, es decir, $b = b_a \in B$. Entonces, si $c \in C$, $a, x \in P$,

$$c(xa) = c(b(x)) = c(bx) = bc(x) = b(c(x)) = c(x)a.$$

Por otra parte, ya que $A = PA$, $1 = \sum x_i a_i$ con $x_i \in P$, $a_i \in A$; entonces

$$a = \sum x_i\, a_i\, a,$$

de donde

$$c(a) = \sum c(x_i\, a_i\, a) = \sum c(x_i)(a_i a) \quad (\text{pues } a_i a \in P)$$

y por tanto

$$c(a) = \sum L(c(x_i)a_i)(a) = L(\sum c(x_i)a_i)(a),$$

es decir,

$$c = L(\sum c(x_i)a_i)$$

con lo que queda demostrado que L es suprayectiva. Finalmente, puesto que $L \neq 0$ y A es simple, L es inyectiva.

Consideremos ahora un anillo simple A y una descomposición de A en ideales izquierdos mínimos

$$A = A_1 \oplus \cdots \oplus A_n.$$

[1] M. A. RIEFFEL: *A general Wedderburn theorem*, Proc. Nat. Acad. Sci. 54 (1965), pág. 1513.

Entonces

$$A_1 \cong A_2 \cong \cdots \cong A_n \text{ (como } A\text{-módulos)}.$$

Sea, además, P otro ideal izquierdo mínimo de A y

$$1 = e_1 + \cdots + e_n \quad (e_i \in A_i),$$

descomposición del 1 en elementos idempotentes y ortogonales dos a dos. Si como antes B es el anillo $\mathrm{End}_A(P)$, P puede considerarse como un B-módulo y la familia

$$e_1P,\ e_2P, \ldots,\ e_nP$$

da una descomposición en suma directa de P en B-módulos. En efecto, si $b: P \to P$ es un A-homomorfismo y $e_ix \in e_iP$ se tiene que $b(e_ix) = e_ib(x)$ que pertenece de nuevo a e_iP. Además, si $x \in P$, evidentemente

$$x = e_1x + \cdots + e_nx$$

y si $0 = e_1x_1 + \cdots + e_nx_n$ con $x_i \in P$, al multiplicar por e_i se tiene que

$$e_ix_i = 0.$$

Consideremos ahora las siguientes aplicaciones:

$$G: e_iP \to \mathrm{Hom}_A(A_i, P)$$
$$\mathrm{Hom}(h, 1): \mathrm{Hom}_A(A_i, P) \to \mathrm{End}_A(P) = B$$

en donde G es la biyección definida en la proposición 3.5 y h es un A-isomorfismo $h: P \to A_i$ (todos los ideales izquierdos de A son isomorfos). Es decir, la segunda aplicación está dada por

$$g \mapsto gh \quad (g: A_i \to P)$$

y es fácil ver que es también biyectiva. También se comprueba directamente que ambas aplicaciones son B-homomorfismos. Por ejemplo,

$$G(be_ix)(ae_i) = ae_ibe_ix = bae_ie_ix = bG(e_ix)(ae_i).$$

Por tanto, se ha demostrado el siguiente resultado:

Proposición 4.3. *Sea* A *un anillo simple y* n *el número de ideales izquierdos mínimos (necesariamente isomorfos entre sí) que aparecen en la descomposición de* A *en suma directa. Sea* P *un ideal izquierdo mínimo de* A *y* B *el anillo (con división) de los* A*-endomorfismos de* P. *Entonces* P, *considerado como espacio vectorial sobre* B, *es de dimensión* n.

Sean ahora, como antes, A un anillo simple, P un ideal izquierdo mínimo de A, $B = \mathrm{End}_A(P)$ y $C = \mathrm{End}_BP$. Entonces la aplicación

$$L: A \to C$$

que asocia a cada elemento de A la multiplicación a la izquierda por ese elemento es un homomorfismo *de anillos* y se tiene el

Teorema 4.4. (Wedderburn.) *Con la notación anterior se tiene que*

1) B *es un anillo con división*
2) L *es un isomorfismo*
3) *la dimensión de* P *como espacio vectorial sobre* B *es igual al número de sumandos de cualquier descomposición de* A *en ideales izquierdos mínimos de* A.

CAPITULO 4

Anillo de las representaciones

1. Anillo de las representaciones de un grupo finito

Asociados a un grupo finito G y un campo K se tienen el conjunto de clases de equivalencia de las representaciones de G con respecto a K y dos operaciones en él definidas; éstas son las inducidas por la suma y el producto de representaciones. La estructura algebraica obtenida es del mismo tipo de la que tienen los enteros positivos, en donde no existen inversos aditivos. En lo que sigue se dará una construcción para extender esta estructura a una estructura de anillo, con lo cual se logra asociar al grupo G y el campo K un anillo, que puede llamarse anillo de las representaciones de G sobre K o anillo de Grothendieck de G sobre K.

Iniciaremos la sección recordando cómo se asocia a cada monoide conmutativo un grupo. Sea X un monoide conmutativo cuya ley de composición denotaremos con $\oplus$. Se construye entonces el grupo abeliano libre generado por X, $\mathbf{Z}^{(X)}$ y el subgrupo de él generado por los elementos de la forma $x \oplus y - x - y (x, y \in X)$. Se definen entonces el grupo abeliano

$$K_0(X) = \mathbf{Z}^{(X)}/Y$$

y el homomorfismo (de monoides)

$$\gamma: X \to K_0(X)$$

dado por la composición de la inclusión y el homomorfismo canónico de paso al cociente

$$X \subset \mathbf{Z}^{(X)} \to \mathbf{Z}^{(X)}/Y.$$

[La demostración de que $\gamma(x \oplus y) = \gamma(x) + \gamma(y)$ se sigue directamente de las definiciones.]

Proposición 1.1. *Se tiene la siguiente propiedad universal de la pareja* $(K_0(X), \gamma)$:

Si $g: X \to H$ *es un homomorfismo del monoide* X *en un grupo abeliano* H, *existe un homomorfismo de grupos único* $h: K_0(X) \to H$ *tal que* $h\gamma = g$.

Demostración. Por ser X una base del $\mathbf{Z}$-módulo $\mathbf{Z}^{(X)}$, $g: X \to H$ se extiende (en forma núica) a un homomorfismo $\overline{g}: \mathbf{Z}^{(X)} \to H$. Como $g(x \oplus y) = g(x) + g(y)$, $\overline{g}(x \oplus y - x - y) = 0$, de donde, $\overline{g}$ se anula en Y y define, por tanto, un homomorfismo $h: K_0(X) \to H$. Si h' es otro homomorfismo con la propiedad requerida, $h\gamma = h'\gamma$, de donde $h = h'$ en una familia de generadores X de $K_0(X)$, por lo que $h = h'$.

Como de costumbre, la propiedad universal de la proposición anterior caracteriza a $K_0(X)$ y γ.

Aquí no está por demás hacer la observación siguiente. Si en el monoide X vale la ley de cancelación, entonces la construcción de tomar clases de equivalencia de parejas de elementos de X, como se hace usualmente al construir los enteros a partir de los naturales, coincide con la definición anterior (es muy fácil ver que la construcción mencionada satisface la propiedad universal).

Supongamos ahora que en el monoide conmutativo X hay una multiplicación asociativa, con elemento unitario y que distribuye a la suma. Como $\mathbf{Z}^{(X)} \otimes \mathbf{Z}^{(X)}$ tiene como base a $X \times X$, la multiplicación $X \times X \to X \subset \mathbf{Z}^{(X)}$ se extiende a una transformación lineal $\mathbf{Z}^{(X)} \otimes \mathbf{Z}^{(X)} \to \mathbf{Z}^{(X)}$, es decir, en $\mathbf{Z}^{(X)}$ se tiene una multiplicación que distribuye a la suma y que es asociativa y conmutativa. Así pues, $\mathbf{Z}^{(X)}$ es un anillo conmutativo con elemento unitario. Ya que $z((x \oplus y) - x - y) = z(x \oplus y) - zx - zy = zx \oplus zy - zx - zy \in Y$ $(z \in \mathbf{Z}^{(X)}, x, y \in X)$, Y es un ideal, $K_0(X)$ un anillo y γ una aplicación aditiva y multiplicativa.

En particular, si X es el conjunto de clases de equivalencia de una categoría pequeña (en donde X resulta ser un conjunto) $\mathcal{M}$ de A-módulos con la operación $\oplus$ inducida por la suma directa de A-módulos, $K_0(X)$ se llama el *grupo de Grothendieck* de la categoría y se denota $K_0(\mathcal{M})$.

Si $\mathcal{M}$ es la categoría de los A-módulos proyectivos, entonces se define $K_0(A) = K_0(\mathcal{M})$.

Finalmente, apliquemos lo antes expuesto a las representaciones. Sea G un grupo y K un campo. En la sección 2 del capítulo 2 se definieron

las operaciones de suma y producto de clases de representaciones matriciales de G sobre K obteniéndose un monoide conmutativo X con un producto asociativo, conmutativo, con 1 y que distribuye a la suma. Aplicando a X la construcción del anillo correspondiente se llega a la siguiente

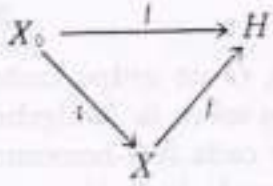
Definición 1.2. *El anillo de las representaciones de un grupo finito* G *con respecto al campo* K *es*

$$K_0(G, K) = K_0(X) = \mathbf{Z}^{(X)}/Y.$$

Más adelante se calculará este anillo para ciertos tipos de grupos y se verá cómo es que el conocimiento de dicho anillo proporciona información acerca de la estructura del grupo.

Definición 1.3. *Una familia* $\mathrm{X}_0 = \{\mathrm{x}_1, \ldots, \mathrm{x}_n\}$ *de elementos de* X *es una base del monoide* X *si todo elemento de* X *puede escribirse en forma única como* $\mathrm{x} = \mathrm{m}_1\mathrm{x}_1 \oplus \cdots \oplus \mathrm{m}_n\mathrm{x}_n$ *con* m_i *enteros no negativos.*

Es claro que si X_0 es una base de X y $f: X_0 \to H$ es una aplicación de X_0 en un monoide H, existe entonces un homomorfismo de monoides único $\bar{f}: X \to H$ tal que extiende a f, es decir, tal que el diagrama

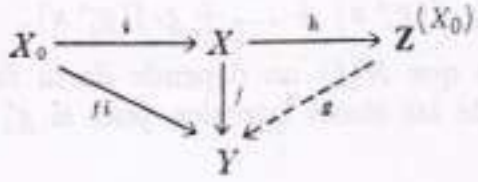


es conmutativo (i es la inclusión).

Teorema 1.4. *Si* $\mathrm{X}_0 = \{\mathrm{x}_1, \ldots, \mathrm{x}_n\}$ *es una base del monoide* X, *entonces la inclusión* $\mathrm{i}: \mathrm{X}_0 \to \mathrm{X}$ *induce un isomorfismo de grupos abelianos*

$$\mathbf{Z}^{(X_0)} \xrightarrow{\cong} K_0(X).$$

Demostración. Por ser X_0 base, existe un homomorfismo de monoides $h: X \to \mathbf{Z}^{(X_0)}$, único, tal que $hi(X_0)$ es una base de $\mathbf{Z}^{(X_0)}$. Para demostrar el teorema probaremos que la pareja $(\mathbf{Z}^{(X_0)}, h)$ tiene la propiedad universal respectiva. Sea Y un grupo abeliano y $f: X \to Y$ un homomorfismo de monoides. Consideremos el diagrama



Ya que $\{x_0, \ldots, x_n\}$ es también una base del grupo abeliano $\mathbf{Z}^{(X_0)}$, existe un homomorfismo de grupos g tal que $ghi = fi$ y como $\{x_0, \ldots, x_n\}$ es base de X, $gh = f$. Si g' es otro homomorfismo del grupo $\mathbf{Z}^{(X_0)}$ en Y tal que $g'h = f$ entonces $g'hi = fi = ghi$, de donde $g' = g$.

Otra demostración del teorema puede darse observando que si un monoide X tiene una base X_0, entonces vale la ley de cancelación en X. En efecto, si $x \oplus y = x \oplus z$ con $x = r_1x_1 \oplus \cdots \oplus r_nx_n$, $y = s_1x_1 \oplus \cdots \oplus s_nx_n$, $z = t_1x_1 \oplus \cdots \oplus t_nx_n$, se tiene que $r_i + s_i = r_i + t_i$, de donde $s_i = t_i$, es decir, $y = z$. Por tanto, según lo dicho al principio, $K_0(X)$ es el grupo abeliano que tiene como elementos las clases de equivalencia de $X \times X$ con respecto a la relación

$$(x, y) \sim (x', y') \Leftrightarrow x \oplus y' = x' \oplus y.$$

Sea, entonces, $u \in \mathbf{Z}^{(X_0)}$ y escribamos

$$u = \sum m_i x_i - \sum n_i x_i \quad (m_i, n_i \geq 0).$$

Es fácil ver que la aplicación $\mathbf{Z}^{(X_0)} \to K_0(X)$ dada por $u \mapsto (\bigoplus m_i\, 1, \bigoplus n_i\, 1)$ está bien definida y es un isomorfismo de grupos.

2. Teorema de Maschke

Sea ahora K un campo, G un grupo finito y H un subgrupo de G. Si M y M' son dos módulos sobre la K-álgebra KG, al considerar éstos como KH-módulos y pensar cada KG-homomorfismo de M en M' como KH-homomorfismo se obtiene la inclusión

$$i: \mathrm{Hom}_{KG}(M, M') \to \mathrm{Hom}_{KH}(M, M').$$

A continuación definiremos una aplicación que, inversamente, a cada KH-homomorfismo se obtiene la inclusión

$$i: \mathrm{Hom}_{KH}(M, M') \to \mathrm{Hom}_{KG}(M, M').$$

Para esto, sea

$$G = g_1H \cup \ldots \cup g_rH$$

una partición de G en clases izquierdas. Si $f: M \to N$ es un KH-homomorfismo de M en M' definimos

$$N(f)(x) = g_1 f(g_1^{-1} x) + \ldots + g_r f(g_r^{-1} x), \quad (x \in M).$$

Observemos primero que $N(f)$ no depende de la familia de representantes $g_1, \ldots, g_r$ de las clases laterales, pues si $g_1' = g_1h_1, \ldots, g_r' = g_rh_r$ $(h_i \in H)$,

$$g'_k f(g'^{-1}_k x) = g_k h_k f(h_k^{-1} g_k^{-1} x) =$$
$$g_k h_k h_k^{-1} f(g_k^{-1} x) = g_k f(g_k^{-1} x).$$

Evidentemente $N(f)$ es un K-homomorfismo de M en M'. Además, es un KG-homomorfismo, puesto que si $g \in G$ existe una permutación σ del conjunto $\{1, 2, \ldots, r\}$ tal que

$$g^{-1} g_k = g_{\sigma(k)} h_k, \ (1 \leq k \leq r)$$

con $h_k \in H$ y se tiene:

$$N(f)(gx) = g_1 f(g_1^{-1} gx) + \ldots + g_r f(g_r^{-1} gx) =$$
$$g_1 f(h_1^{-1} g_{\sigma(1)}^{-1} x) + \ldots = g_1 h_1^{-1} f(g_{\sigma(1)}^{-1} x) + \ldots =$$
$$g g_{\sigma(1)} f(g_{\sigma(1)}^{-1} x) + \ldots + g g_{\sigma(r)} f(g_{\sigma(r)}^{-1} x) =$$
$$g(g_{\sigma(1)} f(g_{\sigma(1)}^{-1} x) + \ldots + g_{\sigma(r)} f(g_{\sigma(r)}^{-1} x)) = g\, N(f)(x).$$

Al considerar $\mathrm{Hom}_{KG}(M, M')$ y $\mathrm{Hom}_{KH}(M, M')$ como espacios vectoriales sobre K, las aplicaciones i y N resultan ser transformaciones lineales. Además, i es multiplicativa, es decir, en el siguiente diagrama

$$\begin{array}{ccc} \mathrm{Hom}_{KH}(M, M') \times \mathrm{Hom}_{KH}(M', M'') & \to & \mathrm{Hom}_{KH}(M, M'') \\ \uparrow{\scriptstyle i \times i} & & \downarrow{\scriptstyle N} \quad \uparrow{\scriptstyle i} \\ \mathrm{Hom}_{KG}(M, M') \times \mathrm{Hom}_{KG}(M', M'') & \to & \mathrm{Hom}_{KG}(M, M'') \end{array}$$

se tiene que $i(gf) = i(g)\, i(f)$. Sin embargo, no pasa lo mismo con la transformación N. En este caso se tiene que si $f \in \mathrm{Hom}_{KG}(M, M')$ y $h \in \mathrm{Hom}_{KH}(M', M'')$ entonces

$$N(h \cdot i(f)) = N(h) \cdot f$$

y si $f \in \mathrm{Hom}_{KH}(M, M')$ y $h \in \mathrm{Hom}_{KG}(M', M'')$ entonces

$$N(i(h) \cdot f) = h \cdot N(f).$$

Proposición 2.1. *Si* $\mathrm{f} \in Hom_{KG}(\mathrm{M}, \mathrm{M}')$ *entonces*

$$Ni(f) = rf, \qquad (r = [G:H]).$$

Demostración. Si $x \in M$, como $i(f)(x) = f(x)$,

$$N(i(f)) = \sum_{k=1}^{r} g_k f(g_k^{-1} x) = \sum_{k=1}^{r} g_k g_k^{-1} f(x) = rf(x).$$

Corolario 2.2. *Si la característica de* K *no divide al índice de* H *en* G, Ni *es un isomorfismo y, por consiguiente,* N *es un epimorfismo.*

Teorema 2.3. (Maschke.) *Si el orden del grupo* G *no es divisible entre la característica del campo* K, *entonces el anillo* KG *es semisimple.*

Demostración. Para esto demostraremos (véase el problema 1.6 y la proposición 1.2, capítulo 3) que todo KG-módulo es semisimple. Sea, pues, M' un KG-submódulo de un KG-módulo M. Considerando a M y M' como espacios vectoriales sobre K, M' es sumando directo de M y, por consiguiente, existe un K-homomorfismo $f: M \to M'$ que, restringido a M', es la identidad de M': $f|M' = 1_{M'}$. Construyamos el KG-homomorfismo $N(f): M \to M'$. Si $x \in M'$, $g_k x \in M'$ $(G = \{g_1, \cdots, g_n\})$ y

$$N(f)(x) = \sum_{k=1}^{n} g_i f(g_i^{-1} x) = \sum g_i g_i^{-1} x = nx.$$

Pero, según la hipótesis, n tiene inverso en K lo cual implica que $N(f)|M'$ es un automorfismo y, por consiguiente, M' es sumando directo de M como KG-módulos.

3. Teoremas de Schur, Burnside y Frobenius

En el capítulo 2 se demostró una propiedad debida a Schur sobre módulos irreducibles (proposición 4.11). Aquí extenderemos este resultado al caso de álgebras arbitrarias, pero limitándonos al caso de que el campo básico sea algebraicamente cerrado.

Proposición 3.1. (Lema de Schur.) *Si* A *es un álgebra sobre un campo algebraicamente cerrado* K, *y* M *un* A*-módulo irreducible y de dimensión finita sobre* K, *entonces la aplicación*

$$\varphi : K \to \mathrm{End}_A(M)$$

dada por $\varphi(t) = t1_M$ *es un isomorfismo de* K*-álgebras.*

Demostración. Es inmediato que φ es un monomorfismo (de K-álgebras). Sea $d \in \mathrm{End}_A(M)$; existe un natural r tal que los elementos $1, d, d^2, \ldots, d^r$ son linealmente dependientes sobre K, es decir, existen $a_0, \cdots, a_r \in K$, no todos nulos, tales que $a_0 + a_1 d + \cdots + a_r d^r = 0$. Entonces el polinomio no nulo $F(X) = a_0 + a_1 X + \cdots + a_r X^r \in K[X]$ se descompone en la forma $F(X) = c(X - c_1) \cdots (X - c_r)$ con $(c \neq 0, c, c_i \in K)$. Es fácil ver que, entonces, $F(d) = c(d - c_1) \cdots (d - c_r) = 0$ y como $\mathrm{End}_A(M)$ es una K-álgebra con división por ser M A-irreducible, se tiene que $d = c_i$ para alguna c_i, lo cual prueba que φ es suprayectiva.

En otras palabras, el lema de Schur significa que todo A-endomorfismo de M puede realizarse mediante la multiplicación a la izquierda por un elemento de K. En forma análoga, el teorema de Burnside que se enunciará más adelante dice que todo K-endomorfismo de M puede

realizarse mediante la multiplicación a la izquierda por un elemento de A.

Lema 3.2. (Teorema chino del residuo.) *Sea* A *un anillo con elemento unitario y* $B_1, \cdots, B_h$ $(h \geq 2)$ *una familia de ideales izquierdos máximos de* A. *Entonces las dos condiciones siguientes son equivalentes:*

a) $B_k \not\supset \bigcap_{j \neq k} B_j \quad (1 \leq k \leq h)$.

b) *El homomorfismo*

$$A \to A/B_1 \oplus \cdots \oplus A/B_h$$

es suprayectivo.

Demostración. Si el homomorfismo es suprayectivo, el elemento $(0, \cdots \overline{a}_k, \cdots, 0)$ con $\overline{a}_k \neq 0$ proviene de un elemento a_k que no pertenece a B_k y que está en $\bigcap_{j \neq k} B_j$. Inversamente, sea $(0, \cdots, \overline{a}_k, \cdots, 0)$ un elemento de la suma directa. Por la hipótesis existe $c_k \in \bigcap_{j \neq k} B_j$ tal que $c_k \notin B_k$. Como B_k es máximo, $Ac_k + B_k = A$ y si a_k es un representante de $\overline{a}_k$, se puede escribir $a_k = ac_k + b_k$ $(a \in A,\ b_k \in B_k)$ y es fácil ver que la imagen de ac_k es $(0, \cdots, \overline{a}_k, \cdots, 0)$. Esto implica que el homomorfismo es suprayectivo.

Observación

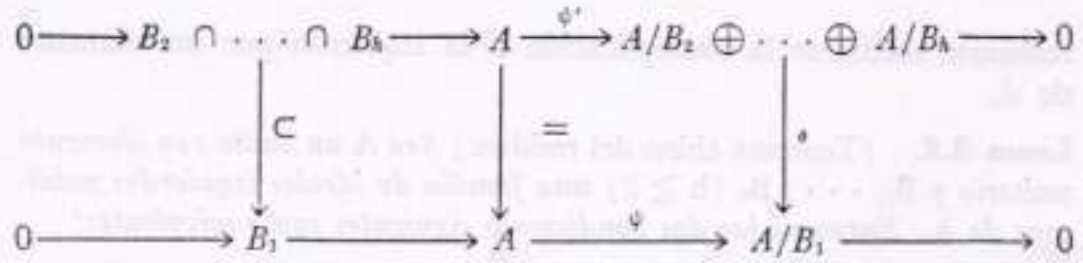
En el caso de que el anillo sea conmutativo, la condición (a) equivale a decir, simplemente, que los ideales $B_1, \ldots, B_h$ son distintos.

Proposición 3.3. *Sea* A *un anillo con elemento unitario y* $B_1, \ldots, B_h$ *una familia de ideales izquierdos máximos tales que si* $i \neq j$, A/B_i *no sea isomorfo a* A/B_j. *Entonces la sucesión de* A*-módulos*

$$0 \to B_1 \cap \cdots \cap B_h \to A \xrightarrow{\psi} A/B_1 \oplus \cdots \oplus A/B_h \to 0$$

es exacta.

Demostración. Para $h = 1$ la afirmación es obvia y por eso supondremos que $h \geq 2$. Siendo el núcleo de ψ $B_1 \cap \cdots \cap B_h$ queda solamente por probar que ψ es suprayectiva. Para ello probaremos por inducción sobre h la condición (a) del lema 3.2. Para $h = 2$ ésta es inmediata. Supongamos, pues, que $h \geq 3$ y que, por ejemplo, $B_1 \supset B_2 \cap \cdots \cap B_h$. Como la familia de ideales $B_2, \cdots, B_h$ cumple las condiciones de la proposición, se tiene el siguiente diagrama conmutativo y con los dos renglones exactos:



el cual da lugar al epimorfismo θ indicado. Así pues, obtenemos una sucesión exacta de A-módulos

$$0 \to C \to A/B_2 \oplus \cdots \oplus A/B_h \to A/B_1 \to 0.$$

Ahora bien, como $A/B_2 \oplus \cdots \oplus A/B_h$ es semisimple, C es sumando directo de dicho módulo y, por tanto, también A/B_1. Por la unicidad de la descomposición de un módulo se tendría, entonces, que A/B_1 sería isomorfo a algún A/B_k con $k \geq 2$, lo cual contradice las hipótesis.

Proposición 3.4. *Sea* A *un anillo artiniano tal que existe un* A*-módulo fiel* $M = M_1 \oplus \cdots \oplus M_h$ *con cada* M_k *irreducible y* $M_j \not\cong M_k$ *si* $j \neq k$. *Entonces*

a) *el anillo* A *es semisimple;*
b) *todo ideal izquierdo mínimo de* A *es isomorfo como* A*-módulo a alguna* M_k.

Demostración. Sean $B_1, \ldots, B_h$ ideales izquierdos máximos de A tales que $A/B_i \cong M_i$ $(1 \leq i \leq h)$. De acuerdo con la proposición 3.3, $M \cong A/(B_1 \cap \cdots \cap B_h)$. Sea $R = \text{rad}(A)$; $RA \subset R \subset B_1 \cap \cdots \cap B_h$, de donde $RM = 0$. Por consiguiente, R está contenido en el anulador de M el cual es 0 por ser el módulo fiel, de donde $R = 0$ y como A es artiniano resulta semisimple.

Sea ahora I un ideal izquierdo mínimo de A. Si $I \not\subset B_1 \cap \ldots \cap B_h$, entonces I no está contenido en alguna B_i, digamos que $I \not\subset B_1$. Entonces $I + B_1 = A$ y $I \cap B_1 = 0$, de donde $I \cong A/B_1 \cong M_1$. Si $I \subset B_1 \cap \cdots \cap B_h$ existiría $x \in A$ tal que $Ix \not\subset B_1 \cap \cdots \cap B_h$. En efecto, sea $y \in I$, $y \neq 0$; si para toda $x \in A$, $yx \in B_1 \cap \cdots \cap B_h$, $y \in \text{an}\, M = 0$, lo cual es una contradicción. Entonces la aplicación $I \to Ix$ dada por $y \mapsto yx$ es un epimorfismo y ya que $Ix \neq 0$ resulta isomorfismo, reduciéndose este segundo caso al primero.

OBSERVACIÓN

Si el anillo A es semisimple, existe siempre un A-módulo fiel $M = M_1 \oplus \cdots \oplus M_h$ con las M_k no isomorfas dos a dos. Esto indica que la proposición 3.4 da otra caracterización de los anillos semisimples.

Corolario 3.5. *Sea* A *un anillo artiniano tal que existe un* A*-módulo fiel e irreducible. Entonces* A *es simple (e inversamente).*

Demostración. La condición (a) de 3.4 nos dice que A es semisimple y la (b), que todos los ideales mínimos de A son isomorfos. Entonces A es simple (capítulo 3, proposición 1.2 y corolario 3.8).

Teorema 3.6. (Burnside). *Si* A *es un álgebra sobre un campo algebraicamente cerrado* K *tal que existe un* A*-módulo* M *fiel, irreducible y de dimensión finita sobre* K*, entonces el homomorfismo de álgebras sobre* K

$$\varphi : A \to \mathrm{End}_K(M)$$

dado por $\varphi(\mathrm{a})(\mathrm{x}) = \mathrm{ax}$ *es un isomorfismo.*

Demostración. Observemos primero que las hipótesis del teorema implican que A es simple. En efecto, por la fidelidad, φ es monomorfismo y A es isomorfo a una subálgebra de $\mathrm{End}_K(M)$. Siendo ésta de dimensión finita sobre K también lo es A y, por tanto, A es artiniano. De acuerdo con el corolario 3.5, A resulta simple. Es posible, entonces, aplicar el teorema de Wedderburn al álgebra A, el cual asegura que $\varphi : A \to \mathrm{End}_D(M)$ con $D = \mathrm{End}_A(M)$ es un isomorfismo (M se puede identificar con un ideal izquierdo mínimo de A). Pero, según el lema de Schur 3.1, $D = K$.

Teorema 3.7. (Frobenius.) *Si* A *es un álgebra sobre un campo algebraicamente cerrado* K *tal que existe un* A*-módulo fiel* $\mathrm{M} = \mathrm{M}_1 \oplus \cdots \oplus \mathrm{M}_h$ *con los* M_i *irreducibles y no isomorfos dos a dos y la dimensión de* M *sobre* K *es finita, entonces el homomorfismo de álgebras*

$$\varphi : A \to \mathrm{End}_K(M_1) \times \cdots \times \mathrm{End}_K(M_h)$$

definido por $\mathrm{a} \mapsto (\varphi_1(\mathrm{a}), \cdots, \varphi_h(\mathrm{a}))$ *con* $\varphi_i(\mathrm{a})(\mathrm{x}) = \mathrm{ax}(\mathrm{x} \in \mathrm{M}_i)$ *es un isomorfismo.*

Demostración. Como en la demostración del teorema anterior se concluye que A es artiniano y de acuerdo con la proposición 3.4, A resulta semisimple y los módulos irreducibles $M_1, \cdots, M_h$ se pueden identificar con ideales izquierdos mínimos no isomorfos de A. Además, todo ideal izquierdo mínimo es isomorfo a uno de esos. Por consiguiente, al descomponer A como producto directo de anillos simples hay h factores: $A = A_1 \times \cdots \times A_h$ y cada M_i es un A_i-módulo que satisface las hipótesis del teorema de Burnside. Entonces $\varphi_i : A_i \to \mathrm{End}_K(M_i)$ son isomorfismos y, por tanto, φ lo es también.

De los resultados anteriores podemos deducir una importante relación entre el orden del grupo y los grados de las representaciones irreducibles no isomorfas del mismo.

Proposición 3.8. *Si* K *es un campo algebraicamente cerrado, cuya característica no divide al orden* n *del grupo* G, *y* $n_1, \cdots, n_h$ *son los grados de las representaciones no equivalentes que figuran en la descomposición regular de* G *sobre* K, *entonces*

$$n = n_1^2 + \cdots + n_h^2$$

Demostración. De acuerdo con el teorema 2.3 (Maschke), KG es semisimple y, según la observación que sucede a la proposición 3.4 y el teorema 3.7 (Frobenius),

$$KG \cong \mathrm{End}_K(M_1) \times \cdots \times \mathrm{End}_K(M_h),$$

siendo $M_1, \cdots, M_h$ KG-módulos correspondientes a las representaciones aludidas.

Proposición 3.9. *Sea* A *un álgebra sobre un campo algebraicamente cerrado* K, $M = M_1 \oplus \cdots \oplus M_h$ *una descomposición de un* A*-módulo* M *en módulos irreducibles no isomorfos dos a dos y de dimensiones* $n_1, \cdots, n_h$ *respectivamente. Sean* $B^k = (b_{j_k}^k)$ *bases de* M_k *sobre* K, *Entonces las transformaciones lineales* $f_{i_k j_k}^k \in \mathrm{Hom}_K(A,K)$ *definidas por*

$$ab_{j_k}^k = f_{i_k j_1}^k(a)\, b_1 + \cdots + f_{i_k j_{n_k}}^k(a) b_{n_k}$$

son linealmente independientes sobre K.

Demostración. Sea $A' = \varphi(A) \subset \mathrm{End}_K(M)$. Entonces M es un A-módulo fiel y se cumplen las hipótesis del teorema de Frobenius para A' de donde

$$A' = \mathrm{End}_K(M_1) \times \cdots \times \mathrm{End}_K(M_h).$$

Sean $E_{i_k j_k}^k \in \mathrm{End}_K(M_k)$ definidos por

$$E_{i_k j_k}^k(b_{m_k}^k) = \begin{cases} b_{i_k} & \text{si} \quad m_k = j_k \\ 0 & \text{si} \quad m_k \neq j_k \end{cases}$$

Existen elementos $a_{i_k j_k}^k \in A$ tales que

$$\varphi(a_{i_k j_k}^k) = (0, \cdots, E_{i_k j_k}^k, \cdots, 0).$$

Entonces

$$\varphi(a_{i_k j_k}^k) = (0, \cdots, E_{i_k j_k}^k, \cdots, 0) = \begin{cases} 0 & \text{si } m \neq k \\ 0 & \text{si } m = k \text{ y } r_k \neq j_k \\ b_{i_k}^k & \text{si } m = k \text{ y } r_k = j_k \end{cases}$$

Por tanto,

$$f^m_{r_m s_m}(a^k_{i_k j_k}) = \begin{cases} 1 & \text{si } m = k,\ r_m = i_k,\ s_m = j_k \\ 0 & \text{en los demás casos,} \end{cases}$$

lo cual implica la independencia sobre K de las $f^k_{i_k j_k}$.

4. Representaciones completamente reducibles

Definición 4.1. *Una representación* $R: G \to GL(n, K)$ *se llama completamente reducible si puede descomponerse en una suma finita* $R = R_1 \oplus \cdots \oplus R_h$ *de representaciones irreducibles* $R_i: G \to GL(n_i, K)$, *o sea, si el* KG*-módulo correspondiente a la representación* R *es semisimple.*

Entonces se tiene, como consecuencia de la proposición 8.7 del capítulo 1, la proposición siguiente:

Proposición 4.2. *La descomposición* $R = R_1 \oplus \cdots \oplus R_h$ *de una representación completamente reducible de* G *en representaciones irreducibles es única* (excepto por permutaciones de los sumandos).

Proposición 4.3. *Si la característica del campo* K *no divide al orden del grupo* G, *entonces todas las representaciones de* G *sobre* K *son completamente reducibles.*

Esto es consecuencia del teorema 2.3 (Maschke) de este capítulo.

Sea ahora S la representación regular de G, es decir, la representación asociada al KG-módulo KG y supongamos nuevamente que el orden de G no es divisible entre la característica K. Sea $S = S_1 \oplus \cdots \oplus S_t$ una descomposición de S en representaciones irreducibles sobre K y $\{R_1, \ldots, R_h\}$ una familia completa de representantes de las clases de equivalencia de las representaciones $S_1, \ldots, S_t$, es decir, si $i \neq j$, R_i no es equivalente a R_j y cada S_i es equivalente a alguna R_j. Denotemos, como antes, con X al monoide formado con las clases de equivalencia de las representaciones de G sobre K y consideremos el subconjunto X_0 de X que tiene como representantes a $R_1, \ldots, R_h$.

Proposición 4.4. *Si el orden del grupo* G *no es divisible entre la característica de* K, *entonces para cada representación* R *de* G *sobre* K *existen enteros no negativos únicos* $m_1, \ldots, m_h$ *tales que* R *es equivalente a* $m_1R_1 \oplus \cdots \oplus m_hR_h$, *en donde* $R_1, \ldots, R_h$ *son las representaciones antes definidas.*

Esto es consecuencia del corolario 1.8 del capítulo 3.

Esta proposición podemos enunciarla diciendo:

Corolario 4.5. X_0 *es una base del monoide* X.

Los resultados anteriores nos permiten calcular el grupo $K_0(G, K)$ en el caso en que la característica de K no divida al orden de G. En efecto, se tiene el siguiente

Teorema 4.6. *Si el orden del grupo* G *no es divisible entre la característica de* K, *entonces el grupo de las representaciones de* G *sobre* K, $K_0(G, K)$ *es un grupo abeliano libre de rango* h, *en donde* h *es el número de representaciones irreducibles no equivalentes que aparecen en la representación regular de* G *sobre* K.

(h es el número de elementos de X_0.)

A continuación determinaremos el número de representaciones irreducibles no equivalentes. Para esto analizaremos el centro de un álgebra semisimple A.

Teorema 4.7. *Si* A *es un álgebra semisimple sobre un campo* K, *entonces el número de componentes simples de* A *es menor o igual que la dimensión de su centro* C *sobre* K. *Si, además,* K *es algebraicamente cerrado, entonces es válida la igualdad.*

Demostración. Sea $A = A_1 \times \cdots \times A_n$ una descomposición de A en álgebras simples. Ya que el centro de A es el producto de los centros de las n componentes simples, es inmediato que la dimensión de C sobre K es mayor o igual que n. Si K es algebraicamente cerrado, cada componente simple es, según el teorema de Burnside 3.6, isomorfo a un álgebra completa de matrices sobre K. Es bien sabido que el centro de dicha álgebra consta de las matrices escalares y, por tanto, es de dimensión 1 sobre K.

Consideremos ahora el caso en que el álgebra A sea el álgebra de grupo KG. Sea $G = S_1 \cup \cdots \cup S_h$ la partición de G en clases de elementos conjugados. Denotemos con c_i a los elementos

$$c_i = \sum_{g \in S_i} g.$$

Teorema 4.8. *Los elementos* $c_1, \ldots, c_h$ *forman una base del centro* C *de* KG.

Demostración. Ya que $S_i g = g S_i$ para toda g en G, es claro que los elementos c_i pertenecen al centro. Además, como $S_i \cap S_j = \emptyset$ si $i \neq j$, la familia $c_1, \ldots, c_h$ es linealmente independiente. Finalmente, sea $u = \sum a_g g$ un elemento del centro. Probaremos que para todas g, $h \in G$ el coeficiente a_g es igual al coeficiente $a_{ghg^{-1}}$. En efecto, ya que $u \in C$, $huh^{-1} = u$, de donde

$$\sum a_g g = \sum a_g h_g h^{-1}.$$

Comparando los coeficientes, resulta $a_g = a_{ghg^{-1}}$.

Como consecuencia de los dos resultados anteriores se tiene el

Teorema 4.9. *Sea* G *un grupo finito y* K *un campo algebraicamente cerrado cuya característica no divide al orden de* G. *Entonces el número de representaciones irreducibles no equivalentes de* G *sobre* K *es igual al número de clases de elementos conjugados de* G.

En el caso de que el campo no sea algebraicamente cerrado, puede asegurarse que el número de representaciones irreducibles no equivalentes es menor o igual que dicho número de clases de conjugados.

Corolario 4.10. *El número de representaciones irreducibles no equivalentes de un grupo* G *sobre un campo* K *es menor o igual que el número de representaciones irreducibles no equivalentes sobre la cerradura algebraica de* K.

Para terminar la sección demostraremos una fórmula relativa al producto de la representación regular por sí misma, utilizando la interpretación de ésta como el KG-módulo izquierdo KG.

Al operar G en $G \times G$ diagonalmente, es decir,

$$g(g', g'') = (gg', gg''),$$

$G \times G$ queda partido en n órbitas de n elementos cada una

$$G \times G = H_1 \cup \cdots \cup H_n,$$

en donde n es el orden de G. Por ejemplo, si $G = \{1 = g_1, \ldots, g_n\}$, los elementos

$$(1, 1), (1, g_2), \cdots, (1, g_n),$$

constituyen una familia de representantes de $H_1, \ldots, H_n$.

La aplicación

$$G \times G \to KG \otimes_K KG$$

dada por $(g, g') \mapsto g \otimes g'$ es una K-base de $KG \otimes_K KG$. Sean $M_1, \ldots, M_n$ los K-módulos con bases $H_1, \ldots, H_n$ respectivamente. Éstos son, evidentemente, KG-módulos (recuérdese que la operación de G en $KG \otimes_K KG$ es diagonal).

Para $1 \leq i \leq n$ la aplicación $KG \to M_i$ dada por $g \mapsto g(1, g_i)$ es un KG-isomorfismo.

Hemos obtenido, así, el siguiente resultado:

Proposición 4.11. *Si* G *es un grupo de orden* n *y la característica de* K *no divide a* n, *entonces, como* KG*-módulos,*

$$KG \otimes_K KG \cong KG \oplus \cdots \oplus KG, \quad (n \text{ sumandos}).$$

Corolario 4.12. *Si* R *es la representación regular de un grupo cuyo orden no sea divisible entre la caracteristica del campo se tiene*

$$[R] \otimes [R] = n[R] \qquad (n = [G:1])$$

en donde [R] *es la clase de equivalencia de* R.

CAPITULO 5

Cálculo de las representaciones de algunos grupos finitos

1. Representaciones de los grupos cíclicos

En esta sección usaremos las siguientes notaciones:

T es un grupo cíclico de orden n;
K es un campo cuya característica no divide a n;
t es un generador de T;
X es el monoide de clases de representaciones de T sobre K con la operación inducida por la suma de representaciones;
$[R]$ denotará la clase de representaciones que contiene a la representación R.

Si denotamos con $K[x]$ al anillo de polinomios en x con coeficientes en K, podemos definir una aplicación

$$\varphi: X \to K[x]$$

asociando a cada clase $[R]$ de representaciones el polinomio característico $\mathrm{car}(R(t))$ de la matriz $R(t)$, es decir,

$$\varphi([R]) = \mathrm{car}(R(t)).$$

Esta aplicación está bien definida, pues si R y R' son representaciones equivalentes, las matrices $R(t)$ y $R'(t)$ son semejantes, por lo cual tienen el mismo polinomio característico. Además, el polinomio característico de la matriz $(R_1 \oplus R_2)(t)$ es igual al producto de los polinomios característicos de $R_1(t)$ y $R_2(t)$. Así pues, φ es un homomorfismo del monoide X en el monoide multiplicativo de $K[x]$.

Lema 1.1. *Si* R *es una representación irreducible de* T *y la matriz* R(t) *satisface un polinomio* f(x) ∈ K [x], *es decir,*

$$f(R(t)) = 0,$$

entonces el grado de f *es mayor o igual que el de la representación.*

Demostración. Sea V el KT-módulo asociado a R, es decir, V es un espacio vectorial sobre K de dimensión m igual al grado de R, con la operación

$$tu = R(t)(u), \quad (u \in V).$$

Sea $v \in V$, $v \neq 0$ y

$$f(x) = a_0 + a_1 x + \cdots + a_q x^q, \ (a_i \in K, \ a_q \neq 0).$$

Ya que $f(R(t)) = 0$, $f(t)v = 0$, de donde,

$$t^q v = -\frac{a_0}{a_q} v - \frac{a_1}{a_q} tv - \cdots - \frac{a_{q-1}}{a_q} t^{q-1} v$$

y, por tanto, $t^r v$ (r arbitraria) es combinación lineal (con coeficientes en K) de los vectores $v, tv, \ldots, t^{q-1}v$. Veremos que estos q elementos generan a V sobre K, con lo cual quedará demostrado que $q \geq m$. En efecto, ya que R es irreducible, V como KT-módulo es irreducible y si u es un elemento arbitrario de V, existe $g(x) \in K[x]$ tal que $g(t)v = u$. Es decir, u es una combinación lineal (con coeficientes en K) de elementos de la forma $t^r v$, y, por lo antes demostrado, de los elementos $v, tv, \ldots, t^{q-1}v$, es decir, éstos generan a V sobre K.

Teorema 1.2. *La aplicación* $\varphi: \mathrm{X} \to \mathrm{K}[\mathrm{x}]$ *dada por* $\varphi([\mathrm{R}]) = \mathrm{car}(\mathrm{R}(\mathrm{t}))$ *es un isomorfismo de* X *en el submonoide de* K [x] *de elementos de la forma*

$$p_1^{s_1} \cdots p_h^{s_h} \quad (s_i \geq 0)$$

en donde $\mathrm{p}_1, \ldots, \mathrm{p}_n$ *son los factores irreducibles de* $\mathrm{x}^n - 1$ *en* K [x]. *Además, una representación* R *es irreducible si y sólo si* $\varphi([\mathrm{R}]) = \mathrm{p}_i(\mathrm{x})$ *para cierta* i.

Demostración. Demostraremos primero que si R es irreducible, $\varphi([R])$ es irreducible. Supongamos que $\varphi([R]) = f(x)g(x)$, $f, g \in K[x]$. Según el teorema de Cayley-Hamilton, si $A = R(t)$.

$$0 = \varphi([R])(A) = f(A)\, g(A).$$

Pero $f(A)$ y $g(A)$ pertenecen a $\mathrm{End}_{KT}(V)$ que, por ser R irreducible, es un álgebra con división. Por tanto, $f(A) = 0$, o bien $g(A) = 0$. De acuerdo con el lema 1.1, $gr(f) \geq m$, o bien $gr(g) \geq m$, con $m = \dim V = gr(\varphi([R]))$ y $\varphi([R])$ es irreducible.

Veremos ahora que si R es una representación tal que $\varphi([R])$ es un polinomio irreducible, entonces R es irreducible. En efecto, si no lo fuera, el KT-módulo V asociado a R se podría escribir como suma directa de KT-submódulos propios

$$V = W_1 \oplus W_2$$

y $\varphi([R]) = \operatorname{car}(R(t)) = \operatorname{car}(R(t)|W_1) \cdot \operatorname{car}(R(t))|W_2)$ siendo estos últimos polinomios de grados iguales a $\dim W_1$ y $\dim W_2$ respectivamente, ambas menores que $\dim V = gr(\varphi([R]))$. Entonces $\varphi([R])$ no sería un polinomio irreducible en $K[x]$.

Ahora bien, ya que $R(t^n) = R(t)^n = 1$, las raíces características de $R(t)$ son ceros del polinomio $x^n - 1$ de donde, si R es irreducible $\varphi([R]) \in K[x]$ es un factor irreducible de $x^n - 1$ en $K[x]$, es decir, es una de las $p_i(x)$.

Recíprocamente, dado un factor irreducible en $K[x]$ de $x^n - 1$, digamos

$$p_i(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_2 x + a_0,$$

definimos la representación determinada por la matriz compañera de este polinomio, a saber,

$$R(t) = (-1)^m \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix},$$

($R(t)^n = 1$ ya que, según el teorema de Cayley-Hamilton, $R(t)$ satisface a $p_i(x)$) y ya que $\operatorname{car}(R(t)) = p_i(x)$, $\varphi([R]) = p_i(x)$.

La restricción de φ al conjunto de clases de representaciones irreducibles es inyectiva. En efecto, supongamos que $\varphi([R]) = \varphi([S])$, con R y S irreducibles. Por lo anterior $\varphi([R]) = \varphi([S]) = p_i(x)$ para cierta i, de donde, las raíces características de las matrices $R(t)$ y $S(t)$ son las raíces de $p_i(x)$, las cuales son todas distintas. Entonces $R(t)$ y $S(t)$ son semejantes. Ahora bien, las clases de representaciones irreducibles forman una base del monoide X y sus imágenes, por lo anterior, constituyen un subconjunto de la base del monoide multiplicativo de $K[x]$ formada por los polinomios irreducibles. Por consiguiente φ es inyectiva en todo X y su imagen es el conjunto de polinomios de la forma

$$p_1^{s_1} \cdots p_h^{s_h}, \quad (s_i \geq 0).$$

Corolario 1.3. *Si*

$$x^n - 1 = p_1(x) \cdots p_h(x)$$

es la descomposición de $x^n - 1$ *en polinomios irreducibles de* $K[x]$, *entonces* T *tiene* h *clases de representaciones irreducibles y éstas están dadas por*

$$R_i(t) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_{i0} \\ 1 & 0 & 0 & \cdots & 0 & -a_{i1} \\ 0 & 1 & 0 & \cdots & 0 & -a_{i2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{im_i-1} \end{pmatrix},$$

en donde,

$$p_i(x) = x^{m_i} + a_{im_i-1}x^{m_i-1} + \cdots + a_{i1}x + a_{i0}.$$

En particular, para el caso en que $K = \mathbf{R}$ es el campo de los números reales tenemos el

Corolario 1.4. *Sea*

$$x^n - 1 = (x-1)(x^2 - 2a_2x + 1)\cdots(x^2 - 2a_{m+1}x + 1) \qquad (\text{si } n = 2m+1)$$

$$x^n - 1 = (x-1)(x^2 - 2a_2x + 1)\cdots(x^2 - 2a_m x + 1)(x+1) \qquad (\text{si } n = 2m)$$

la descomposición de $x^n - 1$ *en polinomios irreducibles sobre* R. *Entonces* T *tiene* m + 1 *clases de representaciones irreducibles y éstas están determinadas por*

$$R_1(t) = 1,\ R_i(t) = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix} \qquad (2 \le i \le m+1) \text{ para } n = 2m+1.$$

y por

$$R_1(t) = 1,\ R_i(t) = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix} \qquad (2 \le i \le m),\ R_{m+1}(t) = -1 \text{ para } n = 2m$$

en donde $a_i^2 + b_i^2 = 1$.

Demostración. De acuerdo con el corolario anterior sabemos que hay $m+1$ clases de representaciones y que éstas están dadas por las fórmulas

$$R_1(t) = 1,\ R_i(t) = \begin{pmatrix} 0 & -1 \\ 1 & 2a_i \end{pmatrix} \qquad (2 \le i \le m+1),$$

en el caso impar y por

$$R_1(t) = 1,\ R_i(t) = \begin{pmatrix} 0 & -1 \\ 1 & 2a_i \end{pmatrix} \qquad (2 \leq i \leq m),\ R_{m+1}(t) = -1$$

en el caso par. Pero ya que

$$\begin{pmatrix} 0 & -1 \\ 1 & 2a \end{pmatrix} = \begin{pmatrix} a & b \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a & b \\ -1 & 0 \end{pmatrix}^{-1},$$

podemos sustituir las representaciones anteriores por las del enunciado del teorema.

Si $K = \mathbf{C}$, se tiene el

Teorema 1.5. *El número de clases de representaciones irreducibles de un grupo cíclico de orden* n *sobre el campo de los números complejos es* n *y éstas están determinadas por*

$$R_i(t) = z^i$$

en donde z es una raíz primitiva n*-ésima de la unidad.*

2. Anillo de las representaciones de un grupo cíclico

De los resultados de la sección precedente se sigue que el grupo aditivo del anillo $K_0(T, K)$ de las representaciones de un grupo cíclico T de orden n sobre un campo K cuya característica no divide a n es un grupo abeliano libre de rango igual al número de factores irreducibles que aparecen en la descomposición del polinomio $x^n - 1$ en $K[x]$. Determinaremos a continuación la estructura multiplicativa de este anillo.

Para simplificar la notación, cuando no dé origen a confusiones, en lo que sigue denotaremos con R tanto a una representación como a su clase de equivalencia $[R]$.

Sean R y S dos representaciones de T sobre K y

$$\operatorname{car}(R(t)) = (x - \alpha_1) \cdots (x - \alpha_r),$$
$$\operatorname{car}(S(t)) = (x - \beta_1) \cdots (x - \beta_s),$$

las descomposiciones en factores lineales de los polinomios característicos de $R(t)$ y $S(t)$, con α_i, β_j en una extensión apropiada de K. Sabemos que α_i, β_j y, por tanto, todos los productos $\alpha_i\beta_j$ son raíces n-ésimas de la unidad.

Por otro lado, se sabe que el polinomio característico del producto de Kronecker $R(t) \otimes S(t)$ es

$$\operatorname{car}(R(t) \otimes S(t)) = \Pi_{i,j}\,(x - \alpha_i\,\beta_j).$$

Pero este polinomio tiene coeficientes en K, pues la matriz $R(t) \otimes S(t)$ está formada con elementos de K. Luego, por lo anterior, las raíces pueden juntarse de manera que

$$\Pi_{i,j}\,(x - \alpha_i\,\beta_j) = p_1^{n_1} \cdot \cdots \cdot p_h^{n_h},$$

en donde, como antes, $p_1(x), \ldots, p_h(x) \in K[x]$ son los factores irreducibles de $x^n - 1$.

O sea,

$$\operatorname{car}\,((R \otimes S)(t)) = p_1^{n_1} \cdot \cdots \cdot p_h^{n_h}$$

y entonces

$$R \otimes S = n_1 R_1 \oplus \cdots \oplus n_h R_h,$$

siendo R_i la representación irreducible cuyo polinomio característico es $p_i(x)$.

Para el caso en que K sea el campo $\mathbf{C}$ de los números complejos, esto nos conduce al siguiente

Teorema 2.1. *El anillo de las representaciones* $\mathrm{K}_0(\mathrm{T}, \mathbf{C})$ *de un grupo cíclico* T *sobre* $\mathbf{C}$ *es isomorfo al anillo de grupo* $\mathbf{Z}\mathrm{T}$.

Calcularemos ahora $K_0(T, \mathbf{R})$, dando fórmulas explícitas para la multiplicación. Para ello observemos primero que los polinomios irreducibles en $\mathbf{R}[x]$ que aparecen en la descomposición de $x^n - 1$ determinan una partición del grupo Z de las raíces n-ésimas de 1, agrupando las raíces que pertenecen al mismo polinomio. En otras palabras, son las clases de equivalencia de Z con respecto a la conjugación de números complejos. Denotaremos con $\overline{Z}$ a este conjunto. Así pues, si z, $\bar{z}$ son las raíces de uno de los polinomios $p(x)$, factor irreducible de $x^n - 1$ en $\mathbf{R}[x]$, a la representación irreducible correspondiente (o sea aquélla cuyo polinomio característico sea $p(x)$) la denotaremos por $R_{(z)}$. Por ejemplo, si $p(x)$ es lineal, $z = \bar{z}$, $R_{(z)}$ es la que corresponde a $x - z$; si $p(x)$ es cuadrático, $z \neq \bar{z}$, $R_{(z)}$ es la representación correspondiente al polinomio $(x - z)(x - \bar{z}) \in \mathbf{R}[x]$. Explícitamente,

$$R_{(z)}(t) = (z) \text{ cuando } z = \bar{z} \quad (\therefore z = \pm 1)$$

$$R_{(z)}(t) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \text{ cuando } z \neq \bar{z}, \quad \text{con} \quad a + bi = z.$$

Para describir el producto en la base de $K_0(T, \mathbf{R})$ conviene hacer la siguiente observación. Si

$$aR \otimes bS = a_1 R_1 \oplus \cdots \oplus a_h R_h \quad (a, b \in \mathbf{Z},\ a, b \neq 0)$$

entonces

$$R \otimes S = (a_1/ab)\, R_1 \oplus \cdots \oplus (a_k/ab) R_k,$$

con a_i/ab forzosamente en $\mathbf{Z}$. O sea, que para conocer el producto en $K_0(T, \mathbf{R})$ basta dar la tabla de la multiplicación para múltiplos arbitrarios (no nulos, desde luego) de los elementos básicos. En nuestro caso, es conveniente considerar las representaciones siguientes. Si $R_{(z)}$ es una representación irreducible de T, definimos

$$R_{(z)} = \begin{cases} R_{(z)} & \text{si} \quad z \neq \bar{z} \\ 2R_{(z)} & \text{si} \quad z = \bar{z} \end{cases}$$

Teorema 2.2. *El anillo de las representaciones* $\mathrm{K}_0(\mathrm{T}, \mathbf{R})$ *de un grupo cíclico* T *de orden* n *sobre un campo cuya característica no divide a* n, *es un grupo abeliano libre de rango* n *con base* $\mathrm{R}_{(z)}$ $((\mathrm{z}) \in \overline{\mathrm{Z}}$, *conjunto de clases de equivalencia del grupo* Z *de raíces* n*-ésimas de la unidad con respecto a la conjugación) y con la multiplicación determinada por*

$$\overline{R}_{(z)} \otimes \overline{R}_{(w)} = \overline{R}_{(zw)} \oplus \overline{R}_{(z\bar{w})}.$$

Demostración. (El producto anterior está bien definido. Por ejemplo, $\overline{R}_{(\bar{z})} \otimes \overline{R}_{(w)} = \overline{R}_{(\bar{z}w)} \oplus \overline{R}_{(\bar{z}\bar{w})} = \overline{R}_{(z\bar{w})} \oplus R_{(zw)} = \overline{R}_{(z)} \otimes \overline{R}_{(\bar{w})}$.) Las raíces características de $\overline{R}_{(z)}(t)$ son z, $\bar{z}$ y las de $\overline{R}_{(w)}(t)$, w, $\bar{w}$. Por tanto, las de $(\overline{R}_{(z)} \otimes \overline{R}_{(w)})(t)$ son zw, $z\bar{w}$, $\bar{z}w$, $\bar{z}\bar{w}$, de donde,

$$\begin{aligned} \operatorname{car}\left((\overline{R}_{(z)} \otimes \overline{R}_{(w)})(t)\right) &= (x - zw)(x - \bar{z}\bar{w})(x - z\bar{w})(x - \bar{z}w) \\ &= \operatorname{car}\left(R_{(zw)}(t)\right) \operatorname{car}\left(R_{(z\bar{w})}(t)\right), \end{aligned}$$

lo cual prueba la fórmula de la multiplicación.

En la sección 8 de este capítulo daremos varios ejemplos de $K_0(T, \mathbf{R})$ con la tabla de multiplicación para los elementos básicos.

3. Anillo de las representaciones de un grupo abeliano

Calcularemos aquí el anillo de las representaciones de un grupo abeliano finito G sobre el campo $\mathbf{C}$ de los números complejos. De acuerdo con los teoremas 4.6 y 4.9 del capítulo 4, el grupo de las representaciones de G sobre $\mathbf{C}$ es un grupo abeliano libre de rango igual al orden n del grupo.

Según la fórmula del teorema 3.8, todas las representaciones irreducibles de G son necesariamente de grado 1. Además, dos representaciones de grado 1 son equivalentes si y sólo si son iguales. Por consiguien-

te, una base del grupo abeliano libre $K_0(G, \mathbf{C})$ la forman los elementos de $\mathrm{Hom}_{\mathbf{Z}}(G, \mathbf{C}^*)$. La multiplicación en el anillo de representaciones $K_0(G, \mathbf{C})$ es la determinada por el producto de Kronecker en la base $\mathrm{Hom}_{\mathbf{Z}}(G, \mathbf{C}^*)$ que en este caso es el producto de funciones $(fg)(x) = f(x)g(x)$

Como es bien sabido, con la multiplicación anterior, $\mathrm{Hom}_{\mathbf{Z}}(G, \mathbf{C}^*)$ es isomorfo a G. Tenemos así:

Proposición 5.1. *El anillo de las representaciones de un grupo abeliano finito* G *sobre* **C**, $\mathrm{K}_0(\mathrm{G}, \mathbf{C})$, *es isomorfo al anillo de grupo* **Z**G.

En el anillo $\mathbf{Z}G = K_0(G, \mathbf{C})$ las sumas cuyos coeficientes son todos positivos, son los elementos que corresponden a las (clases de) representaciones.

Para complementar daremos un isomorfismo entre $\mathrm{Hom}_{\mathbf{Z}}(G, \mathbf{C}^*)$ y el grupo G.

Sea $G = G_1 \times \cdots \times G_h$ la descomposición de G como producto de grupos cíclicos de órdenes $n_1, n_2, \cdots, n_h = n$ respectivamente, tal que $n_1 | n_2,\ n_2 | n_3, \cdots, n_{h-1} | n_h$. Sean $x_1, x_2, \cdots, x_h$ generadores de G_1, $G_2, \cdots, G_h$. Consideremos ahora el grupo $Z \subset \mathbf{C}^*$ de las raíces n-ésimas de la unidad y un generador $z \in Z$. Sean $m_i = n/n_i$. Si $f \in \mathrm{Hom}_{\mathbf{Z}}(G, \mathbf{C}^*)$, $f(x_i)^{n_i} = 1$, de donde $f(x_i)$ es de la forma $f(x_i) = z^{m_i s_i}$ con $0 \leq m_i s_i \leq n - 1$. Podemos, entonces, definir $\theta: \mathrm{Hom}_{\mathbf{Z}}(G, \mathbf{C}^*) \to G$ mediante

$$\theta(f) = (x_1^{s_1}, x_2^{s_2}, \cdots, x_h^{s_h}).$$

Se debe comprobar que θ está bien definida, que es homomorfismo y que es biyectiva.

4. Representaciones de los grupos de simetrías de los polígonos regulares (grupos diédricos)

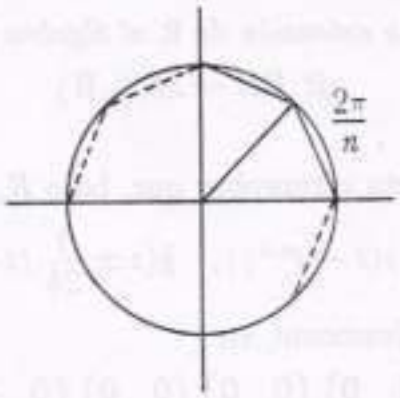
Denotaremos con D o D_n al grupo de simetrías de un polígono regular de n lados. D está generado por dos elementos s, t sujetos a las relaciones

$$s^2 = t^n = 1$$
$$sts = t^{n-1}.$$

Los elementos de D pueden, por tanto, escribirse como sigue:

$$D = \{1, t, t^2, \cdots, t^{n-1}, s, st, \cdots, st^{n-1}\}.$$

Si el polígono regular es



s es la reflexión alrededor del eje de las abscisas y t es la rotación de $2\pi/n$ alrededor del origen.

El elemento t genera un subgrupo cíclico T de D de orden n. Extenderemos ahora las representaciones que obtuvimos en las secciones anteriores para T sobre $\mathbf{R}$ a representaciones reales de D.

Sea $R:T \to GL(1,\mathbf{R})$ una representación de grado 1 de T. Definimos dos extensiones:

$$R', R'':D \to GL(1,\mathbf{R})$$

mediante las fórmulas

$$\begin{cases} R'(t) = R(t) \\ R'(s) = 1 \end{cases} \qquad \begin{cases} R''(t) = R(t) \\ R''(s) = -1, \end{cases}$$

las cuales, evidentemente, son representaciones.

Sea $R:T \to GL(2,\mathbf{R})$ la representación irreducible de grado 2 dada por

$$R(t) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \left(a = \cos\frac{2k\pi}{n},\ b = \operatorname{sen}\frac{2k\pi}{n},\ 0 < k < \frac{n}{2}\right).$$

Definimos en este caso una extensión que denotaremos con la misma letra

$$R:D \to GL(2,\mathbf{R})$$

mediante las fórmulas

$$\begin{cases} R(t) = R(t) \\ R(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{cases}$$

Las representaciones de D sobre $\mathbf{R}$ así obtenidas son irreducibles por serlo las de T. Para las de grado 2 tenemos:

Proposición 4.1. *La extensión de* R *al álgebra de grupo:*

$$R:\mathbf{R}D \to M(2,\mathbf{R})$$

es suprayectiva.

Demostración. Basta comprobar que, bajo R, los elementos

$$\tfrac{1}{2}(1 \pm \frac{1}{2b}s(t - t^{n-1})), \quad \tfrac{1}{2}(s \pm \frac{1}{2b}(t - t^{n-1})),$$

se transforma, respectivamente, en

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

Es conveniente observar que las representaciones irreducibles obtenidas, para D sobre $\mathbf{R}$ pueden considerarse también como representaciones de D sobre $\mathbf{C}$ y siguen siendo irreducibles.

Proposición 4.2. *Las representaciones de* D *sobre* C *antes definidas son irreducibles.*

Demostración. En efecto, la extensión de R a

$$R:\mathbf{C}D \to M(2,\mathbf{C})$$

es también suprayectiva y ya que $\mathbf{C}^2$ no tiene submódulos propios como $M(2,\mathbf{C})$-módulo, tampoco los tiene como $\mathbf{C}D$-módulo, por lo que R es irreducible.

Así pues, tanto sobre los reales como sobre los complejos hemos obtenido, en el caso impar, si $n = 2m + 1$, dos representaciones de grado 1 y m representaciones de grado 2 y, en el caso par, si $n = 2m$, cuatro de grado 1 y $m - 1$ de grado 2. De acuerdo con la fórmula de la suma de los cuadrados (proposición 3.8, capítulo 4), como

$$1 + 1 + 2^2 + \cdots + 2^2 = 2 + 4m = 2(2m + 1) = 2n$$

en el caso impar, y

$$1 + 1 + 1 + 1 + 2^2 + \cdots + 2^2 = 4 + 4(m - 1) = 4m = 2n,$$

en el caso par, se sigue que las representaciones mencionadas forman un sistema completo de representantes de clases de representaciones irreducibles de D sobre $\mathbf{C}$.

Además, según el corolario 4.10 del capítulo 4, el número de clases de representaciones irreducibles de D sobre $\mathbf{R}$ es menor o igual que el correspondiente sobre $\mathbf{C}$, con lo que hemos obtenido *todas* las clases de representaciones irreducibles de D sobre $\mathbf{R}$ y sobre $\mathbf{C}$. O sea:

Teorema 4.3. *El número de clases de representaciones irreducibles del grupo diédrico de orden* 2n *sobre* **R** *y sobre* **C** *es,*

$$\textit{cuando } n = 2m+1, \begin{cases} 2 \textit{ de grado } 1 \textit{ y} \\ m \textit{ de grado } 2; \end{cases}$$

$$\textit{cuando } n = 2m, \begin{cases} 4 \textit{ de grado } 1 \textit{ y} \\ m\text{-}1 \textit{ de grado } 2. \end{cases}$$

Éstas están dadas por:
De grado 1,

$$\begin{cases} R'_{(1)}(t) = 1 \\ R'_{(1)}(s) = 1 \end{cases} \qquad \begin{cases} R''_{(1)}(t) = 1 \\ R''_{(1)}(s) = -1 \end{cases}$$

y, sólo en el caso par,

$$\begin{cases} R'_{(-1)}(t) = -1 \\ R'_{(-1)}(s) = 1 \end{cases} \qquad \begin{cases} R''_{(-1)}(t) = -1 \\ R''_{(-1)}(s) = -1; \end{cases}$$

de grado 2,

$$\begin{cases} R_{(z)}(t) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad (z = a + bi) \\ R_{(z)}(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{cases}$$

con $z \neq \bar{z}$ *y* $(z) \in \bar{\bar{Z}}$, *conjunto de clases de equivalencia del grupo de raíces* n*-ésimas de la unidad con respecto a la conjugación.*

Además, en el caso complejo, para $R_{(z)}$ puede tomarse:

$$R_{(z)}(t) = \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$$

$$R_{(z)}(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (z \neq \bar{z})$$

5. Anillo de las representaciones de un grupo diédrico

De los resultados de la sección precedente se sigue que el grupo aditivo de los anillos $K_0(D, \mathbf{R})$ y $K_0(D, \mathbf{C})$ de las representaciones del grupo diédrico de orden $2n$ sobre los reales y los complejos, es un grupo abeliano libre de rango $m+2$ cuando $n = 2m+1$ y $m+3$ cuando $n = 2m$. En esta sección determinaremos la estructura multiplicativa de estos anillos que, como veremos a continuación, son isomorfos.

Proposición 5.1. *La inclusión* $\mathbf{R} \to \mathbf{C}$ *induce un isomorfismo* $K_0(D, \mathbf{R}) \cong K_0(D, \mathbf{C})$ *de los anillos de representaciones del grupo diédrico sobre* $\mathbf{R}$ *y sobre* $\mathbf{C}$.

Demostración. Si $R: D \to GL(n, \mathbf{R})$ es una representación, la composición de R con la inclusión $GL(n, \mathbf{R}) \subset GL(n, \mathbf{C})$ da una representación $D \to GL(n, \mathbf{C})$. Esto define una aplicación $K_0(D, \mathbf{R}) \to K_0(D, \mathbf{C})$ que es homomorfismo de anillos. Como bajo este homomorfismo la base que dimos en la sección 4 para las representaciones reales se transforma en la base, ahí también mencionada, para los complejos, éste resulta biyectivo.

Para calcular la tabla de multiplicación serán útiles las siguientes representaciones de grado 2 de D sobre $\mathbf{C}$:

$$\overline{R}_{(z)}(t) = \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$$

$$\overline{R}_{(z)}(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

en donde, como antes, (z) recorre el conjunto $\overline{Z}$ de clases de equivalencia del grupo Z de las raíces n-ésimas de la unidad con respecto a la conjugación. Así pues,

$$\overline{R}_{(z)} = R_{(z)} \qquad \text{para } z \neq \bar{z}$$

$$\overline{R}_{(z)} = R'_{(z)} \oplus R''_{(z)} \qquad \text{para } z = \bar{z}$$

(la segunda igualdad es, en realidad, en clases de equivalencia; pero seguiremos denotando con un mismo símbolo a una representación y a su clase de equivalencia). En efecto, la primera igualdad es la definición. La segunda se sigue de que

$$(R'_{(1)} \oplus R''_{(1)})(t) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$(R'_{(1)} \oplus R''_{(1)})(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

y (sólo en el caso par),

$$(R'_{(-1)} \oplus R''_{(-1)})(t) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$(R'_{(-1)} \oplus R''_{(-1)})(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

y de las relaciones

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Teorema 5.2. *El anillo* $\mathbf{K}_0(\mathbf{D}, \mathbf{C})$ *de las representaciones del grupo diédrico* $\mathbf{D}$ *de orden* $2n$ *sobre* $\mathbf{C}$ *es un grupo abeliano libre de rango*

$$\begin{array}{lll} m+2 & \textit{cuando} & n = 2m+1 \\ m+3 & \textit{cuando} & n = 2m \end{array}$$

con base

$$\mathbf{R}'_{(z)}, \mathbf{R}''_{(z)}, \mathbf{R}_{(z)} \quad ((z) \in \overline{\mathbf{Z}},\ z \neq \bar{z}) \textit{ cuando } n = 2m+1$$

o bien

$$\mathbf{R}'_{(z)}, \mathbf{R}''_{(z)}, \mathbf{R}'_{(-z)}, \mathbf{R}''_{(-z)}, \mathbf{R}_{(z)} \quad ((z) \in \overline{\mathbf{Z}},\ z \neq \bar{z}) \textit{ cuando } n = 2m$$

y con la multiplicación determinada por la tabla

	$\otimes$	$R'_{(1)}$	$R''_{(1)}$	$R'_{(-1)}$	$R''_{(-1)}$	$R_{(w)}$	$(w \neq \overline{w})$
	$R'_{(1)}$	$R'_{(1)}$	$R''_{(1)}$	$R'_{(-1)}$	$R''_{(-1)}$	$R_{(w)}$	
	$R''_{(1)}$		$R'_{(1)}$	$R''_{(-1)}$	$R'_{(-1)}$	$R_{(w)}$	
	$R'_{(-1)}$			$R'_{(1)}$	$R''_{(1)}$	$R_{(-w)}$	
	$R''_{(-1)}$				$R'_{(1)}$	$R_{(-w)}$	
$(z \neq \overline{z})$	$R_{(z)}$					$\overline{R}_{(zw)} \oplus \overline{R}_{(z\overline{w})}$	

($R'_{(-1)}$ y $R''_{(-1)}$ solamente en el caso par).

Demostración. El cálculo del producto de dos representaciones de grado uno es directo.

Para probar las fórmulas restantes demostraremos primero que

$$\overline{R}_{(z)} \otimes \overline{R}_{(w)} = \overline{R}_{(zw)} \oplus \overline{R}_{(z\overline{w})}.$$

Tenemos,

$$(\overline{R}_{(z)} \otimes \overline{R}_{(w)})(t) = \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix} \otimes \begin{pmatrix} w & 0 \\ 0 & \overline{w} \end{pmatrix} = \begin{pmatrix} zw & 0 & 0 & 0 \\ 0 & \overline{z}w & 0 & 0 \\ 0 & 0 & z\overline{w} & 0 \\ 0 & 0 & 0 & \overline{zw} \end{pmatrix}$$

$$(\overline{R}_{(z)} \otimes \overline{R}_{(w)})(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$(\overline{R}_{(zw)} \oplus \overline{R}_{(z\overline{w})})(t) = \begin{pmatrix} zw & 0 & 0 & 0 \\ 0 & \overline{zw} & 0 & 0 \\ 0 & 0 & z\overline{w} & 0 \\ 0 & 0 & 0 & \overline{z}w \end{pmatrix}$$

$$(\overline{R}_{(zw)} \oplus \overline{R}_{(z\overline{w})})(s) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Y las relaciones

$$\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}\begin{pmatrix}zw&0&0&0\\0&\bar{z}w&0&0\\0&0&z\bar{w}&0\\0&0&0&\bar{z}\bar{w}\end{pmatrix}=\begin{pmatrix}zw&0&0&0\\0&\bar{z}\bar{w}&0&0\\0&0&z\bar{w}&0\\0&0&0&\bar{z}w\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}$$

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

demuestran la fórmula.

La relación

$$R''_{(1)}\otimes R_{(w)}=R_{(w)}\qquad(w\neq\bar{w})$$

se sigue de que, por un lado,

$$\bar{R}_{(1)}\otimes\bar{R}_{(w)}=\bar{R}_{(w)}\oplus\bar{R}_{(\bar{w})}=2\bar{R}_{(w)}=2R_{(w)}$$

y, por otro,

$$\begin{aligned}\bar{R}_{(1)}\otimes\bar{R}_{(w)}&=(R'_{(1)}\oplus R''_{(1)})\otimes R_{(w)}\\&=R_{(w)}\oplus R''_{(1)}\otimes R_{(w)}.\end{aligned}$$

Demostraremos ahora que

$$R'_{(-1)}\otimes R_{(w)}=R_{(-w)},\qquad(w\neq\bar{w}).$$

Tenemos,

$$(R'_{(-1)}\otimes R_{(w)})(t)=\begin{pmatrix}-w&0\\0&-\bar{w}\end{pmatrix}$$

$$(R'_{(-1)}\otimes R_{(w)})(s)=\begin{pmatrix}0&-1\\-1&0\end{pmatrix}$$

$$R_{(-w)}(t)=\begin{pmatrix}-w&0\\0&-\bar{w}\end{pmatrix}$$

$$R_{(-w)}(s)=\begin{pmatrix}0&1\\1&0\end{pmatrix}.$$

Y las relaciones siguientes demuestran la fórmula:

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}-w & 0\\ 0 & -\overline{w}\end{pmatrix}=\begin{pmatrix}-w & 0\\ 0 & -\overline{w}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

La demostración de que

$$R''_{(-1)}\otimes R_{(w)}=R_{(-w)},\qquad (w\neq\overline{w})$$

es análoga a la de $R''_{(1)}\otimes R_{(w)}$.

6. Representaciones del grupo de los cuaternios

Denotaremos con H al grupo de los cuaternios. Sus ocho elementos son

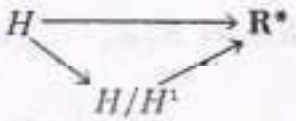
$$\{\pm 1, \pm i, \pm j, \pm k\}$$

con la multiplicación determinada por las relaciones usuales

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

Es fácil ver que el conmutador H^1 de H es $H^1=\{-1,1\}$ y que $H/H^1=T_2\times T_2$, producto directo de dos grupos cíclicos de orden 2.

Así pues, ya que todo homomorfismo de H en el grupo multiplicativo de los reales, puede factorizarse a través de H/H^1,



las representaciones de grado 1 de H sobre $\mathbf{R}$ quedan determinadas por los homomorfismos de $T_2\times T_2$ en $\mathbf{R}^*$. Hay cuatro de éstos y las cuatro representaciones reales así obtenidas de H son:

	± 1	$\pm i$	$\pm j$	$\pm k$
R_1	1	1	1	1
R_i	1	1	−1	−1
R_j	1	−1	1	−1
R_k	1	−1	−1	1

Observemos ahora que la partición de H en clases de conjugados es:

$$H = \{1\} \cup \{-1\} \cup \{i, -i\} \cup \{j, -j\} \cup \{k, -k\}.$$

Del teorema 4.9 y su corolario 4.10 del capítulo 4 se sigue, entonces, que el número de clases de representaciones irreducibles de H sobre $\mathbf{R}$ es menor o igual que 5. Daremos a continuación una representación irreducible (de grado 4) de H sobre $\mathbf{R}$ con lo cual quedarán determinadas todas las clases de representaciones irreducibles.

El grupo H podemos considerarlo como subgrupo del grupo de las unidades del álgebra de los cuaternios sobre el campo de los números reales. Ésta es un espacio vectorial de dimensión 4 sobre $\mathbf{R}$ con base $1, i, j, k$ y con la multiplicación determinada por las mismas relaciones de antes. A esta álgebra la denotaremos con $\mathbf{R}_H$. Es un álgebra (con 1) asociativa y con división.

La representación regular del álgebra $\mathbf{R}_H$, restringida al grupo $H \subset \mathbf{R}_H$ da la siguiente representación $S: H \to M(4, \mathbf{R})$:

$$S(\pm 1) = \pm \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad S(\pm i) = \pm \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$S(\pm j) = \pm \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \qquad S(\pm k) = \pm \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

El hecho de que el álgebra de los cuaternios $\mathbf{R}_H$ sea un álgebra con división implica que S es una representación irreducible de H sobre los reales.

Podemos entonces enunciar la

Proposición 6.1. *El grupo de los cuaternios tiene cinco clases de representaciones irreducibles sobre los reales. Éstas están determinadas por las representaciones* R_1, R_2, R_3, R_4, S, *siendo de grado uno las cuatro primeras y de grado cuatro la última.*

Para encontrar las representaciones de H sobre el campo de los números complejos observemos que las representaciones R_1, R_2, R_3, R_4 anteriores son también representaciones irreducibles de H sobre $\mathbf{C}$. Pero S, como representación sobre $\mathbf{C}$ ya no es irreducible. En efecto, si fuera

irreducible, la fórmula de la suma de cuadrados (proposición 3.8, capítulo 4) nos daría $1^2 + 1^2 + 1^2 + 1^2 + 4^2 = 8$, lo cual no es cierto. Esta misma fórmula nos indica que, debido a que no hay más representaciones de grado 1 de H, la única posibilidad es que haya una representación irreducible más y de grado 2:

$$1^2 + 1^2 + 1^2 + 1^2 + 2^2 = 8.$$

Nos será útil el álgebra $\mathbf{C}_H$ de los cuaternios sobre los complejos. La definición de $\mathbf{C}_H$ es análoga a la de $\mathbf{R}_H$. Para evitar confusiones denotaremos con $\sqrt{-1}$ al número complejo para distinguirlo del cuaternio i. Esta $\mathbf{C}$-álgebra $\mathbf{C}_H$, pensada como $\mathbf{R}$-álgebra contiene como subálgebra a $\mathbf{R}_H$.

Proposición 6.2. *El álgebra* $\mathbf{C}_H$ *de los cuaternios sobre* $\mathbf{C}$ *es isomorfa al álgebra de matrices* $\mathrm{M}(2, \mathbf{C})$.

Demostración. Buscaremos un $\mathbf{C}H$-módulo que nos dará una representación $T: H \to GL(2, \mathbf{C})$ y, al mismo tiempo, el isomorfismo de la proposición. Para ello construiremos un ideal I en $\mathbf{C}_H$ que resultará ser un $\mathbf{C}H$-módulo e irreducible.

Empezaremos encontrando un vector característico de la transformación lineal determinada por la multiplicación por el cuaternio i. La matriz asociada a i en la base $1, i, j, k$ es

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Su polinomio característico es $(x^2 + 1)^2$ y los vectores característicos correspondientes a la raíz característica, $\sqrt{-1}$, son los vectores $(a, b, c, d) = a + bi + cj + dk$ tales que

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \sqrt{-1} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

es decir, de la forma $(a, -\sqrt{-1}\, a, c, -\sqrt{-1}\, c)$. Consideremos uno de estos vectores característicos, por ejemplo, $u = 1 - \sqrt{-1}\, i$ y busquemos el ideal I de $\mathbf{C}_H$ generado por u. Si denotamos con $v \in I$ al elemento $v = ju$, se tienen las relaciones

$$iu = \sqrt{-1}\,u$$
$$ju = v$$
$$iv = -\sqrt{-1}\,v$$
$$jv = -u$$

de las cuales se deduce que I consta de los elementos de $\mathbf{C}_H$ de la forma

$$zu + z'v \text{ con } z, z' \in \mathbf{C}$$

Evidentemente I es un $\mathbf{C}H$-módulo y la representación matricial T asociada a éste, con respecto a la base u, v de $\mathbf{C}_H$ es

$$T(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ T(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix},$$

$$T(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ T(k) = \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}.$$

Esta representación determina la representación de la $\mathbf{C}$-álgebra $\mathbf{C}_H$:

$$x + yi + zj + wk \mapsto \begin{pmatrix} x + \sqrt{-1}\,y & -z - \sqrt{-1}\,w \\ z - \sqrt{-1}\,w & x - \sqrt{-1}\,y \end{pmatrix}.$$

Como las cuatro matrices anteriores son linealmente independientes se obtiene el isomorfismo de $\mathbf{C}$-álgebras $\mathbf{C}_H \cong M(2, \mathbf{C})$, con lo que queda demostrada la proposición.

Proposición 6.3. *La representación* $\mathrm{T}:\mathrm{H} \to \mathrm{M}(2, \mathbf{C})$ *dada por las fórmulas anteriores es irreducible.*

Demostración. Como el homomorfismo $\mathbf{C}H \to \mathbf{C}_H$ determinado por la inclusión de H en $\mathbf{C}_H$ es suprayectivo, los ideales izquierdos de $\mathbf{C}_H$ coinciden con los $\mathbf{C}H$-submódulos de $\mathbf{C}_H$. Por consiguiente, los ideales mínimos de $\mathbf{C}_H \cong M(2, \mathbf{C})$ son los que correspondan a los $\mathbf{C}H$-submódulos irreducibles de $M(2, \mathbf{C})$. Y, en nuestro caso, al $\mathbf{C}H$-módulo $I = \{zu + z'v | z, z' \in \mathbf{C}\}$ le corresponde el ideal de $M(2, \mathbf{C})$ formado por las matrices cuya segunda columna es 0, el cual es mínimo. En efecto,

$$u \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \sqrt{-1} \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

$$v \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \sqrt{-1}\begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix},$$

de donde

$$zu + z'v \mapsto \begin{pmatrix} 2z & 0 \\ 2z' & 0 \end{pmatrix}.$$

Lo anterior podemos resumirlo en la

Proposición 6.4. *El grupo de los cuaternios tiene cinco clases de representaciones irreducibles sobre los complejos. Éstas están determinadas por las representaciones* R_1, R_I, R_J, R_K, T, *siendo de grado uno las cuatro primeras y de grado dos la última.*

Terminaremos la sección con varias observaciones. La primera es que el isomorfismo de la proposición 6.2 da una representación del álgebra de los cuaternios reales $\mathbf{R}_H$ por medio de matrices complejas de 2×2. En efecto, la aplicación $\mathbf{C} \to \mathbf{R}_H$ determinada por $\sqrt{-1} \mapsto i$ permite pensar en $\mathbf{R}_H$ como en un espacio vectorial de dimensión 2 sobre $\mathbf{C}$. Así, todo cuaternio puede escribirse, de manera única, en la forma

$$z + z'j \qquad (z, z' \in \mathbf{C}).$$

Por consiguiente, la representación T determina la siguiente representación $\mathbf{R}_H \to M(2, \mathbf{C})$:

$$z + z'j \mapsto \begin{pmatrix} z & -z' \\ z' & z \end{pmatrix}, \qquad (z, z' \in \mathbf{C}).$$

Observemos que si $z + z'j \neq 0$, la matriz anterior es no singular, lo cual prueba, de paso, que el álgebra de los cuaternios $\mathbf{R}_H$ es un álgebra con división.

Finalmente observemos que si $z, z' \in \mathbf{R}$ se obtiene la representación usual de los complejos como matrices reales de 2×2:

$$a + b\sqrt{-1} \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

7. Anillo de las representaciones del grupo de los cuaternios

De los resultados de la sección anterior sabemos que el grupo aditivo de los anillos de las representaciones $K_0(H, \mathbf{R})$ y $K_0(H, \mathbf{C})$ del grupo

H de los cuaternios sobre los reales y complejos es un grupo abeliano libre con cinco generadores, R_1, R_i, R_j, R_k, S en el caso real y R_1, R_i, R_j, R_k, T en el caso complejo. En lo que sigue determinaremos la estructura multiplicativa de cada uno de estos anillos.

Empezaremos con el caso real. Un cálculo directo demuestra que para todo elemento h de H,

$$h\,R_i(h) = i\,h\,i^{-1}.$$

Por otro lado, ya que S es la restricción de la representación regular

$$\mathrm{reg}: \mathbf{R}_H \to M(4, \mathbf{R}),$$

se tiene que, para h en H,

$$\mathrm{reg}(h) = S(h),$$
$$\mathrm{reg}(h\,R_i(h)) = S(h) \otimes R_i(h)$$

(como antes $R_i(h) \in \mathbf{R} \subset \mathbf{R}_H$ con la inclusión $r \mapsto r1$). De lo anterior se sigue que las matrices

$$S(h) \text{ y } S(h) \otimes R_i(h)$$

son semejantes siendo $\mathrm{reg}(i)$ la matriz que da la semejanza. Con esto queda probado que

$$R_i \otimes S = S.$$

Razonamientos completamente análogos demuestran que

$$R_j \otimes S = S, \qquad R_k \otimes S = S.$$

Con esto y con las definiciones de las representaciones podemos elaborar la tabla de multiplicación para el anillo $K_0(H, \mathbf{R})$:

$\otimes$	R_1	R_i	R_j	R_k	S
R_1	R_1	R_i	R_j	R_k	S
R_i	R_i	R_1	R_k	R_j	S
R_j	R_j	R_k	R_1	R_i	S
R_k	R_k	R_j	R_i	R_1	S
S	S	S	S	S	$4(R_1 \oplus R_i \oplus R_j \oplus R_k)$

En ésta solamente nos falta probar que $S \otimes S = 4(R_1 \oplus R_i \oplus R_j \oplus R_k)$. Sabemos que (corolario 4.12, capítulo 4)

$$(R_1 \oplus R_i \oplus R_j \oplus R_k \oplus S)^2 = 8(R_1 \oplus R_i \oplus R_j \oplus R_k \oplus S),$$

o sea,

$$4(R_1 \oplus R_i \oplus R_j \oplus R_k) \oplus 8S \oplus S \otimes S = 8(R_1 \oplus R_i \oplus R_j \oplus R_k \oplus S)$$

de donde se sigue la fórmula.

Podemos así enunciar el

Teorema 7.1. *El anillo* $K_0(H, \mathbf{R})$ *de las representaciones del grupo de los cuaternios sobre el campo de los números reales es un grupo abeliano libre de rango* 5 *con base* R_1, R_i, R_j, R_k, S *y con la multiplicación determinada por la tabla anterior.*

Para el caso de las representaciones complejas de H un razonamiento análogo al del caso real demuestra que $R_i \otimes T = R_j \otimes T = R_k \otimes T = T$. Para calcular el valor de $T \otimes T$ seguimos también el mismo razonamiento de antes:

$$(R_1 \oplus R_i \oplus R_j \oplus R_k \oplus 2T)^2 = 4(R_1 \oplus R_i \oplus R_j \oplus R_k) \oplus 16T \oplus 4T \otimes T = 8(R_1 \oplus R_i \oplus R_j \oplus R_k \oplus 2T),$$

de donde,

$$T \otimes T = R_1 \oplus R_i \oplus R_j \oplus R_k$$

O sea,

Teorema 7.2. *El anillo* $K_0(H, \mathbf{C})$ *de las representaciones del grupo de los cuaternios sobre el campo de los números complejos es un grupo abeliano de rango* 5 *con base* R_1, R_i, R_j, R_k, T *y con la multiplicación determinada por la siguiente tabla:*

$\otimes$	R_1	R_i	R_j	R_k	T
R_1	R_1	R_i	R_j	R_k	T
R_i	R_i	R_1	R_k	R_j	T
R_j	R_j	R_k	R_1	R_i	T
R_k	R_k	R_j	R_i	R_1	T
T	T	T	T	T	$(R_1 \oplus R_i \oplus R_j \oplus R_k)$

8. Ejemplos: representaciones de grupos de orden pequeño

Daremos primero la lista completa de los anillos de las representaciones *complejas* de los grupos de orden menor que 12. Todos los resultados aquí reunidos han sido ya probados en párrafos anteriores.

8.1. Grupos de orden 1

El grupo $T_1 = \{1\}$ tiene una representación irreducible, la trivial, y el anillo

$$K_0(T_1, \mathbf{C}) \cong \mathbf{Z}.$$

8.2. Grupos de orden 2

El grupo $T_2 = \{1, t\}$ cíclico de orden 2 tiene dos clases de representaciones irreducibles, ambas de grado 1 dadas por

$$R_1(t) = 1, \qquad R_2(t) = 1.$$

La tabla de multiplicación es

$\otimes$	R_1	R_2
R_1	R_1	R_2
R_2	R_2	R_1

y el anillo

$$K_0(T_2, \mathbf{C}) \cong \mathbf{Z}\,T_2.$$

8.3. Grupos de orden 3

El grupo cíclico $T_3 = \{1, t, t^2\}$ tiene tres clases de representaciones irreducibles, de grado 1, dadas por

$$R_1(t) = 1,\ R_2(t) = w,\ R_3(t) = w^2$$

con $w = \exp\left(\frac{2\pi}{3} i\right)$.

La tabla de multiplicación es

$\otimes$	R_1	R_2	R_3
R_1	R_1	R_2	R_3
R_2	R_2	R_3	R_1
R_3	R_3	R_1	R_2

y el anillo de las representaciones.

$$K_0(T_3, \mathbf{C}) \cong \mathbf{Z}\,T_3.$$

8.4. Grupos de orden 4

Hay dos grupos de orden 4, T_4 y $T_2 \times T_2$.

8.4.1. $T_4 = \{1, t, t^2, t^3\}$ tiene cuatro clases de representaciones irreducibles, de grado 1, dadas por

$$R_1(t) = 1,\ R_i(t) = i,\ R_{-1}(t) = -1,\ R_{-i}(t) = -i$$

con la multiplicación

$\otimes$	R_1	R_i	R_{-1}	R_{-i}
R_1	R_1	R_i	R_{-1}	R_{-i}
R_i	R_i	R_{-1}	R_{-i}	R_1
R_{-1}	R_{-1}	R_{-i}	R_1	R_i
R_{-i}	R_{-i}	R_1	R_i	R_{-1}

y el anillo

$$K_0(T_4, \mathbf{C}) \cong \mathbf{Z}\, T_4.$$

8.4.2. $T_2 \times T_2 = \{(1,1), (t,1), (1,t), (t,t)\}$ tiene cuatro clases de representaciones irreducibles, de grado 1, $R_{(1,1)}$, $R_{(t,1)}$, $R_{(1,t)}$, $R_{(t,t)}$ dadas por la tabla de valores

	$(t,1)$	$(1,t)$
$R_{(1,1)}$	1	1
$R_{(t,1)}$	-1	1
$R_{(1,t)}$	1	-1
$R_{(t,t)}$	-1	-1

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \qquad (g, g' \in T_2 \times T_2).$$

Y, como anillos,

$$K_0(T_2 \times T_2, \mathbf{C}) \cong \mathbf{Z}(T_2 \times T_2).$$

8.5. Grupos de orden 5. $T_5 = \{1, t, t^2, t^3, t^4\}$ tiene cinco clases de representaciones, de grado 1, dadas por

$$R_k(t) = z^k \qquad \left(z = \exp\left(\frac{2\pi}{5} i\right),\ 0 \le k \le 4\right)$$

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \qquad (g, g' \in T_5)$$

y el anillo

$$K_0(T_5, \mathbf{C}) \cong \mathbf{Z}\, T_5.$$

8.6. Grupos de orden 6

Hay dos grupos de orden 6, T_6 y $D_3 = S_3$ (el diédrico, que en este caso coincide con el simétrico).

8.6.1. $T_6 = \{1, t, \ldots, t^5\}$ tiene 6 clases de representaciones irreducibles, dadas por

$$R_{ik}(t) = z^k \qquad \left(z = \exp\left(\frac{2\pi}{6} i\right),\ 0 \leq k \leq 5\right).$$

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \qquad (g, g' \in T_6)$$

y el anillo

$$K_0(T_6, \mathbf{C}) \cong \mathbf{Z}\, T_6.$$

8.6.2. $D_3 = \{1, t, t^2, s, st, st^2\}$ tiene dos clases de representaciones irreducibles de grado 1 y una de grado 2:

	t	s
R'	1	1
R''	1	-1
S	$\begin{pmatrix} w & 0 \\ 0 & \overline{w} \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

La multiplicación es

$\otimes$	R'	R''	S
R'	R'	R''	S
R''	R''	R'	S
S	S	S	$(R' \oplus R'' \oplus S)$

El anillo de las representaciones

$$K_0(D_3, \mathbf{C}) \cong \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \text{ (como grupos abelianos)}$$

con base R', R'', S y el producto anteriormente definido.

8.7. Grupos de orden 7

$T_7 = \{1, t, \cdots, t^6\}$ tiene 7 clases de representaciones irreducibles de grado 1,

$$R_k(t) = z^k \qquad \left(z = \exp\left(\frac{2\pi}{7} i\right),\ 0 \leq k \leq 6\right).$$

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \quad (g, g' \in T_7)$$

y el anillo

$$K_0(T_7, \mathbf{C}) \cong \mathbf{Z}\, T_7.$$

8.8. Grupos de orden 8

Hay cinco grupos de orden 8: T_8, $T_2 \times T_4$, $T_2 \times T_2 \times T_2$, D_4 y el grupo H de los cuaternios.

8.8.1. $T = (1, t, \ldots, t^7)$ tiene 8 clases de representaciones irreducibles, de grado 1,

$$R_k(t) = z^k \qquad \left(z = \exp\left(\frac{\pi}{4} i\right),\ 0 \leq k \leq 7\right).$$

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \quad (g, g' \in T_8)$$

y el anillo

$$K_0(T_8, \mathbf{C}) \cong \mathbf{Z}\, T_8.$$

8.8.2. $T_2 \times T_4 = \{(1,1), (1,s), (1,s^2), (1,s^3), (t,1), (t,s), (t,s^2), (t,s^3)\}$ tiene ocho clases de representaciones irreducibles, $T_g (g \in T_2 \times T_4)$, de grado 1, con la tabla de valores:

	$(t,1)$	$(1,s)$
$R_{(1,1)}$	1	1
$R_{(1,s)}$	i	1
$R_{(1,s^2)}$	-1	1
$R_{(1,s^3)}$	$-i$	1
$R_{(t,1)}$	1	-1
$R_{(t,s)}$	i	-1
$R_{(t,s^2)}$	-1	-1
$R_{(t,s^3)}$	$-i$	-1

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \quad (g, g' \in T_2 \times T_4)$$

y el anillo

$$K_0(T_2 \times T_4, \mathbf{C}) \cong \mathbf{Z}(T_2 \times T_4).$$

8.8.3. $T_2 \times T_2 \times T_2 = \{(1, 1, 1), (1, 1, t), (1, t, 1), (1, t, t), (t, 1, 1), (t, 1, t), (t, t, 1), (t, t, t)\}$ tiene ocho clases de representaciones irreducibles $R_g (g \in T_2 \times T_2 \times T_2)$, de grado 1, dadas por la tabla de valores:

	$(t,1,1)$	$(1,t,1)$	$(1,1,t)$
$R_{(1,1,1)}$	1	1	1
$R_{(1,1,t)}$	1	1	−1
$R_{(1,t,1)}$	1	−1	1
$R_{(1,t,t)}$	1	−1	−1
$R_{(t,1,1)}$	−1	1	1
$R_{(t,1,t)}$	−1	1	−1
$R_{(t,t,1)}$	−1	−1	1
$R_{(t,t,t)}$	−1	−1	−1

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \quad (g, g' \in T_2 \times T_2 \times T_2)$$

y el anillo

$$K_0(T_2 \times T_2 \times T_2, \mathbf{C}) \cong \mathbf{Z}(T_2 \times T_2 \times T_2).$$

8.8.4. El grupo D_4 de simetrías del cuadrado

$$D_4 = \{1, t, t^2, t^3, s, st, st^2, st^3\}$$

tiene cuatro clases de representaciones irreducibles de grado 1 y una de grado 2:

	t	s
R'_1	1	1
R''_1	1	-1
R'_{-1}	-1	1
R''_{-1}	-1	-1
R_i	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

La tabla de multiplicar es

$\otimes$	R'_1	R''_1	R'_{-1}	R''_{-1}	R_i
R'_1	R'_1	R''_1	R'_{-1}	R''_{-1}	R_i
R''_1		R'_1	R''_{-1}	R'_{-1}	R_i
R'_{-1}			R'_1	R''_1	R_i
R''_{-1}				R'_1	R_i
R_i					$(R'_1 \oplus R''_1 \oplus R'_{-1} \oplus R''_{-1})$

El anillo de las representaciones

$$K_0(D_4, \mathbf{C}) \cong \mathbf{Z}^5$$

(como grupos abelianos) con el producto dado por la tabla anterior.

8.8.5. El grupo de los cuaternios

$$H = \{\pm 1, \pm i, \pm j, \pm k\}$$

tiene cinco clases de representaciones irreducibles, sobre $\mathbf{C}$, cuatro de grado 1 y una de grado 2, dadas por la tabla de valores:

	± 1	$\pm i$	$\pm j$	$\pm k$
R_1	1	1	1	1
R_i	1	1	-1	-1
R_j	1	-1	1	-1
R_k	1	-1	-1	1
T	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}$

La tabla de multiplicación es

$\otimes$	R_1	R_i	R_j	R_k	T
R_1	R_1	R_i	R_j	R_k	T
R_i	R_i	R_1	R_k	R_j	T
R_j	R_j	R_k	R_1	R_i	T
R_k	R_k	R_j	R_i	R_1	T
T	T	T	T	T	$(R_1 \oplus R_i \oplus R_j \oplus R_k)$

El anillo de las representaciones

$$K_0(H, \mathbf{C}) \cong \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \text{ (como grupos abelianos)}$$

con base R_1, R_i, R_j, R_k, T y el producto dado por la tabla anterior.

8.9. Grupos de orden 9

Hay dos grupos de orden 9, T_9 y $T_3 \times T_3$.

8.9.1. $T_9 = \{1, t, t^2, \ldots, t^8\}$ tiene nueve clases de representaciones irreducibles, de grado 1,

$$R_k(t) = z^k \qquad \left(z = \left(\frac{2\pi}{9} i\right), \quad 0 \leq k \leq 8\right).$$

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \quad (g, g' \in T_9)$$

y el anillo

$$K_0(T_9, \mathbf{C}) \cong \mathbf{Z}T_9.$$

8.9.2. $T_3 \times T_3 = \{(1,1)\ (1,t),\ (1,t^2),\ (t,1),\ (t,t),\ (t,t^2),\ (t^2,1)\ (t^2,t),\ (t^2,t^2)\}$ tiene nueve clases de representaciones irreduciles, de grado 1, dadas por:

	$(t,1)$	$(1,t)$
$R_{(1,1)}$	1	1
$R_{(1,t)}$	1	w
$R_{(1,t^2)}$	1	w^2
$R_{(t,1)}$	w	1
$R_{(t,t)}$	w	w
$R_{(t,t^2)}$	w	w^2
$R_{(t^2,1)}$	w^2	1
$R_{(t^2,t)}$	w^2	w
$R_{(t^2,t^2)}$	w^2	w^2

$\left(w = \exp\left(\frac{2\pi}{3} i\right)\right)$

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \quad (g, g' \in T_3 \times T_3)$$

y el anillo

$$K_0(T_3 \times T_3, \mathbf{C}) \cong \mathbf{Z}(T_3 \times T_3).$$

8.10. Grupos de orden 10

Hay dos grupos de orden 10, T_{10} y el grupo diédrico D_5 (de permutaciones de un pentágono regular).

8.10.1. $T_{10} = \{1, t, t^2, \ldots, t^9\}$ tiene 10 clases de representaciones irreducibles, de grado 1,

$$R_k(t) = z^k \qquad \left(z = \exp\left(\frac{2\pi}{10} i\right), \quad 0 \leq k \leq 9\right).$$

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \quad (g, g' \in T_{10})$$

y el anillo

$$K_0(T_{10}, \mathbf{C}) \cong \mathbf{Z}\, T_{10}.$$

8.10.2. $D_5 = \{1, t, t^2, t^3, t^4, s, st, st^2, st^3, st^4\}$ tiene 4 clases de representaciones irreducibles R_1, R_2, R_3, R_4, de grado 1 las dos primeras y de grado 2 las dos últimas:

	s	t
R_1	1	1
R_2	1	-1
R_3	$\begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
R_4	$\begin{pmatrix} z^2 & 0 \\ 0 & \bar{z}^2 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\left(z = \exp\left(\frac{2\pi}{10} i\right)\right)$

La multiplicación es

$\otimes$	R_1	R_2	R_3	R_4
R_1	R_1	R_2	R_3	R_4
R_2	R_2	R_1	R_3	R_4
R_3	R_3	R_3	$(R_1 \oplus R_2 \oplus R_4)$	$(R_3 \oplus R_4)$
R_4	R_4	R_4	$(R_3 \oplus R_4)$	$(R_1 \oplus R_2 \oplus R_3)$

El anillo

$$K_0(D_5, \mathbf{C}) \cong \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$$

como grupos abelianos y el producto de la tabla anterior.

8.11. Grupos de orden 11

$T_{11} = \{1, t, \ldots, t^{10}\}$ tiene 11 clases de representaciones irreducibles, de grado 1,

$$R_{t^k}(t) = z^k \qquad (z = \exp\frac{2\pi}{11} i, \quad 0 \leq k \leq 10).$$

La multiplicación es

$$R_g \otimes R_{g'} = R_{gg'} \quad (g, g' \in T_{11})$$

y el anillo

$$K_0(T_{11}, \mathbf{C}) \cong \mathbf{Z}\, T_{11}.$$

Finalmente daremos dos ejemplos de representaciones reales.

Representaciones de T_9 *sobre* $\mathbf{R}$. Hay 5 clases de representaciones irreducibles de $T_9 = \{1, t, \ldots, t^8\}$ sobre $\mathbf{R}$,

$$R_{(1)}, R_{(s)}, R_{(s^2)}, R_{(s^3)}, R_{(s^4)},$$

que, por comodidad, pueden denotarse

$$R_0, R_1, R_2, R_3, R_4,$$

dadas por:

$$R_0(t) = 1$$

$$R_i(t) = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}, \quad a_i = \cos\frac{2\pi}{9}, \quad b_i = \operatorname{sen}\frac{2\pi}{9},$$

$(1 \leq i \leq 4)$. El anillo $K_0(T, \mathbf{R})$ es el grupo abeliano libre con base R_0, R_1, R_2, R_3, R_4 y la multiplicación

$\otimes$	R_0	R_1	R_2	R_3	R_4
R_0	R_0	R_1	R_2	R_3	R_4
R_1		$2R_0 \oplus R_2$	$R_1 \oplus R_3$	$R_2 \oplus R_4$	$R_3 \oplus R_4$
R_2			$2R_0 \oplus R_4$	$R_1 \oplus R_4$	$R_2 \oplus R_3$
R_3				$2R_0 \oplus R_3$	$R_1 \oplus R_2$
R_4					$2R_0 \oplus R_1$.

Representaciones del grupo diédrico de orden 12 *sobre* $\mathbf{R}$. El grupo de simetrías del exágono regular es $D_6 = \{1, t, \ldots, t^5, s, st, \ldots, st^5\}$. D_6 tiene 6 representaciones sobre $\mathbf{R}$:

	t	s	
R_1	1	1	
R_2	1	-1	
R_3	-1	1	
R_4	-1	-1	
R_5	$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$a = \cos\frac{\pi}{3}, \quad b = \operatorname{sen}\frac{\pi}{3}$
R_6	$\begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$a' = \cos\frac{2\pi}{3}, \quad b' = \operatorname{sen}\frac{2\pi}{3}$

El anillo de las representaciones

$$K_0(D_6, \mathbf{R}) \cong \mathbf{Z}^6$$

como grupo abeliano y con la multiplicación

$\otimes$	R_1	R_2	R_3	R_4	R_5	R_6
R_1	R_1	R_2	R_3	R_4	R_5	R_6
R_2		R_1	R_4	R_3	R_5	R_6
R_3			R_1	R_2	R_6	R_5
R_4				R_1	R_6	R_5
R_5					$(R_5 \oplus R_6)$	$(R_5 \oplus R_4 \oplus R_5)$
R_6						$(R_1 \oplus R_2 \oplus R_6)$

9. Algunas álgebras de grupo

En esta sección daremos la descomposición del álgebra de grupo de algunos grupos finitos como producto de álgebras simples. Los resultados han sido ya probados en las secciones anteriores de este capítulo.

9.1. Grupos abelianos (sobre $\mathbf{C}$).

Si G es un grupo abeliano de orden n,

$$\mathbf{C}G = \mathbf{C} \times \mathbf{C} \times \cdots \times \mathbf{C}, \quad (n \text{ factores}).$$

9.2. Grupos cíclicos (sobre $\mathbf{R}$).

Si T es un grupo cíclico de orden impar $2m + 1$,

$$\mathbf{R}T = \mathbf{R} \times \underbrace{\mathbf{C} \times \mathbf{C} \times \cdots \times \mathbf{C}}_{m \text{ factores}}$$

y si T es de orden par $2m$,

$$\mathbf{R}T = \mathbf{R} \times \mathbf{R} \times \underbrace{\mathbf{C} \times \mathbf{C} \times \cdots \times \mathbf{C}}_{m\text{-}1 \text{ factores}}$$

9.3. Grupos diédricos (sobre $\mathbf{C}$)

Si D es el grupo de las simetrías de un polígono regular de n lados y $n = 2m + 1$,

$$\mathbf{C}D = \mathbf{C} \times \mathbf{C} \times \underbrace{M(2, \mathbf{R}) \times \cdots \times M(2, \mathbf{R})}_{m \text{ factores}}$$

y si $n = 2m$,

$$\mathbf{C}D = \mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \underbrace{M(2,\mathbf{R}) \times \cdots \times M(2,\mathbf{R})}_{m\text{-}1 \text{ factores}}$$

9.4. Grupos diédricos (sobre $\mathbf{R}$).

Si D es el grupo de las simetrías de un polígono regular de n lados y $n = 2m + 1$,

$$\mathbf{R}D = \mathbf{R} \times \mathbf{R} \times \underbrace{\mathbf{C} \times \cdots \times \mathbf{C}}_{m \text{ factores}}$$

y si $n = 2m$,

$$\mathbf{R}D = \mathbf{R} \times \mathbf{R} \times \mathbf{R} \times \mathbf{R} \times \underbrace{\mathbf{C} \times \cdots \times \mathbf{C}}_{m\text{-}1 \text{ factores}}$$

9.5. El grupo de los cuaternios (sobre $\mathbf{C}$).

Si H es el grupo de los cuaternios,

$$\mathbf{C}H = \mathbf{C} \times \mathbf{C} \times \mathbf{C} \times \mathbf{C} \times M(2,\mathbf{C}).$$

9.6. El grupo de los cuaternios (sobre $\mathbf{R}$)

$$\mathbf{R}H = \mathbf{R} \times \mathbf{R} \times \mathbf{R} \times \mathbf{R} \times \mathbf{R}_H,$$

en donde $\mathbf{R}_H$ es el álgebra de los cuaternios sobre $\mathbf{R}$.

INDICE ANALITICO

A

Álgebra, 45, 48, 49
  con división, 54
  de grupo, 122
  de un grupo, 47
  envolvente, 49
Anillo:
  de Grothendieck, de las representaciones, 75, 77
  semisimple, 60
  simple, 65
Aplicación bilineal, 10, 29
Artin, 20

B

Base, 18
  de un monoide, 77

C

Cadena:
  ascendente, 20
  descendente, 21
Centro, 86
Composición, 10
Conmutador, 54

E

$\mathrm{End}_K(V)$, 39
Epimorfismo, 11
Espacio de una representación, 39
  vectorial, 9

F

Función:
  inyectiva, 11
  suprayectiva, 11

G

$GL(n, K)$, 40
$GL_K(V)$, 39
Grado de una representación, 39
Grupo:
  abeliano, 95
  cíclico, 89, 93
  de Grothendieck, 76
  de los cuaternios, 104, 108
  de simetrías, 96

H

Hom, 10
Homomorfismo, 10

I

Ideal nilpotente, 64
Im, 11
Imagen, 11
Isomorfismo, 11:
  primer teorema, 13
  segundo teorema, 13
  tercer teorema, 14

J

Jordan-Hölder, 25

K

Ker, 11
KG, 46
K^G, 46
Kronecker, 37
Krull-Schmidt, 27

L

Lema de Schur, 80
Longitud de un módulo, 24
  de una serie de composición, 22

M

Maschke, 78
Matriz, 35
$M(m \times n, K)$, 35
$Mm(K)$, 35
Módulo, 9, 48:
  artiniano, 21
  cociente, 12
  correspondiente a una representación, 50
  derecho, 9
  inescindible, 25
  irreducible, 22, 54
  izquierdo, 9
  libre, 18
  máximo (existencia), 22
  noetheriano, 20
  proyectivo, 19
  semisimple, 59
  simple, 22
  sobre un álgebra, 46, 47, 48
Monomorfismo, 11

N

Nakayama, 62
Nilideal, 64
Noether, 20
Núcleo, 11

P

Producto de Kronecker, 37, 43
  de representaciones, 43, 53
  directo de módulos, 14
  tensorial de homomorfismos, 31
  tensorial de módulos, 29, 34
Propiedad universal:
  de la suma directa, 16
  del producto directo, 15
  del producto tensorial, 30

R

Radical de un anillo, 62
  de un módulo, 62
Representación asociada a un KG-módulo, 50
  fiel, 39
  grado de, 39
  inducida, 55
Representación irreducible, 54
  matricial, 40
  matricial asociada, 51
  por endomorfismos, 39
  regular, 58
  trivial, 39

Representaciones:
equivalentes, 41, 51
regulares, 86
Restricción de una representación, 55

S

Schur, 54, 80
Serie de composición, 22
equivalente, 24
Submódulo, 11
finitamente generable, 21
generado por, 13
Sucesión de homomorfismos, 11
escindible, 18
exacta, 11
Suma de representaciones, 43, 52
directa de módulos, 16

T

Teorema de:
Burnside, 80, 82
Frobenius, 80, 83
Maschke, 78, 79
Transformación lineal, 35

W

Wedderburn, 73

Esta obra terminó de imprimirse el día 2 de enero de 1970, en los talleres de Programex Editora, S. A., Mesones 62-E, México 1, D. F.

Se tiraron 2 000 ejemplares