serie de matemática

monografía no. 12

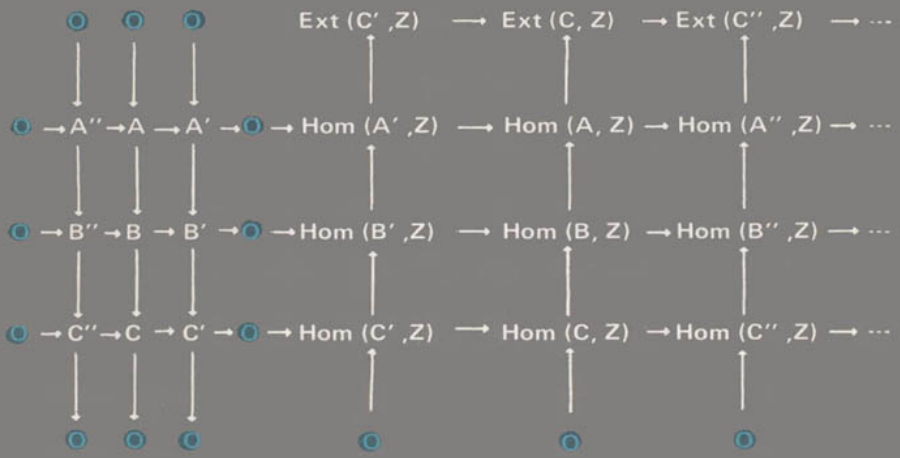
ESTRUCTURAS ALGEBRAICAS, II

Programa Regional de Desarrollo Científico y Tecnológico

Departamento de Asuntos Científicos

Secretaría General de la

Organización de los Estados Americanos



ESTRUCTURAS ALGEBRAICAS, II

(álgebra lineal)

por

ENZO R. GENTILE

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Buenos Aires, Argentina

Programa Regional de Desarrollo Científico y Tecnológico
Departamento de Asuntos Científicos
Secretaría General de la
Organización de los Estados Americanos
Washington, D.C.

Esta monografía ha sido preparada para su publicación en el Departamento de Asuntos Científicos de la Secretaría General de la Organización de los Estados Americanos.

Editora: Eva V. Chesneau

Asesor Técnico: Dr. Mario O. González
Departamento de Matemáticas
Universidad de Alabama
University, Alabama, Estados Unidos

A los lectores

El programa de monografías científicas es una faceta de la vasta labor de la Organización de los Estados Americanos, a cargo del Departamento de Asuntos Científicos de la Secretaría General de dicha Organización, a cuyo financiamiento contribuye en forma importante el Programa Regional de Desarrollo Científico y Tecnológico.

Concebido por los Jefes de Estado Americanos en su Reunión celebrada en Punta del Este, Uruguay, en 1967, y cristalizado en las deliberaciones y mandatos de la Quinta Reunión del Consejo Interamericano Cultural, llevada a cabo en Maracay, Venezuela, en 1968, el Programa Regional de Desarrollo Científico y Tecnológico es la expresión de las aspiraciones preconizadas por los Jefes de Estado Americanos en el sentido de poner la ciencia y la tecnología al servicio de los pueblos latinoamericanos.

Demostrando gran visión, tal altas autoridades reconocieron que la ciencia y la tecnología están transformando la estructura económica y social de muchas naciones y que, en esta hora, por ser instrumento indispensable de progreso en América Latina, necesitan un impulso sin precedentes.

El Programa Regional de Desarrollo Científico y Tecnológico es un complemento de los esfuerzos nacionales de los países latinoamericanos y se orienta hacia la adopción de medidas que permitan el fomento de la investigación, la enseñanza y la difusión de la ciencia y la tecnología; la formación y perfeccionamiento de personal científico; el intercambio de informaciones, y la transferencia y adaptación a los países latinoamericanos del conocimiento y las tecnologías generadas en otras regiones.

En el cumplimiento de estas premisas fundamentales, el programa de monografías representa una contribución directa a la enseñanza de las ciencias en niveles educativos que abarcan importantísimos sectores de la población y, al mismo tiempo, propugna la difusión del saber científico.

La colección de monografías científicas consta de cuatro series, en español y portugués, sobre temas de física, química, biología y matemática. Desde sus comienzos, estas obras se destinaron a profesores y alumnos de ciencias de enseñanza secundaria y de los primeros años de la universitaria; de éstos se tiene ya testimonio de su buena acogida.

Este prefacio brinda al Programa Regional de Desarrollo Científico y Tecnológico y a la Secretaría General de la Organización de los Estados Americanos la ocasión de agradecer al doctor Enzo R. Gentile, autor de esta monografía, y a quienes tengan el interés y buena voluntad de contribuir a su divulgación.

junio de 1971

NOTA DE INTRODUCCIÓN

En nuestra primer monografía sobre Estructuras Algebraicas estudiamos las propiedades generales de las leyes de composición y las propiedades elementales de grupos y anillos. El material allí tratado constituye una introducción a temas de la llamada álgebra moderna. Una forma natural de continuar este estudio podría ser profundizar los mismos temas. Por ejemplo, estudiar con más detalle la estructura de grupo, encarando los grupos finitos, los grupos de permutaciones, los teoremas de Sylow. Así mismo, se podría intensificar el estudio de ciertos ejemplos importantes de anillos, como son los anillos de polinomios, anillos de matrices, anillos noetherianos e ideales. Todo esto sería, sin dudas, una sana y estimulante labor a desarrollar. Sin embargo, nos parece más interesante encarar un proyecto mucho más ambicioso, que es el de hacer franca irrupción en el álgebra moderna, mediante el desarrollo sistemático de la *teoría de módulos*. La estructura de módulo generaliza naturalmente las estructuras de grupo y anillo. Y así, los grupos abelianos y los espacios vectoriales constituyen ejemplos importantes de módulos.

El desarrollo reciente de la matemática muestra la importancia y resonancia del álgebra en dicho desarrollo. La llamada *Álgebra homológica* puede considerarse su centro de irradiación. En ésta, lo más importante es precisamente la noción de módulo sobre un anillo, o más técnicamente, "la categoría de módulos sobre un anillo". En la actualidad, analistas y topólogos trabajan con módulos sobre anillos de funciones (continuas, diferenciables, analíticas, etc.), los geómetras con módulos sobre los más variados anillos conmutativos. La teoría algebraica de números clásica se encara hoy estudiando los módulos sobre distintos anillos aritméticos, en combinación con K-teoría, cohomología galoisiana, "projective class group", etc.

Pensamos que el adoptar el punto de vista de la teoría de módulos en esta monografía nos permite efectuar un avance más pronunciado y de mayores perspectivas futuras. Por ejemplo, conociendo la teoría de módulos se puede enriquecer y dar un significado especial al estudio de grupos finitos, "vía" la teoría de representación (véase, por ejemplo, (6) y (21a)). Igualmente, los métodos del álgebra homológica resultan de gran utilidad para estudiar grupos abelianos infinitos (véase, por ejemplo, (7b)).

El material aquí presentado, asimilado satisfactoriamente por el lector, le permitirá encarar el estudio serio de variados temas de la matemática actual. Hasta podríamos decir tal vez que ese material constituye una introducción al lenguaje de la matemática moderna.

A lo largo del texto, se ha tratado de ilustrar en forma sistemática las nociones introducidas con ejemplos, notas, etc. Para ello nos he-

mos valido fundamentalmente de la típica estructura de módulo, que es la de grupo abeliano. Observe el lector que en una monografía de este tipo es fácil caer en la enfermedad actual de la enseñanza de la matemática (y aun de la investigación matemática), que es: "la generalidad por la generalidad", o en lo que se ha dado en llamar "abstract nonsense". Se aconseja decididamente que al terminar el estudio de esta monografía se profundice temas de corte más clásico que permitan afianzar las ideas y métodos desarrollados. Esto estimulará y beneficiará el trabajo posterior, y evitará contraer la enfermedad de la generalidad, verdadero azote de la matemática actual.

En vista de lo anterior, convendría hacer las siguientes sugerencias: a) Léase con más detenimiento grupos abelianos infinitos, donde abundan las ideas y métodos elementales. Para ello el librito de Kaplansky (15) o algún capítulo de Fuchs (7a) (por ejemplo, el de grupos abelianos sin torsión) son altamente aconsejables. b) Estúdiese la teoría algegraica de números, que es una fuente de ejemplos importantes estrechamente vinculados con la aritmética. Al final de la monografía se da referencias al respecto.

La monografía adolece de una omisión fundamental referente al producto tensorial. Este tema debió excluirse a fin de no extender demasiado la obra. El lector debe estudiarlo, y en este sentido le aconsejamos el libro de Chevalley (5) y/o Bourbaki (3c). Las ideas y métodos de estudio del producto tensorial son similares a las expuestas en este tra-
VI bajo, por lo que el interesado no tendrá mayores dificultades en estudiar el tema por sí mismo.

Una aplicación importante de la teoría de módulos es la relativa al estudio de la teoría de una transformación lineal definida sobre un espacio vectorial. Es éste un ejemplo distinto y fecundo, en que la teoría muestra su real poder. Se basa en considerar el espacio vectorial como un módulo sobre el anillo de polinomios "vía" la transformación lineal dada. Si el espacio vectorial es de dimensión finita, entonces encaja exactamente en la teoría de módulos de tipo finito sobre un dominio principal, la cual se conoce perfectamente. Esto posibilita clasificar las transformaciones lineales sobre un espacio vectorial de dimensión finita.

En general, el problema clave de la teoría de módulos consiste en: dado un anillo, caracterizar diversas categorías de módulos sobre dicho anillo, por ejemplo, la categoría de módulos proyectivos de tipo finito. Este estudio ha sido unificado y enmarcado dentro de teorías generales, como son la K-teoría. En la actualidad es febril la actividad matemática sobre estas cuestiones.

Para finalizar deseamos expresar nuestro sincero agradecimiento al Departamento de Asuntos Científicos de la Organización de los Estados Americanos por habernos invitado a escribir esta Segunda Parte de Estructuras Algebraicas. Es nuestra esperanza que la misma sea de utilidad en América Latina.

ÍNDICE

1

ESTRUCTURA DE MÓDULO SOBRE UN ANILLO

1. DEFINICIONES Y PRIMERAS PROPIEDADES

Sea R un anillo con identidad $1 \neq 0$ y sea A un grupo abeliano. Denotemos por End(A) el anillo de endomorfismos de A, es decir el conjunto de todos los morfismos de A en A, dotado de la estructura de anillo definida por las leyes de composición ($a \in A$)

$$(f + g)(a) = f(a) + g(a)$$

$$(f \cdot g)(a) = f(g(a)).$$

Por $I = id_A$ denotaremos el elemento neutro o identidad de End(A).

Definición 1.1.1. Se llama *representación* de R a todo morfismo de anillos

$$\rho : R \to End(A)$$

Entonces, para cada $r \in R$, $\rho(r)$ es un morfismo de A y se satisfacen las propiedades

$$(*) \qquad \begin{aligned} \rho(r_1 + r_2) &= \rho(r_1) + \rho(r_2) \\ \rho(r_1 \cdot r_2) &= \rho(r_1) \cdot \rho(r_2) \\ \rho(1) &= I. \end{aligned}$$

En estas condiciones decimos también que R *opera* sobre A y que los elementos de R son *operadores* de A, y basándonos en esta observación escribimos

$$\rho(r)(a) = r \cdot a$$

El hecho que $\rho(r)$ sea un morfismo de A se traduce en la propiedad

$$m1) \qquad r \cdot (a_1 + a_2) = r \cdot a_1 + r \cdot a_2$$

y las propiedades (*) se traducen análogamente en las siguientes:

$$m2) \qquad (r_1 + r_2) \cdot a = r_1 \cdot a + r_2 \cdot a$$

$$m3) \qquad (r_1 \cdot r_2) \cdot a = r_1 \cdot (r_2 \cdot a)$$

$$m4) \qquad 1 \cdot a = a$$

en donde $r, r_1, r_2 \in R$ y $a, a_1, a_2 \in A$.

Podemos independizarnos, en sólo una pequeña medida, de End(A) e imaginar una nueva estructura definida en A por el anillo R. Específicamente, la estructura definida por las propiedades m1), m2), m3), m4).

Definición 1.1.2. Se llama estructura de *módulo a la izquierda sobre el anillo* R, o también estructura de *R-módulo a la izquierda sobre* A a la estructura determinada sobre A por toda aplicación $R \times A \to A$, tal que si

$$(r, a) \mapsto r \cdot a$$

se satisfacen las propiedades

m1) $$r \cdot (a_1 + a_2) = r \cdot a_1 + r \cdot a_2$$

m2) $$(r_1 + r_2) \cdot a = r_1 \cdot a + r_2 \cdot a$$

m3) $$(r_1 \cdot r_2) \cdot a = r_1 \cdot (r_2 \cdot a)$$

m4) $$1 \cdot a = a$$

cualesquiera que sean $a, a_1, a_2 \in A$ y $r, r_1, r_2 \in R$.

Notas. 1) Una aplicación del tipo mencionado en la definición se suele llamar una ley de composición externa. 2) m1) y m2) expresan que la aplicación $(r, a) \mapsto r \cdot a$ es *bi*lineal. 3) m3) expresa un tipo de asociatividad de la ley de composición. 4) m4) se expresa diciendo que A es un R-módulo a la izquierda *unitario*.

Una representación de R sobre A determina una estructura de R-módulo a la izquierda, como se acaba de ver. Recíprocamente, supongamos definida sobre A una estructura de R-módulo a la izquierda por una
2 aplicación $(r, a) \to r \cdot a$. Vamos a demostrar que dicha estructura es derivable de una representación de R. En efecto, la observación de la propiedad m1) nos dice que los elementos de R "operan" linealmente sobre A. Por lo tanto, sugiere la siguiente definición.

Sea

$$\rho : R \to \mathrm{End}(A)$$

definida por

$$\rho(r)(a) = r \cdot a$$

si $r \in R$ y $a \in A$. Entonces, m2), m3) y m4) no dicen otra cosa que ρ es un morfismo del anillo R en el anillo End(A). Por lo tanto, ha quedado definida una representación de R sobre A. Es claro que dicha representación induce la estructura de módulo de partida. Por lo tanto, se ha probado que existe una correspondencia biyectiva entre representaciones del anillo R en End(A) y estructuras de R-módulos a la izquierda definidas sobre A.

Antes de dar algunos ejemplos, digamos que es posible definir sobre A una estructura de *R-módulo a la derecha*. La única variante es que, en vez de m3), imponemos la condición

m3') $$(r_1 \cdot r_2) \cdot a = r_2 \cdot (r_1 \cdot a).$$

En estas condiciones conviene más escribir los operadores a la derecha $a \cdot r$ en vez de $r \cdot a$, y entonces la definición de R-módulo a la derecha está enteramente en simetría con la correspondiente a la izquierda. Si R es un anillo *conmutativo*, entonces m3) y m3') son propiedades equivalentes y no es necesario hacer distinciones a la izquierda o a la derecha.

En lo sucesivo se considerarán R-*módulos a la izquierda*, salvo pocas excepciones que se aclararán oportunamente. En la teoría de módulos interesa considerar también bi-módulos, o sea módulos simultáneamente a la izquierda y a la derecha, y aun casos en que se tiene una estructura de R-módulo a la izquierda y S-módulo a la derecha, donde R y S son anillos no necesariamente iguales. En estos casos se impone la condición asociativa

$$(r \cdot x) \cdot s = r \cdot (x \cdot s) \quad \text{si } r \in R,\ x \in A,\ s \in S.$$

No obstante, no se estudiarán bi-módulos en esta monografía. Convendremos, entonces, en que R-módulo significa R-módulo a la izquierda (salvo mención expresa) y, si no hay lugar a confusión, en que "módulo" significa R-módulo. Todos los módulos a estudiar serán *unitarios*.

Ejemplo 1. Todo grupo abeliano es un $\mathbf{Z}$-módulo, en forma natural. Para ello, hasta definir la única representación $\rho : \mathbf{Z} \to \mathrm{End}(A)$ $\rho(m)(a) = m \cdot a = ma$. Recuérdese que $m \cdot a$ significa

$$\begin{cases} a + \ldots + a & (m \text{ sumandos}), \text{ si } m > 0 \\ 0, & \text{si } m = 0 \\ (-a) + \ldots + (-a) & (-m \text{ sumandos}), \text{ si } m < 0. \end{cases}$$

Ejemplo 2. Si $A = \{0\}$, entonces A admite una (única) estructura de R-módulo, cualquiera que sea el anillo R. Denotaremos dicha estructura simplemente por 0. 3

Ejemplo 3. Sea R un anillo. El producto de anillo en R

$$(r, x) \mapsto r \cdot x$$

determina sobre R una estructura de R-módulo a la izquierda.

Ejemplo 4. Para el lector familiarizado con el álgebra lineal le recordamos que la estructura de *espacio vectorial sobre un cuerpo* es un ejemplo muy importante de estructura de módulo. Precisamente, en muchas etapas del desarrollo de la teoría de módulos haremos uso de ideas y métodos del álgebra lineal. Por ejemplo, la noción de módulo libre es una clara generalización de la de espacio vectorial.

Ejemplo 5. Todo grupo abeliano A es un End(A)-módulo a la izquierda por la representación identidad $\mathrm{id}_{\mathrm{End}(A)} : \mathrm{End}(A) \to \mathrm{End}(A)$.

El siguiente resultado permite definir, en ciertas condiciones, sobre un R-módulo A una estructura de R/I-módulo, donde I denota un ideal (bilátero) de R.

Proposición 1.1.3. Sea A un R-módulo y sea I un ideal de R. Si $I \cdot A = \{y \cdot a / y \in I \text{ y } a \in A\} = 0$, entonces existe sobre A una única estructura de R/I-módulo con la propiedad

$$(*) \qquad r \cdot a = \bar{r} \cdot a$$

si $a \in A$, $r \in R$ y $\bar{r}$ es la imagen de r por el morfismo canónico $R \to R/I$. Recíprocamente, si sobre A está definida una estructura de R/I-módulo que satisface (*), entonces $I \cdot A = 0$.

Demostración. Consideremos el diagrama

$$\begin{array}{ccc} R & \xrightarrow{\rho} & End(A) \\ & \searrow & \\ & & R/I \end{array}$$

donde ρ es la representación de R que induce la dada estructura de R-módulo sobre A y $R \to R/I$ es el morfismo canónico. La condición necesaria y suficiente para que exista un morfismo (de anillos) $\rho' : R/I \to End(A)$, que haga conmutativo el diagrama, es que

$$I \subset Nu(\rho) = \text{Núcleo de } \rho$$

lo cual equivale a que para todo $y \in I$, $a \in A$ se tenga

$$y \cdot a = 0, \quad \text{o sea } I \cdot A = 0.$$

El teorema queda probado.

Para conveniencia del lector, se hará una demostración del resultado sobre morfismos de anillos utilizado en la demostración de la proposición 1. 1. 3. Un resultado enteramente análogo para módulos se considerará posteriormente.

Lema 1.1.4. Sea R y S anillos, sea I un ideal de R. Sea el diagrama

$$\begin{array}{ccc} R & \xrightarrow{\rho} & S \\ & \searrow \quad \nearrow_{\rho'} & \\ & R/I & \end{array}$$

donde $R \to R/I$ denota el morfismo canónico $r \to \bar{r}$. La condición necesaria y suficiente para que exista un morfismo ρ', tal que el diagrama sea conmutativo, es que

$$I \subset Nu(\rho).$$

Con esas propiedades, el morfismo ρ' es único.

Demostración. Sean $I \subset Nu(\rho)$, $r \in R$ y $\bar{r} \in R/I$ su clase de equivalencia en el anillo cociente R/I. Nótese que si $\bar{r} = \bar{t}$, $r, t \in R$, entonces $r - t \in I \subset Nu(\rho)$, por lo tanto $\rho(r) = \rho(t)$, lo cual dice exactamente que

$$\bar{r} \mapsto \rho(r)$$

define una aplicación ρ' de R/I en S. $\bar{\rho}$, así definida, tiene las propiedades pedidas.

Recíprocamente, sea $\rho' : R/I \to S$ un morfismo que hace conmutativo aquel diagrama, y sea $y \in I$. Entonces $\bar{y} = 0$, por lo tanto

$$\rho(y) = \rho'(\bar{y}) = 0$$

o sea $y \in Nu(\rho)$, lo cual prueba la inclusión $I \subset Nu(\rho)$. Finalmente, la condición de que el diagrama sea conmutativo impone que ρ' sea única. El lema queda probado.

Veamos algunas aplicaciones de 1. 1. 3.

1) Sea $n \in \mathbf{N}$, y sea $\mathbf{Z}_n$ el anillo de restos módulo n. $\mathbf{Z}_n$ es el anillo cociente de $\mathbf{Z}$ por el ideal $\langle n \rangle$ de múltipos de n. Puesto que $n \cdot \mathbf{Z} \neq 0$, se deduce que sobre $\mathbf{Z}$ no existe ninguna estructura de $\mathbf{Z}_n$-módulo *unitario*.

2) $\mathbf{Z}_m$ es $\mathbf{Z}_n$-módulo unitario si, y sólo si, m/n. En efecto, $\langle n\rangle \cdot \mathbf{Z}_m = 0$ si, y sólo si, $n \cdot \mathbf{Z}_m = 0$, lo cual equivale a que m/n. Por ejemplo, la estructura de $\mathbf{Z}_4$-módulo sobre $\mathbf{Z}_2$ está dada por

	$\underline{0}$	$\underline{1}$
$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$
$\underline{2}$	$\underline{0}$	$\underline{0}$
$\underline{3}$	$\underline{0}$	$\underline{1}$

donde el elemento en la fila $\underline{i}$ y columna $\underline{j}$ se obtiene multiplicando $\underline{i} \cdot \underline{j} (\underline{i} \in \mathbf{Z}_4$ y $\underline{j} \in \mathbf{Z}_2)$.

La proposición 1.1.3 dice que la estructura de $\mathbf{Z}_n$-módulo sobre $\mathbf{Z}_m$ (en el caso m/n) coincide con la de $\mathbf{Z}$-módulo sobre $\mathbf{Z}_m$ en el sentido siguiente: si $\underline{i} \in \mathbf{Z}_n$, $i \in \mathbf{Z}$ entonces para todo $x \in \mathbf{Z}_m$ se tiene

$$\underline{i} \cdot x = i \cdot x$$

Así, en el ejemplo de $\mathbf{Z}_2$ como $\mathbf{Z}_4$-módulo

$$\underline{2} \cdot \underline{1} = 2 \cdot \underline{1} = \underline{0}$$

Así, en $\mathbf{Z}_3$ como $\mathbf{Z}_6$-módulo,

$$\underline{2} \cdot \underline{2} = 2 \cdot \underline{2} = \underline{1}$$

$$\underline{5} \cdot \underline{2} = 5 \cdot \underline{2} = \underline{1}.$$

3) Sea A un grupo abeliano y sea p un número primo. Entonces A posee una estructura de $\mathbf{Z}_p$-módulo si, y sólo si,

$$p \cdot a = 0$$

cualquiera que sea $a \in$ A. En estas condiciones, A es un espacio vectorial sobre el *cuerpo* $\mathbf{Z}_p$.

4) Sea R un anillo con identidad $1 \neq 0$. Sea A un R-módulo. Sea I = $= \{r/r \in$ R y $\forall a \in$ A, $r \cdot a = 0\}$. Afirmamos que I es un ideal bilátero de R. En efecto, valen las propiedades

$r, r' \in$ I $\Rightarrow$ $r + r' \in$ I

$s \in$ R, $r \in$ I $\Rightarrow$ $s \cdot r \in$ I (dado que si $0 = r \cdot a$, entonces

$0 = s \cdot (r \cdot a) = (s \cdot r) \cdot a$, con lo que $s \cdot r \in$ I)

$s \in$ R, $r \in$ I $\Rightarrow$ $r \cdot s \in$ I (dado que si $r \cdot a = 0$ cualquiera que sea $a \in$ A, entonces $0 = r(s \cdot a) = (r \cdot s) \cdot a$, con lo que $r \cdot s \in$ I).

I es pues un ideal bilátero de R. Puesto que trivialmente I $\cdot$ A = 0, se puede concluir que A es un R/I-módulo tal que

$$r \cdot a = \bar{r} \cdot a$$

donde $\bar{r}$ denota la clase de $r \in$ R, módulo I. El ideal I se denomina el *anulador de* A; se denota por An(A).

Definición 1.1.5. Un R-módulo a la izquierda A se dice *fiel* si su anulador es el ideal $\{0\}$ de R. Si la estructura de R-módulo está dada por la representación $\rho : R \to End(A)$, entonces A es un R-módulo fiel si, y sólo si, ρ es un morfismo inyectivo. Si R es un anillo con identidad (que es la situación que estudiamos en esta monografía), entonces R es un R-módulo fiel. Si A es un grupo abeliano, entonces A es un End(A)-módulo a la izquierda fiel. En efecto, si $\sigma \in End(A)$, entonces $\forall a \in A$, $0 = \sigma \cdot a = \sigma(a)$ si, y sólo si, $\sigma = 0$.

2. SUBMÓDULOS

Sea A un R-módulo a la izquierda.

Definición 1.2.1. Diremos que un subconjunto A' de A es un *submódulo* de A si

s1) A' es un subgrupo del grupo abeliano subyacente en A.

s2) A' es *estable* por R, es decir

$$r \in R,\ a' \in A' \Rightarrow r \cdot a' \in A'.$$

Se deja al lector la verificación de la siguiente proposición.

Proposición 1.2.2. $A' \subset A$ es submódulo si, y sólo si, son válidas las propiedades siguientes

i) $A' \neq \emptyset$

ii) $x, y \in A' \Rightarrow x - y \in A'$

iii) $r \in R,\ x \in A' \Rightarrow r \cdot x \in A'$.

Nótese que si A' es submódulo de A, entonces A' es en forma natural un R-módulo, por restricción de las leyes de composición de A.

Ejemplo 1. Si A es un módulo, entonces $\{0\}$ y A son submódulos.

Ejemplo 2. Si R es un anillo. Por el ejemplo 3) de la §1, R es un R-módulo a la izquierda. Los submódulos de R son exactamente los ideales *a la izquierda* de R.

Ejemplo 3. Sea A un R-módulo y sea $a \in A$. Entonces

$$R \cdot a = \{r \cdot a / r \in R\}$$

es un submódulo de A, que denotamos también por $R \cdot a = \langle a \rangle$ y que denominamos el submódulo cíclico de A generado por a. Más generalmente, si $\{a_1, \ldots, a_n\}$ es un conjunto finito de elementos de A, el conjunto A' de *todas* las "combinaciones lineales"

$$\sum_{i=1}^{n} r_i \cdot a_i, \quad r_i \in R$$

constituye un submódulo de A, que denominamos el submódulo de A generado por $a_1, \ldots, a_n$ y denotamos por $\langle a_1, \ldots, a_n \rangle$.

Ejemplo 4. Sea A un R-módulo y sean A', A'' submódulos de A. Sea

$$A' + A'' = \{a' + a''/a' \in A' \text{ y } a'' \in A''\}$$

Entonces A' + A'' es submódulo de A y se denomina el submódulo *suma* de A' y A''. Se verifica A' + A'' = A'' + A'. Si R = **Z** y A = **Z**, los submódulos de **Z** son los ideales $\langle n \rangle$. Dejamos a cargo del lector la verificación de la siguiente relación

$$\langle m \rangle + \langle n \rangle = \langle (m, n) \rangle$$

donde (m, n) denota el máximo común divisor de m y n. En particular, $\langle m \rangle + \langle n \rangle = \mathbf{Z}$ si, y sólo si, $(m, n) = 1$. Dejamos también a cargo del lector verificar que si A_1, A_2 son submódulos de A, entonces $A_1 \cap A_2$ es un submódulo de A. Analícese esta situación en **Z**.

Ejemplo 5. Sea A un grupo abeliano con su estructura de End(A)-módulo a la izquierda. Sean $a \in A$ e $I \subset \mathrm{End}(A)$ un ideal a la izquierda de End(A). Entonces

$$A_{a,I} = \{\sigma(a) \mid \sigma \in I\}$$

es un submódulo de A. Se deja a cargo del lector encontrar otros submódulos de A.

3. MORFISMOS y $\mathrm{Hom}_R(A, B)$

Sea R un anillo con identidad $1 \neq 0$. Sean A y B, R-módulos a la izquierda. Sea $f : A \to B$ una aplicación de A en B.

Definición 1.3.1. Se dice que f es un *morfismo de módulos*, o simplemente un morfismo, si para todo $x, y, a \in A$, $r \in R$, se cumplen las siguientes propiedades

m1) f es un morfismo de grupos: $f(x + y) = f(x) + f(y)$

m2) f preserva operadores: $f(r \cdot a) = r \cdot f(a)$.

Dejamos a cargo del lector la verificación de las siguientes proposiciones ya estudiadas en el caso de grupos y anillos.

Proposición 1.3.2. Sea $f : A \to B$ un morfismo de módulos. Entonces

i) $\mathrm{Nu}(f) = \{x/f(x) = 0\}$ es un submódulo de A

ii) $\mathrm{Im}(f) = \{y/y \in B$, existe $x \in A$, tal que $y = f(x)\}$ es submódulo de B

iii) f es un morfismo inyectivo si, y sólo si, $\mathrm{Nu}(f) = 0$.

Definición 1.3.3. Se dice que un morfismo de módulos es

a) monomorfismo, si f es inyectiva

b) epimorfismo, si f es sobre

c) endomorfismo, si A = B

d) isomorfismo, si f es monomorfismo y epimorfismo. Se escribe entonces $f : A \simeq B$, o $A \overset{f}{\simeq} B$, o $A \simeq B$ si se sobreentiende la f;

e) automorfismo, si f es un isomorfismo y A = B.

Ejemplo 1. Sea R con su estructura natural de módulo a la izquierda. Vamos a determinar *todos* los endomorfismos de R (como R-módulo). Sea $f : R \to R$ un endomorfismo, y sea $a = f(1)$. Entonces, si $r \in R$, resulta $f(r) = f(r \cdot 1) = r \cdot f(1) = r \cdot a$, es decir f es una "multiplicación *a la derecha* por un elemento de R". Recíprocamente, toda multiplicación a la derecha es un R-endomorfismo. Se deja a cargo del lector la determinación de *todos* los automorfismos (como R-módulo) de R.

Ejemplo 2. Sea $A = \langle a_1, \ldots, a_n \rangle$ un módulo a la izquierda de tipo finito sobre un anillo R. Sea C un R-módulo a la izquierda. Vamos a estudiar el siguiente problema. Dados $c_1, \ldots, c_n$ en C, nos preguntamos: ¿cuáles son las condiciones para que exista un morfismo $f : A \to C$, tal que $f(a_i) = c_i$, si $i = 1, \ldots, n$? Sean $r_1, \ldots, r_n \in R$, tales que $\sum_{i=1}^{n} r_i \cdot a_i = 0$, entonces si existe un morfismo f con las propiedades pedidas debe verificarse $\sum_{i=1}^{n} r_i \cdot c_i = 0$. Recíprocamente, si $r_i \in R$ y si

$$(c) \qquad \sum_{i=1}^{n} r_i \cdot a_i = 0 \Rightarrow \sum_{i=1}^{n} r_i \cdot c_i = 0,$$

entonces, de

8

$$(1) \qquad x = \sum_{i=1}^{n} r_i \cdot a_i = \sum_{i=1}^{n} r'_i \cdot a_i, \text{ resulta } 0 = \sum_{i=1}^{n} (r_i - r'_i) \cdot a_i$$

por lo que

$$0 = \sum_{i=1}^{n} (r_i - r'_i) \cdot c_i, \text{ o sea } \sum_{i=1}^{n} r_i \cdot c_i = \sum_{i=1}^{n} r'_i \ c_i .$$

Es decir, aun cuando x pudiera tener distintas representaciones como combinación lineal de los generadores a_i, como muestra (1), el valor $\sum_{i=1}^{n} r_i \cdot c_i$ *no* depende de las mismas, por lo que

$$f : \sum_{i=1}^{n} r_i \cdot a_i \to \sum_{i=1}^{n} r_i \cdot c_i$$

define una aplicación de A en C. Se verifica fácilmente que f es un morfismo y además $f(a_i) = c_i$. En definitiva, la condición necesaria y suficiente para que exista un morfismo f de A en C, tal que $f(a_i) = c_i$, está dada por (c).

En particular, si $A = \langle a \rangle$, la condición (c) se expresa

$$r \cdot a = 0 \Rightarrow r \cdot c = 0, \text{ si } r \in R$$

es decir, $An(a) \subset An(c)$.

Se deja a cargo del lector demostrar, a manera de aplicación de lo que se acaba de exponer, que no existe ningún morfismo no trivial de $\mathbf{Z}_n$ en $\mathbf{Z}$, considerado como Z-módulo.

Sean A y B, R-módulos. Sea

$$\mathrm{Hom}_R(A, B)$$

la totalidad de morfismos de R-módulos de A en B. Entonces

Proposición 1.3.4. 1) La ley de composición

$$\mathrm{Hom}_R(A, B) \times \mathrm{Hom}_R(A, B) \to \mathrm{Hom}_R(A, B)$$
$$(f, g) \to f + g$$

tal que

$$(f + g)(a) = f(a) + g(b)$$

define sobre $\mathrm{Hom}_R(A, B)$ una estructura de grupo abeliano.

2) Si R es *conmutativo,* la aplicación

$$(r, f) \to r \cdot f$$

tal que

$$(r \cdot f)(a) = r \cdot f(a)$$

define sobre el grupo abeliano $\mathrm{Hom}_R(A, B)$ una estructura de R-módulo.

Demostración. 1) Dados $f, g \in \mathrm{Hom}_R(A, B)$, vamos a demostrar que $f + g$ pertenece a $\mathrm{Hom}_R(A, B)$. Sean, pues, $a, a' \in A$. Se tiene

$$\begin{aligned}(f + g)(a + a') &= f(a + a') + g(a + a') \\ &= f(a) + f(a') + g(a) + g(a') \\ &= f(a) + g(a) + f(a') + g(a') \\ &= (f + g)(a) + (f + g)(a').\end{aligned}$$

en donde se ha hecho uso de la propiedad conmutativa de + en B. Además,

$$\begin{aligned}(f + g)(r \cdot a) &= f(r \cdot a) + g(r \cdot a) \\ &= r \cdot f(a) + r \cdot g(a) \\ &= r \cdot (f(a) + g(a)) \\ &= r \cdot (f + g)(a).\end{aligned}$$

El resto de los axiomas de grupo abeliano se prueban sin dificultad.

2) En lo que hay que tener cuidado es en la verificación de si $r \in R$, $f \in \mathrm{Hom}_R(A, B)$, entonces $r \cdot f \in \mathrm{Hom}_R(A, B)$. Que $r \cdot f$ es aditiva, o sea

$$(r \cdot f)(a + a') = (r \cdot f)(a) + (r \cdot f)(a')$$

es inmediato. Veamos el comportamiento de $r \cdot f$ respecto de operadores,

$$\begin{aligned}(r \cdot f)(r' \cdot a) &= r \cdot (f(r' \cdot a)) \\ &= r \cdot (r' \cdot f(a)) = (r \cdot r') \cdot f(a)\end{aligned}$$

$= (r' \cdot r) \cdot f(a)$ (por la propiedad conmutativa de R)

$= r' \cdot (r \cdot f(a))$

$= r' \cdot ((r \cdot f)(a))$

lo cual prueba bien que $r \cdot f$ es un R-morfismo. Las otras propiedades de estructura de módulo sobre R se prueban sin dificultad.

Proposición 1.3.5. Sean $f: B \to C$, $g: A \to B$ morfismos de R-módulos. Entonces la composición $(f \cdot g)(x) = f(g(x))$

$$f \cdot g: A \to C$$

es un R-morfismo.

Demostración. Es fácil.

Sea $f: A \to C$ un morfismo de R-módulos. Sean B y D R-módulos. Quedan definidos entonces morfismos naturales de grupos abelianos

$$f^*: \mathrm{Hom}_R(B, A) \to \mathrm{Hom}_R(B, C)$$

$$f_*: \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(A, D)$$

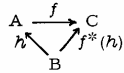
por

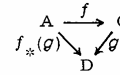
10

$$f^*(h) = f \cdot h$$

$$f_*(g) = g \cdot f$$

respectivamente. Las definiciones corresponden a los diagramas conmutativos





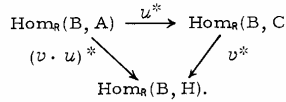
y valen las propiedades siguientes

i) si $\mathrm{id}_A: A \to A$ es el morfismo identidad, $(\mathrm{id}_A)^* = \mathrm{id}_{\mathrm{Hom}_R(B, A)}$.

ii) si $u: A \to C$ y $v: C \to H$ son R-morfismos y B es un R-módulo, entonces $v \cdot u: A \to H$ induce

$$(v \cdot u)^* = v^* \cdot u^*$$

o sea



iii) si $u: A \to C$ y $v: C \to H$ y D es un R-módulo, entonces $v \cdot u: A \to H$ induce

$$(v \cdot u)_* = u_* \cdot v_*$$

o sea

$$\begin{array}{ccc} \mathrm{Hom}_R(H, D) & \xrightarrow{v^*} & \mathrm{Hom}_R(C, D) \\ & {\scriptstyle (v\cdot u)_*}\searrow \quad \swarrow{\scriptstyle u_*} & \\ & \mathrm{Hom}_R(A, D) & \end{array}$$

ii') si A = H en ii) y $v \cdot u = \mathrm{id}_A$, entonces $v^* \cdot u^* = \mathrm{id}_{\mathrm{Hom}_R(B, A)}$

iii') si A = H en iii) y $v \cdot u = \mathrm{id}_A$, entonces $u_* \cdot v_* = \mathrm{id}_{\mathrm{Hom}_R(A, D)}$.

En resumen, se puede considerar a Hom_R como una "función" de dos variables X e Y, definida sobre los pares de R-módulos a la izquierda X, Y y que toma valores en la clase de grupos abelianos

$$\mathrm{Hom}_R : (X, Y) \to \mathrm{Hom}_R(X, Y)$$

tal que, si fijamos una variable, se obtiene las "funciones" de la otra variable

$$\mathrm{Hom}_R(B, \ ) : Y \to \mathrm{Hom}(B, Y)$$

$$\mathrm{Hom}_R(\ , D) : X \to \mathrm{Hom}_R(X, D)$$

con las propiedades de asociar a cada morfismo $A \xrightarrow{f} C$ los morfismos

$$f^* = \mathrm{Hom}_R(B, f) : \mathrm{Hom}_R(B, A) \to \mathrm{Hom}_R(B, C)$$

$$f_* = \mathrm{Hom}_R(f, D) : \mathrm{Hom}_R(C, D) \to \mathrm{Hom}_R(A, D)$$

tales que

$$\mathrm{Hom}_R(B, \mathrm{id}_A) = \mathrm{id}_{\mathrm{Hom}_R(B, A)}$$

$$\mathrm{Hom}_R(\mathrm{id}_A, D) = \mathrm{id}_{\mathrm{Hom}_R(A, D)}.$$

Las ideas subyacentes en las propiedades enumeradas de Hom_R conducen a la definición de la noción de "funtor" de fundamental importancia en el álgebra y matemática modernas. Técnicamente, se dice que Hom_R es un "funtor" en dos variables definido en la categoría de pares de R-módulos a la izquierda y con valores en la categoría de grupos abelianos, covariante en la primer variable y contravariante en la segunda. Véase (4), (17).

Proposición 1.3.6. (Un isomorfismo importante). Sea A un R-módulo a la izquierda. Entonces

i) $\mathrm{Hom}_R(R, A)$ admite una estructura natural de R-módulo a la izquierda, definiendo

$$(r \cdot f)(x) = f(x \cdot r) \quad \text{si } r \in R, \ x \in R.$$

ii) $\mathrm{Hom}_R(R, A)$ es naturalmente isomorfo, como R-módulo, a A, o sea, $\mathrm{Hom}_R(R, A) \simeq A$. Dicho isomorfismo asocia a cada $a \in A$ el único morfismo f_a que aplica 1 en a.

Demostración. a) Sólo hay que probar las propiedades siguientes $r \cdot f \in \mathrm{Hom}_R(R, A)$ y $(r_1 \cdot r_2) \cdot f = r_1 \cdot (r_2 \cdot f)$, pues las restantes propie-

dades de módulo se derivan sin dificultad y, por lo tanto, se omite su verificación. Se tiene

$$(r \cdot f)(s \cdot x) = f(s \cdot x \cdot r) = s \cdot f(x \cdot r)$$
$$= s \cdot ((r \cdot f)(x))$$

con lo que $r \cdot f$ respeta operadores. Que $r \cdot f$ es aditivo, no ofrece dificultad alguna. Por otra parte

$$((r_1 \cdot r_2) \cdot f)(x) = f(x \cdot r_1 \cdot r_2) = (r_2 \cdot f)(x \cdot r_1)$$
$$= (r_1 \cdot (r_2 \cdot f))(x)$$

con lo que $(r_1 \cdot r_2) \cdot f = r_1 \cdot (r_2 \cdot f)$ y así a) queda probado. La naturalidad de la definición consiste en que la misma utiliza el producto de anillo de R.

b) Siendo R un módulo cíclico, la identidad 1 es un generador, y el hecho $r \cdot 1 = 0$ si, y sólo si, $r = 0$, permite definir para cada elemento $a \in A$ un morfismo $f_a : R \to A$ por

$$f_a(r) = r \cdot a.$$

Además, se satisfacen las propiedades $f_{a+a'} = f_a + f_{a'}$ y $f_{r \cdot a} = r \cdot f_a$ (en efecto, $f_{r \cdot a}(x) = x \cdot (r \cdot a)$ y $(r \cdot f_a)(x) = f_a(x \cdot r) = x \cdot r \cdot a$). Sea $F : A \to \mathrm{Hom}_R(R, A)$ el morfismo $F(a) = f_a$. Recíprocamente, si $f : R \to A$, entonces $f(1) = a$ satisface $f(r) = f(r \cdot 1) = r \cdot f(1) = r \cdot a$. Por lo tanto, $f \to f(1)$ determina un morfismo $G : \mathrm{Hom}_R(R, A) \to A$. Ambos F y G son R-morfismos y satisfacen

12

$$F \cdot G = \mathrm{id}_{\mathrm{Hom}_R(R, A)}$$
$$G \cdot F = \mathrm{id}_A$$

lo cual prueba el isomorfismo en cuestión.

Una vez más la naturalidad del isomorfismo está determinada por utilizarse en su definición únicamente el producto de anillo.

Nota. En general, no es posible definir una estructura de R-módulo en $\mathrm{Hom}_R(A, B)$ si A y B son *solamente* R-módulos a la izquierda y el anillo no es conmutativo. En el caso de bimódulos sobre R (o sea módulos que son simultáneamente módulos a la izquierda y a la derecha) es posible definir una estructura de R-módulo en $\mathrm{Hom}_R(A, B)$, pero esto no se analizará en esta monografía. El lector interesado puede consultar las referencias (3c), (4).

4. MÓDULO COCIENTE

Sea A un R-módulo. Vamos a investigar cuáles son las relaciones de equivalencia $\sim$ en A compatibles con la estructura de R-módulo a la izquierda, es decir las relaciones de equivalencia $\sim$ que satisfacen

c1) $\quad a \sim a'$ y $b \sim b' \Rightarrow a + a' \sim b + b'$

c2) $\quad r \in R$ y $b \sim b' \Rightarrow r \cdot b \sim r \cdot b'$.

Las relaciones de equivalencia compatibles con la suma están caracterizadas por los subgrupos de A. Exactamente, si $\sim$ es una relación de equivalencia que satisface c1), entonces existe un subgrupo de A' de A tal que

$$b \sim b' \text{ si, y sólo si, } b - b' \in A'$$

Si, además, satisface c2), se tiene que

$$\begin{aligned} r \in R \text{ y } a \in A' &\Leftrightarrow r \in R \text{ y } a \sim 0 \\ &\Rightarrow r \cdot a \sim r \cdot 0 \\ &\Leftrightarrow r \cdot a \in A' \end{aligned}$$

de manera que A' es un submódulo de A.

Recíprocamente, si A' es un submódulo de A, la relación

$$b \sim b' \text{ si, y sólo si, } b - b' \in A'$$

es una relación de equivalencia compatible con las estructuras de R-módulo.

En definitiva, se tiene una correspondencia biyectiva entre relaciones de equivalencia sobre A, compatibles con la estructura de R-módulo a la izquierda y submódulos de A.

Sea A un R-módulo y A' un submódulo. Sea $\sim$ la relación de equivalencia inducida por A'; por $A/\sim$, o también por A/A', denotamos el conjunto cociente de A por $\sim$. Sea $\theta : A \to A/A'$ la aplicación canónica.

Proposición 1.4.1. Existe sobre A/A' una única estructura de R-módulo a la izquierda que hace de θ un morfismo.

Demostración. Todo elemento de A/A' es de la forma $\theta(a)$ con $a \in A$. Debemos, pues, definir

$$r \cdot \theta(a) \text{ y } \theta(a) + \theta(b).$$

Para ello notemos que

$$\begin{aligned} \theta(a) = \theta(a') &\Leftrightarrow a - a' \in A' \\ &\Rightarrow r \cdot a - r \cdot a' \in A' \\ &\Leftrightarrow \theta(r \cdot a) = \theta(r \cdot a') \end{aligned}$$

por lo tanto, para todo $r \in R$ y $a \in A$, $\theta(r \cdot a)$ determina un único elemento en A/A', que sólo depende de r y $\theta(a)$. Definiremos

$$r \cdot \theta(a) = \theta(r \cdot a).$$

Análogamente, si $\theta(a) = \theta(a')$ y $\theta(b) = \theta(b')$, entonces

$$a - a' \in A' \quad y \quad b - b' \in A'$$

por lo que

$$(a + b) - (a' + b') \in A'$$

o sea

$$\theta(a + b) = \theta(a' + b')$$

por lo tanto $\theta(a + b)$ determina un elemento de A/A', que sólo depende de $\theta(a)$ y $\theta(b)$. Definiremos entonces

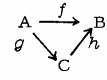
$$\theta(a) + \theta(b) = \theta(a + b).$$

Las definiciones dadas automáticamente hacen de θ un morfismo, el cual es sobre y transporta todas las propiedades de R-módulo de A sobre A/A'. La unicidad se prueba del mismo modo que para grupos y se deja como ejercicio para el lector.

Nótese que el núcleo del morfismo canónico $\theta : A \to A/A'$ es exactamente A'. De manera que, como en la oportunidad de estudiar grupos, hemos realizado todo submódulo de A como núcleo de un morfismo de A en un módulo conveniente.

Proposición 1.4.2. Sean A, B, C, R-módulos a la izquierda y sean $f : A \to B$, $g : A \to C$ morfismos. Entonces, la condición necesaria y suficiente para que exista un morfismo $h : C \to B$, tal que

$$f = h \cdot g$$



es que

$$\mathrm{Nu}(g) \subset \mathrm{Nu}(f).$$

Con esas propiedades el morfismo h es único.

Demostración. Es la misma que en 1.1.3, aunque con pequeños cambios.

Corolario 1.4.3. Sean A y C, R-módulos y sea A' un submódulo de A. Sea $f : A \to C$ un morfismo. Si $\theta : A \to A/A'$ denota el morfismo canónico, entonces a) existe un único morfismo $h : A/A' \to C$, tal que $h \cdot \theta = f$ si, y sólo si, $A' \subset \mathrm{Nu}(f)$.

b) Si f es un epimorfismo, entonces h es un epimorfismo.

c) h es un isomorfismo si, y sólo si, f es un epimorfismo y además $A' = \mathrm{Nu}(f)$.

Demostración. a) Es consecuencia inmediata de 1.4.2.

b) Resulta de la relación $h \cdot \theta = f$.

c) Si h es un isomorfismo, entonces f es claramente un epimorfismo. Además, si $x \in A$ es tal que $f(x) = 0$, entonces $h(\theta(x)) = f(x) = 0$, pero como h es un monomorfismo se tiene $\theta(x) = 0$, es decir $x \in A'$. Se ha probado que $\mathrm{Nu}(f) \subset A'$. Como $A' \subset \mathrm{Nu}(f)$, resulta $\mathrm{Nu}(f) = A'$. Esto prueba la parte *sólo si*. Lo que resta de la demostración se deja a cargo del lector.

De acuerdo con 1. 4. 3, c) se tiene que *si*

$$f : A \to C$$

es un epimorfismo, entonces

$$\boxed{C \simeq A/\mathrm{Nu}(f)}$$

Este resultado es de gran utilidad.

Ejemplo 1. Sea A un R-módulo. Sea $a \in A$. La aplicación

$$f : R \to A$$

dada por

$$f(r) \to r \cdot a$$

es un morfismo de R-módulos. Calculemos Nu(f).

$$x \in \mathrm{Nu}(f) \Leftrightarrow 0 = f(x) = x \cdot a.$$

Por lo tanto, Nu(f) es el ideal a la izquierda denotado por

$$\mathrm{An}(a) = \{r / r \cdot a = 0\}$$

y que se denomina el *anulador de a* (en R). Por lo tanto,

$$R \cdot a = \mathrm{Im}(f) \simeq R/\mathrm{An}(a)$$

En particular, si $A = R \cdot a$, o sea A es un R-módulo cíclico, se tiene que A es isomorfo a un cociente de R(como módulo) por un ideal a la izquierda. En conclusión, *los módulos cíclicos se identifican con los módulos cocientes* R/I *de* R *por un ideal a la izquierda* I *de* R.

Ejemplo 2. Sea A un R-módulo y sean A' y A'' submódulos de A. Existe un isomorfismo natural

$$\boxed{\frac{A''}{A' \cap A''} \simeq \frac{A'' + A'}{A'}}$$

En efecto, sean los morfismos

$$A'' \xrightarrow{i} A'' + A' \xrightarrow{\sigma} \frac{A'' + A'}{A'}$$

donde i es la inclusión y σ es el morfismo canónico. Sea $\sigma = \sigma \cdot i$ la composición de dichos morfismos. Calculemos Nu(σ) e Im(σ).

$$\begin{aligned} a \in A'' \text{ y } a \in \mathrm{Nu}(\sigma) &\Leftrightarrow \sigma(i(a)) = 0 \text{ y } a \in A'' \\ &\Leftrightarrow a = i(a) \in A' \text{ y } a \in A'' \\ &\Leftrightarrow a \in A' \cap A'', \end{aligned}$$

por lo tanto, $\mathrm{Nu}(\sigma) = A' \cap A''$.

Probemos que $\mathrm{Im}(\sigma) = \frac{A'' + A'}{A'}$, es decir σ es un epimorfismo. Todo elemento de $\frac{A'' + A'}{A'}$ es de la forma $\sigma(a'' + a')$, $a'' \in A''$ y $a' \in A'$, pero

$$\sigma(a'' + a') = \sigma(a'') = \sigma(\imath(a'')) = \sigma(a'')$$

por lo tanto σ es un epimorfismo. Se sigue que

$$\frac{A'' + A'}{A'} \simeq \frac{A''}{A' \cap A''}$$

como se quería probar.

Corolario 1.4.4. Sea $f : A \to C$ un morfismo de módulos y sea A' un submódulo de A. Entonces f induce un morfismo

$$\bar{f} : A/A' \to C/f(A')$$

cuyo núcleo $\mathrm{Nu}(\bar{f}) \simeq \frac{\mathrm{Nu}(f) + A'}{A'}$. En particular, si $A' \supset \mathrm{Nu}(f)$, $\bar{f}$ es un monomorfismo.

Demostración. Sean los morfismos

$$A \xrightarrow{f} C \xrightarrow{k} C/f(A')$$
$$\searrow^{k'} \quad \nearrow_{\bar{f}}$$
$$A/A'$$

donde k y k' son los morfismos canónicos. Se trata de definir un morfismo de A/A' en $C/f(A')$ que haga conmutativo el diagrama resultante.
16 Para ello debe verificarse que

$$A' = \mathrm{Nu}(k') \subset \mathrm{Nu}(k \cdot f)$$

lo cual es evidentemente cierto. Queda pues probada la primera parte del corolario. Calculemos el $\mathrm{Nu}(\bar{f})$. Sea $x \in A$, $x' = k'(x)$

$$\begin{aligned} x' \in \mathrm{Nu}(\bar{f}) &\Leftrightarrow k(f(x)) = 0 \\ &\Leftrightarrow f(x) \in f(A') \\ &\Leftrightarrow f(x) = f(a'),\ a' \in A' \\ &\Leftrightarrow x = a' + u,\ u \in \mathrm{Nu}(f) \end{aligned}$$

por lo tanto

$$\mathrm{Nu}(\bar{f}) = k'(A' + \mathrm{Nu}(f)) \simeq \frac{A' + \mathrm{Nu}(f)}{A'}.$$

En particular, si $\mathrm{Nu}(f) \subset A'$, resulta $\mathrm{Nu}(\bar{f}) = 0$; o sea $\bar{f}$ es un monomorfismo. El corolario 1.4.4 queda probado.

A manera de aplicación del corolario 1.4.4 consideremos el siguiente ejemplo.

Ejemplo. Sea A un R-módulo y sean A' y A'' submódulos, tales que $A' \subset A''$. La aplicación inclusión $A'' \to A$ induce un morfismo $A''/A' \to A/A'$ cuyo núcleo es 0, es decir, es un monomorfismo. Por dicho monomorfismo identificamos A''/A' con su imagen en A/A'. Nos proponemos determinar el módulo cociente

$$(A/A')/(A''/A')$$

Nótese para ello el morfismo (natural) composición

$$A \to A/A' \to (A/A')/(A''/A')$$

que es un epimorfismo por ser composición de epimorfismos. Hallemos su núcleo. Entonces si

$$a \in A,\ a \mapsto \underline{a} \mapsto 0$$

en aquella composición, implica que $\underline{a} \in A''/A'$, lo cual significa que existe $a'' \in A''$ con $\underline{a} = \underline{a''}$ en A''/A'. O sea, $a - a'' \in A'$. Pero, como $A' \subset A''$, resulta inmediatamente que $a \in A''$. Recíprocamente, si $a \in A''$, con la composición resulta $a \mapsto \underline{a} \mapsto 0$. Hemos probado que el núcleo buscado es A''. Por lo tanto, se obtiene el isomorfismo

$$\boxed{A/A'' \simeq (A/A')/(A''/A')}$$

Corolario 1.4.5. Sea A un módulo y sean A' y A'' submódulos. Entonces el morfismo identidad id_A induce un morfismo

$$i' : A/A' \to A/A''$$

si, y sólo si, $A' \subset A''$. i' es un epimorfismo.

Demostración. Consideremos el diagrama

$$\begin{array}{ccc} A & \xrightarrow{k''} & A/A'' \\ & {\scriptstyle k'}\searrow & \\ & & A/A' \end{array}$$

donde k' y k'' son los morfismos canónicos. El resultado a probar es consecuencia de la proposición 1.4.2.

Proposición 1.4.6. Sea $f : A \to C$ un epimorfismo de módulos. Sea, para cada submódulo A' de A, $f(A')$ el submódulo de C, imagen de A' por f. Entonces

$$A' \mapsto f(A')$$

define una biyeccción del conjunto de submódulos de A que contienen a $\mathrm{Nu}(f)$ sobre el conjunto de submódulos de C.

Demostración. Sea para cada submódulo C' de C, $f^{-1}(C') = \{x \in A,\ f(x) \in C'\}$. Vamos a probar que si A' es submódulo de A que contiene $\mathrm{Nu}(f)$, entonces $f^{-1}(f(A')) = A'$, y si C' es submódulo de C, entonces $f(f^{-1}(C')) = C'$.

Por definición de f^{-1}, se tiene que $A' \subset f^{-1}(f(A'))$. Si $x \in f^{-1}(f(A'))$, entonces $f(x) \in f(A')$, por lo tanto $f(x) = f(a')$ con $a' \in A'$. Por lo tanto $x - a' \in \mathrm{Nu}(f)$. Como $\mathrm{Nu}(f) \subset A'$, resulta que $x - a' \in A'$. Por lo tanto $x \in A'$. Hemos pues probado que $f^{-1}(f(A')) = A'$.

De modo análogo se prueba que $f(f^{-1}(C')) = C'$. Se sigue que f induce la biyección indicada en la proposición.

Ejemplo. Sea $\mathbf{Z} = R$ y sea $A = \mathbf{Z}$. Si A' es un submódulo de $\mathbf{Z}$, entonces $A' = \langle n \rangle$. Los submódulos de $\mathbf{Z}_n$ están en correspondencia biyec-

tiva con los submódulos de $\mathbf{Z}$ que contienen $\langle n\rangle$. Estos últimos están dados por los divisores de n puesto que

$$\langle n\rangle \subset \langle m\rangle \Leftrightarrow m/n$$

Los submódulos de $\mathbf{Z}_n$ se identifican con los módulos cocientes

$$\frac{\langle m\rangle}{\langle n\rangle}.$$

Probaremos el isomorfismo

$$\frac{\langle m\rangle}{\langle n\rangle} \simeq \mathbf{Z}_{\frac{n}{m}}, \text{ si } m/n.$$

Para ello sea la composición de morfismos

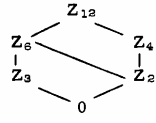
$$\mathbf{Z} \xrightarrow{t} \langle m\rangle \xrightarrow{s} \frac{\langle m\rangle}{\langle n\rangle}$$

donde $t(x) = m \cdot x$ y s es el morfismo canónico. Como ambos t y s son epimorfismos, se tiene que $s \cdot t$ es un epimorfismo. Calculemos $\mathrm{Nu}(s \cdot t)$:

$$\begin{aligned} x \in \mathrm{Nu}(s \cdot t) &\Leftrightarrow s(t(x)) = 0 \\ &\Leftrightarrow n/t(x) \\ &\Leftrightarrow m \cdot x = r \cdot n,\ r \in \mathbf{Z} \\ &\Leftrightarrow x = r \cdot \frac{n}{m} \\ &\Leftrightarrow x \in \langle \tfrac{n}{m}\rangle \end{aligned}$$

Por lo tanto, $\frac{\langle m\rangle}{\langle n\rangle} \simeq \mathbf{Z}/\langle \frac{n}{m}\rangle \simeq \mathbf{Z}_{\frac{n}{m}}$, como se quería probar.

Los subgrupos de, por ejemplo, $\mathbf{Z}_{12}$ se pueden representar en el siguiente diagrama de Hasse



donde los segmentos representan la inclusión en dirección ascendente.

Si p es un entero positivo primo, los submódulos de $\mathbf{Z}_{p^k}$ son

$$0 \subset \mathbf{Z}_p \subset \mathbf{Z}_{p^2} \subset \ldots \subset \mathbf{Z}_{p^{k-1}} \subset \mathbf{Z}_{p^k}$$

Ilustremos con un ejemplo el isomorfismo dado en uno de los ejemplos que sigue al corolario 1.4.3. Sean r, s enteros positivos. Sean

$d = (r, s)$ el máximo común divisor de r y s

$m = [r, s]$ el mínimo común múltiplo de r y s.

Se tiene $\langle r\rangle + \langle s\rangle = \langle d\rangle$ y $\langle r\rangle \cap \langle s\rangle = \langle m\rangle$. Entonces

$$\mathbf{Z}_{\frac{r}{d}} \simeq \frac{\langle d\rangle}{\langle r\rangle} = \frac{\langle r\rangle + \langle s\rangle}{\langle r\rangle} \simeq \frac{\langle s\rangle}{\langle r\rangle \cap \langle s\rangle} = \frac{\langle s\rangle}{\langle m\rangle} \simeq \mathbf{Z}_{\frac{m}{s}}$$

y, por razones de cardinalidad, este isomorfismo implica la conocida relación aritmética $r \cdot s = [r,s] \cdot (r,s)$.

Ejemplo. Sea p un número primo. Sea H_p el subgrupo de $\mathbf{Q}$ formado por todos los números racionales que admiten una representación del tipo $\frac{m}{p^i}$, $m \in \mathbf{Z}$, $i \in \mathbf{N}$.

Una verificación sencilla nos dice que H_p es submódulo de $\mathbf{Q}$. Si para cada n natural o cero designamos por H_p^n la totalidad de fracciones que admiten una representación $\frac{m}{p^i}$, $m \in \mathbf{Z}$, $i = 0$ ó $i \in [\![1,n]\!]$, se tiene la siguiente cadena de submódulos

$$(*) \qquad \mathbf{Z} = H_p^0 \subset H_p^1 \subset H_p^2 \subset \ldots \subset H_p^n \subset H_p^{n+1} \subset \ldots$$

y

$$H_p = \text{unión de la familia } \{H_p^n\}.$$

Vamos a estudiar el módulo cociente $H_p/\mathbf{Z}$.

(*) al pasar al cociente da lugar a una sucesión de submódulos de $H_p/\mathbf{Z}$

$$(**) \qquad 0 \subset \frac{H_p^1}{\mathbf{Z}} \subset \frac{H_p^2}{\mathbf{Z}} \subset \ldots \subset \frac{H_p^n}{\mathbf{Z}} \subset \ldots \text{ (Véase Fig. 1)}$$

Pero, notemos que

$$H_p^n = p^{-n} \cdot \mathbf{Z} = \frac{1}{p^n} \cdot \mathbf{Z}$$

por lo tanto, la aplicación

$$\mathbf{Z} \to p^{-n} \cdot \mathbf{Z} \quad \text{dada por } m \mapsto \frac{m}{p^n},\ m \in \mathbf{Z}$$

es un isomorfismo y es tal que

$$p^n \cdot \mathbf{Z} \to \mathbf{Z} \text{ (sobre)}$$

por lo tanto

$$\mathbf{Z}_{p^n} = \frac{\mathbf{Z}}{p^n \cdot \mathbf{Z}} \simeq \frac{p^{-n} \cdot \mathbf{Z}}{\mathbf{Z}}$$

y así (**) se convierte en la sucesión

$$0 \subset \mathbf{Z}_p \subset \mathbf{Z}_{p^2} \subset \ldots \mathbf{Z}_{p^n} \subset \ldots$$

y, por lo tanto

$$H_p/\mathbf{Z} = \text{Unión de la familia } \mathbf{Z}_{p^n}.$$

Se denota al cociente H_p/Z por

$$\mathbf{Z}_{p^\infty}$$

y este grupo abeliano tiene propiedades muy importantes. Digamos de

paso que el anillo de endomorfismos de $\mathbf{Z}_{p^\infty}$ es el anillo de enteros p-ádicos. Probemos la siguiente propiedad de $\mathbf{Z}_{p^\infty}$.

Propiedad. Los únicos subgrupos de $\mathbf{Z}_{p^\infty}$ son de la forma $\mathbf{Z}_{p^i}$ ó 0 ó $\mathbf{Z}_{p^\infty}$. En efecto, sea H un subgrupo de $\mathbf{Z}_{p^\infty}$, $0 \neq H$ y $\mathbf{Z}_{p^\infty} \neq H$. Si $\mathbf{Z}_{p^i} \subset H$ cualquiera que sea i, entonces $\mathbf{Z}_{p^\infty} = H$. Sea pues $\mathbf{Z}_{p^n} \subset H$, pero $\mathbf{Z}_{p^{n+1}} \not\subset H$. Dado que los subgrupos de $\mathbf{Z}_{p^t}$ son de la forma $0 \subset \mathbf{Z}_p \subset \mathbf{Z}_{p^2} \subset \ldots \subset \mathbf{Z}_{p^{t-1}} \subset \mathbf{Z}_{p^t}$, se tiene que

$$H \cap \mathbf{Z}_{p^{n+1}} = \mathbf{Z}_{p^n}$$

Además, cualquiera que sea $i \in N$

$$H \cap \mathbf{Z}_{p^{n+i}} \text{ es subgrupo de } Z_{p^{n+i}}$$

y, por lo tanto, debe ser de la forma

$$\mathbf{Z}_{p^{n+j}}, \text{ dado que } \mathbf{Z}_{p^n} \subset H$$

pero j no puede ser mayor que cero, porque entonces $\mathbf{Z}_{p^{n+1}}$ estaría contenido en H, lo cual no es así. Se sigue que

$$H \cap \mathbf{Z}_{p^{n+i}} = \mathbf{Z}_{p^n}$$

cualquiera que sea i en N. Por lo tanto,

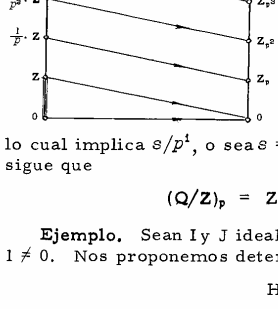
$$H = H \cap \mathbf{Z}_{p^\infty} = H \cap (\cup_i \mathbf{Z}_{p^i})$$

20

$$= \cup_i (H \cap \mathbf{Z}_{p^i}) = \mathbf{Z}_{p^n}$$

lo que prueba nuestra afirmación.

Fig. 1



Un resultado que se utilizará más adelante es el siguiente. El grupo abeliano $\mathbf{Q}/\mathbf{Z}$ es de torsión, o sea para todo $x \in \mathbf{Q}/\mathbf{Z}$ existe $m \in \mathbf{Z}$, $m \neq 0$ tal que $m \cdot x = 0$. Sea p primo. Vamos a calcular la totalidad de elementos de $\mathbf{Q}/\mathbf{Z}$ anulados por alguna potencia de p. Sea, entonces, $(\mathbf{Q}/\mathbf{Z})_p = \{x/p^i \cdot x = 0 \text{ para algún } i \in \mathbf{N}\}$. Sea $x \in (\mathbf{Q}/\mathbf{Z})_p$, con $p^i \cdot x = 0$. Representando a x por un elemento $r/s \in \mathbf{Q}$, $r/s \in \mathbf{Z}$, $s \neq 0$ y $(r, s) = 1$, resulta

$$\frac{p^i \cdot r}{s} = p^i \cdot (r/s) \in \mathbf{Z}$$

lo cual implica s/p^i, o sea $s = p^j$, $0 \leq j \leq i$. Por lo tanto, $r/s \in H_p$. Se sigue que

$$(\mathbf{Q}/\mathbf{Z})_p = \mathbf{Z}_{p^\infty}.$$

Ejemplo. Sean I y J ideales de un anillo *conmutativo* R con identidad $1 \neq 0$. Nos proponemos determinar el R-módulo

$$\mathrm{Hom}_R(R/I,\ R/J).$$

Introduzcamos primero el ideal (J : I) definido por

$$(J:I) = \{r/r \in R \text{ y } r \cdot I \subset J\}.$$

Dejamos a cargo del lector verificar que (J:I) es un ideal y que $J \subset (J:I)$.

Si $f \in \mathrm{Hom}_R(R/I, R/J)$, entonces, puesto que R/I es un módulo cíclico (por ejemplo, la clase $\bar{1}$ de 1 módulo I es generador) f está determinado por $f(\bar{1})$. A su vez, R/J también es cíclico, por lo que $f(\bar{1}) = k \cdot \bar{1}$, $k \in R$, donde, por abuso de notación, hemos denotado con el mismo $\bar{1}$ las clases de 1 módulo I y J. Probemos que $k \in (J:I)$. En efecto, si $y \in I$, entonces $y \cdot \bar{1} = 0$ en R/I, por lo tanto $(y \cdot k) \cdot \bar{1} = 0$ en R/J (dado que f es un morfismo), por lo tanto

$$y \cdot k \in J \quad \text{o sea} \quad k \in (J:I).$$

Recíprocamente, si $k \in (J:I)$ se prueba en forma análoga que

$$f_k : \bar{1} \mapsto k \cdot \bar{1}$$

define un morfismo de R/I en R/J. En definitiva,

$$k \mapsto f_k$$

define un epimorfismo de (J:I) sobre $\mathrm{Hom}_R(R/I, R/J)$ cuyo núcleo es J:

$$f_k = 0 \Leftrightarrow k \cdot \bar{1} = 0 \text{ en } R/J \Leftrightarrow k \in J$$

Por lo tanto, hemos probado el isomorfismo

$$\boxed{\mathrm{Hom}_R(R/I, R/J) \simeq (J:I)/J}$$

Analicemos el caso de $R = \mathbf{Z}$. Podemos escribir $I = \langle n \rangle$ y $J = \langle m \rangle$, con $n, m \in N$. Afirmamos que

$$(\langle m \rangle ; \langle n \rangle) = \left\langle \frac{m}{d} \right\rangle \quad \text{con } d = (m, n)$$

En efecto, es claro que $\left\langle \frac{m}{d} \right\rangle \subset (\langle m \rangle ; \langle n \rangle)$. Recíprocamente sea $d = (m, n) = n \cdot s + m \cdot h$, $s, h \in \mathbf{Z}$. Si $x \in (\langle m \rangle ; \langle n \rangle)$, se tiene que $n \cdot x = m \cdot t$ con $t \in \mathbf{Z}$. Por lo tanto

$$s \cdot n \cdot x = s \cdot m \cdot t, \quad \text{o sea}$$

$$d \cdot x = s \cdot m \cdot t + m \cdot h \cdot x = m \cdot (s \cdot t + h \cdot x)$$

con lo que

$$x = \frac{m}{d} \cdot (s \cdot t + h \cdot x) \text{ y así } x \in \left\langle \frac{m}{d} \right\rangle.$$

Resulta, en definitiva, que

$$\boxed{\mathrm{Hom}_R(\mathbf{Z}_m, \mathbf{Z}_n) \simeq \frac{\left\langle \frac{m}{d} \right\rangle}{\langle m \rangle} \simeq \mathbf{Z}_d}$$

En particular, si $(n, m) = 1$, se tiene $\mathrm{Hom}_R(\mathbf{Z}_m, \mathbf{Z}_n) = 0$.

5. SUCESIONES EXACTAS

Sean A', A y A'' R-módulos, y sean $f : A' \to A$, $g : A \to A''$ morfismos.

Definición 1.5.1. Se dice que la sucesión de módulos y morfismos

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

es *exacta* (o exacta en A), si $Nu(g) = Im(f)$, es decir $\forall a \in A$, $g(a) = 0$ si y sólo si, existe $a' \in A'$ tal que $a = f(a')$.

Definición 1.5.2. Se dice que la sucesión de módulos y morfismos $(2 < n)$

$$A_{i_1} \xrightarrow{t_1} A_{i_2} \xrightarrow{t_2} \cdots A_{i_{k-1}} \xrightarrow{t_{k-1}} A_{i_k} \xrightarrow{t_k} A_{i_{k+1}} \xrightarrow{t_{n-1}} A_{i_n}$$

es exacta, si *para cada* índice k, $1 < k < n$, la sucesión

$$A_{i_{k-1}} \to A_{i_k} \to A_{i_{k+1}}$$

es exacta. Incluso es permitido que la sucesión se extienda indefinidamente a la derecha o la izquierda.

Ejemplo 1. Sea A un R-módulo. Indiquemos con $0 \to A$ el único morfismo del R-módulo 0 en A. Entonces la sucesión de módulos y morfismos

$$0 \to A \xrightarrow{f} C$$

es exacta si, y sólo si, f es un monomorfismo.

Ejemplo 2. Sea C un R-módulo. Indiquemos con $C \to 0$ el morfismo trivial. Entonces la sucesión de módulos y morfismos

$$A \xrightarrow{f} C \to 0$$

es exacta si, y sólo si, f es un epimorfismo.

Ejemplo 3. La sucesión de módulos y morfismos

$$0 \to A \xrightarrow{f} C \to 0$$

es exacta si, y sólo si, f es un isomorfismo.

Ejemplo 4. Sean A un R-módulo y A' un submódulo de A. Entonces la sucesión

$$0 \to A' \xrightarrow{i} A \xrightarrow{\theta} A/A' \to 0 \tag{1}$$

(donde i es la inclusión y θ es el morfismo canónico) es exacta.

Definición 1.5.3. Se llama sucesión *exacta corta* a toda sucesión exacta del tipo

$$0 \to A' \to A \to A'' \to 0. \tag{A}$$

Vamos a demostrar que toda sucesión exacta corta es equivalente (en un sentido a precisar) a una sucesión exacta del tipo (1).

Definición 1.5.4. Sean

$$(A): 0 \to A' \xrightarrow{u} A \xrightarrow{v} A'' \to 0$$

$$(B): 0 \to B' \xrightarrow{u'} B \xrightarrow{v'} B'' \to 0$$

sucesiones exactas cortas. Llamaremos *morfismo* de (A) en (B) a toda terna $(f) = (f', f, f'')$ formada por morfismos $f' : A' \to B'$, $f : A \to B$, $f'' : A'' \to B''$, tales que el diagrama

$$\begin{array}{ccccccccc} 0 & \to & A' & \xrightarrow{u'} & A & \xrightarrow{v} & A'' & \to & 0 \\ & & f' \downarrow & & f \downarrow & & f'' \downarrow & & \\ 0 & \to & B' & \xrightarrow{u'} & B & \xrightarrow{v'} & B'' & \to & 0 \end{array}$$

es conmutativo (es decir sus dos cuadrados son conmutativos).

Se dice que (f) es un monomorfismo (resp. epimorfismo, isomorfismo) si cada uno de los morfismos f', f, f'' es un monomorfismo(resp. epimorfismo, isomorfismo).

Proposición 1.5.5. Sea la situación de módulos y morfismos siguiente,

$$\begin{array}{ccccccccc} 0 & \to & A' & \xrightarrow{u} & A & \xrightarrow{v} & A'' & \to & 0 \\ & & f' \downarrow & & f \downarrow & & & & \\ 0 & \to & B' & \xrightarrow{u'} & B & \xrightarrow{v'} & B'' & \to & 0 \end{array}$$

con filas exactas y cuadrado conmutativo. Existe entonces un único morfismo $f'' : A'' \to B''$ que hace de (f', f, f'') un morfismo de (A) en (B) Si f' y f son isomorfismos, también lo es f''.

Demostración. Sea $a'' \in A''$. Por ser v un epimorfismo, $v(a) = a''$, para algún $a \in A$. Afirmamos que el elemento $v'(f(a))$ esta unívocamente determinado por a'' (o sea que no depende esencialmente del $a \in A$, tal que $v(a) = a''$). En efecto, si $\underline{a} \in A$ es tal que $v(\underline{a}) = a''$, entonces $a - \underline{a} \in$ $\in Nu(v) = Im(u)$, por lo tanto $a - \underline{a} = u(a')$, $a' \in A'$. Por lo tanto, aplicando f resulta

$$f(a) - f(\underline{a}) = f(u(a')) = u'(f'(a'))$$

(por la conmutatividad del primer cuadrado). Aplicando v' resulta

$$\begin{aligned} v'(f(a)) - v'(f(a)) &= v'(u'(f'(a'))) = (v' \cdot u')(f'(a')) \\ &= 0 \text{ pues } v' \cdot u' = 0. \end{aligned}$$

Nuestra afirmación queda probada. Definamos entonces

$$f''(a'') = v'(f(a)) \text{ si } v(a) = a''$$

y así queda determinada una aplicación $f'' : A'' \to B''$. Una verificación sencilla nos dice que f'' es un morfismo con las propiedades pedidas. Probemos que si f' y f son isomorfismos, entonces f'' también lo es. El hecho de ser f y v' epimorfismos y la propiedad de conmutatividad $v' \cdot f =$ $= f'' \cdot v$ implican que f'' es epimorfismo. Sea $a'' \in A''$, tal que $f''(a'') = 0$. Por su definición se tiene $0 = f''(a'') = v'(f(a))$, si $a \in A$ es tal que $v(a) = a''$. Por lo tanto, $f(a) \in Nu(v') = Im(u')$, o sea $f(a) = u'(b')$. Siendo f' un isomorfismo $b' = f'(a')$, $a' \in A'$. Se tiene

$$f(a) = u'(f'(a')) = f(u(a'))$$

y siendo f un isomorfismo $a = u(a')$. Por lo tanto, $a'' = v(a) = v(u(a')) = 0$, pues $v \cdot u = 0$. Se ha probado que f'' es un monomorfismo. En definitiva, f'' es un isomorfismo y la proposición queda demostrada.

Proposición 1.5.6. Sea $(B): 0 \to B' \xrightarrow{u'} B \xrightarrow{v'} B'' \to 0$ una sucesión exacta. Existe entonces una sucesión exacta corta del tipo

$$(A): 0 \to A' \xrightarrow{i} A \xrightarrow{v} A/A' \to 0$$

y un isomorfismo

$$(f): (A) \to (B).$$

(i denota una inclusión y v el morfismo canónico)

Demostración. Sea $A' = u'(B')$, $A = B$, $i: A' \to A$ la inclusión. Sea $v: A \to A/A'$ el morfismo canónico. Se tiene el diagrama

$$\begin{array}{ccccccccc} 0 & \to & A' & \xrightarrow{i} & A & \xrightarrow{v} & A/A' & \to & 0 \\ & & f' \downarrow & & f \downarrow & & \downarrow & & \\ 0 & \to & B' & \xrightarrow{u'} & B & \xrightarrow{v'} & B'' & \to & 0 \end{array}$$

donde $f' = u'^{-1}$, $f = \mathrm{id}_A$. El cuadrado indicado en el diagrama es conmutativo. Se sigue de la proposición 1.5.5 la existencia de un isomorfismo $f'': A/A' \to B''$ que hace de (f', f, f'') un isomorfismo. La proposición queda probada.

En virtud de la proposición 1.5.6 se dice que la sucesión (B) *es equivalente* a (A) (o viceversa). En general se puede definir sobre la familia de sucesiones exactas cortas de R-módulos una relación de equivalencia, a saber: $(A) \sim (B)$ si, y sólo si, existe un isomorfismo $(f): (A) \to (B)$. Un problema importante en la teoría de módulos es: dados dos R-módulos A' y A'' determinar (salvo equivalencias) todas las (llamadas) *extensiones de* A' *por* A''

$$0 \to A' \xrightarrow{u} X \xrightarrow{v} A'' \to 0$$

que son las sucesiones exactas cortas con X un R-módulo y u, v morfismos convenientes. Un problema de fácil formulación, cuya solución general ignoramos es el de determinar (salvo equivalencias) todas las *extensiones de* $\mathbf{Z}$ por $\mathbf{Q}$, o sea las sucesiones exactas cortas del tipo

$$0 \to \mathbf{Z} \to A \to \mathbf{Q} \to 0.$$

La siguiente proposición muestra un tipo de propiedad que el álgebra homológica estudia sistemáticamente y que se denomina *preservación de exactitud.*

Proposición 1.5.7. i) Sea $(A): 0 \to A' \xrightarrow{u} A \xrightarrow{v} A'' \to 0$ una solución exacta de R-módulos a la izquierda. Sea C un R-módulo a la izquierda. Entonces la sucesión inducida (de grupos abelianos)

$$0 \to \mathrm{Hom}_R(C, A') \xrightarrow{u^*} \mathrm{Hom}_R(C, A) \xrightarrow{v^*} \mathrm{Hom}_R(C, A'')$$

es exacta.

ii) Sea $(C): 0 \to C' \xrightarrow{s} C \xrightarrow{t} C'' \to 0$ una sucesión exacta de R-módulos a la izquierda. Sea A un R-módulo a la izquierda. Entonces la

sucesión inducida (de grupos abelianos)

$$0 \to \mathrm{Hom}_R(C'', A) \xrightarrow{t^*} \mathrm{Hom}_R(C, A) \xrightarrow{s^*} \mathrm{Hom}_R(C', A)$$

es exacta.

Demostración. Vamos a probar solamente ii), y dejamos i) como ejercicio para el lector.

t_* es un monomorfismo: Sea $g \in \mathrm{Hom}_R(C'', A)$ tal que $t_*(g) = 0$. Esto equivale a decir que el morfismo $C \xrightarrow{t} C'' \xrightarrow{g} A$ es trivial. Siendo t un epimorfismo, g debe ser 0.

$\mathrm{Im}(t_*) \subset \mathrm{Nu}(s_*)$. En efecto, $0 = t \cdot s$ implica $0 = s_* \cdot t_*$ lo cual prueba que $\mathrm{Im}(t_*) \subset \mathrm{Nu}(s_*)$.

$\mathrm{Nu}(s_*) \subset \mathrm{Im}(t^*)$. En efecto, sea $g \in \mathrm{Hom}_R(C, A)$ tal que $s_*(g) = 0$. Esto equivale a decir que el morfismo $C' \xrightarrow{s} C \xrightarrow{t} A$ es 0. Consideremos el diagrama

$$\begin{array}{ccccc} C' & \xrightarrow{s} & C & \xrightarrow{t} & C'' \\ & & g\downarrow & & \\ & & A & & \end{array}$$

$g \cdot s = 0$ implica

$$\mathrm{Nu}(t) = \mathrm{Im}(s) \subset \mathrm{Nu}(g)$$

con lo que existe un único morfismo $g'' : C'' \to A$ tal que $g'' \cdot t = g$. Pero $g'' \cdot t$ no es otra cosa que $t_*(g'')$, o sea, hemos probado que si $s_*(g) = 0$, entonces $g = t_*(g'')$ con $g'' \in \mathrm{Hom}_R(C'', A)$. Esto prueba la inclusión $\mathrm{Im}(t_*) \subset \mathrm{Nu}(s_*)$. La proposición queda demostrada.

Ejemplo 1. Mostremos que en la proposición anterior, ni v^* ni s_* necesitan ser epimorfismos (o, como suele decirse, mostremos que $\mathrm{Hom}_R(\cdot)$ no preserva en general la exactitud a la derecha). Sea la sucesión exacta $0 \to \langle 2 \rangle \to \mathbf{Z} \to \mathbf{Z}_2 \to 0$, con morfismos naturales. Aplicando $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_2,)$ resulta la sucesión

$$0 \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_2, \langle 2 \rangle) \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_2, \mathbf{Z}) \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_2, \mathbf{Z}_2) \to 0$$

equivalente a la sucesión

$$0 \to 0 \to 0 \to \mathbf{Z}_2 \to 0$$

la cual no es exacta.

Aplicando $\mathrm{Hom}_{\mathbf{Z}}(, \mathbf{Z}_2)$ resulta

$$0 \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_2, \mathbf{Z}_2) \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_2) \to \mathrm{Hom}_{\mathbf{Z}}(\langle 2 \rangle, \mathbf{Z}_2) \to 0$$

equivalente a la sucesión

$$0 \to \mathbf{Z}_2 \to \mathbf{Z}_2 \to \mathbf{Z}_2 \to 0$$

la cual no es exacta. Hemos probado nuestra afirmación.

Ejemplo 2. Sean R un anillo conmutativo y A un R-módulo. Por A* denotamos el R-módulo

$$A^* = \mathrm{Hom}_R(A, R)$$

Además escribimos $A^{**} = (A^*)^* = \mathrm{Hom}_R(\mathrm{Hom}_R(A, R), R)$. A* se denomina el módulo *dual* de A. Entonces, son válidas las afirmaciones

i) Si $0 \to A' \xrightarrow{i} A \xrightarrow{p} A'' \to 0$ es una sucesión exacta de R-módulos, se tiene la sucesión exacta

$$0 \to A''^* \xrightarrow{p^*} A^* \xrightarrow{i^*} A'^*$$

ii) Si $f : A \to B$ es un isomorfismo de R-módulos, entonces el morfismo inducido $f^* : B^* \to A^*$ es un isomorfismo.

iii) La aplicación $a \to a^{**}$ de A en A** definida por:

$$\forall\, f \in A^*, \qquad a^{**}(f) = f(a)$$

es un morfismo de módulos. La condición necesaria y suficiente para que $a \to a^{**}$ sea un monomorfismo es que para todo $a \in A$, $a \neq 0$ exista un $f \in \mathrm{Hom}_R(A, R)$, tal que $f(a) \neq 0$.

Un R-módulo A se dice *reflexivo*, si $A \to A^{**}$ es un isomorfismo. Dejamos a cargo del lector dar ejemplos de diferentes situaciones del morfismo $A \to A^{**}$.

2

MÓDULOS DE TIPO FINITO. MÓDULOS Y ANILLOS NOETHERIANOS

1. DEFINICIONES Y EJEMPLOS

En este capítulo R denotará un anillo con identidad $1 \neq 0$.

Definición 2.1.1. Sea A un R-módulo a la izquierda. Se dice que A es de *tipo finito*, o también que A es *finitamente generado* (sobre R), si existen elementos (llamados *generadores*)

$$a_1, \ldots, a_n$$

pertenecientes a A, tales que para todo $a \in A$ existen

$$r_1, \ldots, r_n \in R$$

tales que

$$a = \sum_{i=1}^{n} r_i \cdot a_i$$

o, en otros términos, *todo* elemento de A es una *combinación* lineal de $a_1, \ldots, a_n$, con coeficientes $r_1, \ldots, r_n$ en R.

En virtud de las condiciones de la definición 2.1.1 escribimos

$$A = \langle a_1, \ldots, a_n \rangle.$$

Si $n = 1$, se dice que A es un módulo *cíclico*. Ya hemos visto que los módulos cíclicos están determinados (salvo isomorfismos) por los módulos cociente R/I de R por un ideal a la izquierda I de R.

Definición 2.1.2. Sea I un ideal a la izquierda de R. Se dice que I es de tipo finito (o que I es finitamente generado) si I es un R-módulo de tipo finito.

Nótese que si M y N son submódulos de tipo finito de un módulo A, entonces M + N es de tipo finito. Sin embargo, $M \cap N$ no necesita ser de tipo finito. En general, un submódulo de un módulo de tipo finito *no* necesita ser de tipo finito, como muestra el ejemplo siguiente.

Ejemplo 1. Sea **R** el cuerpo real. Sea $\mathbf{R}^{[0,1]} = F$ el anillo de todas las funciones definidas sobre el intervalo $[0,1] = \{x/x \in \mathbf{R} \text{ y } 0 \leq x \leq 1\}$ y con valores reales. F es un F-módulo cíclico dado que $F = \langle 1 \rangle$. Vamos a demostrar la existencia de submódulos (es decir, ideales a la izquierda) de F que no son de tipo finito. Sea, en efecto, J la totalidad de elementos de F con la propiedad siguiente:

$f \in J$ si, y sólo si, f se anula en todos los puntos de $[0,1]$ salvo a lo sumo en un número finito de ellos. (Una tal función se dice que se anula en

casi todos los puntos de $[0,1]$.) Es fácil ver que J es un ideal de F, aunque no de tipo finito. En efecto, razonemos por el absurdo. Supongamos que

$$I = \langle f_1, \ldots, f_n \rangle. \tag{1}$$

Sea I_j la totalidad de puntos de $[0,1]$ donde f_j no se anula, $j = 1, \ldots, n$. I_j es un conjunto finito y así también lo es

$$I = I_1 \cup \ldots \cup I_n.$$

Sea $x \in [0,1]$, $x \notin I$. Sea $f_x : [0,1] \to R$ tal que $f_x(x) = 1$ y $f_x(y) = 0$ si $x \neq y$. Es claro que $f \in J$. Sin embargo, es evidente que no existen funciones $g_j \in F$ tales que

$$f_x = \sum_{j=1}^{n} g_j \cdot f_j$$

dado que $f_x(x) = 1$, en tanto que el segundo miembro toma el valor 0 en el punto x. Por lo tanto (1) es imposible. (Un ejemplo de módulo A y submódulos M y N de tipo finito, tales que $M \cap N$ no es de tipo finito, puede consultarse en Bourbaki (3c), §L, página 259.)

Definición 2.1.3. Un anillo R tal que todo ideal a la izquierda es cíclico se dice un anillo principal (a la izquierda). Si R es conmutativo, sin divisores de cero $\neq 0$ y principal, se dice que R es un dominio principal.

28

Ejemplo 0. Z es un dominio principal.

Ejemplo 1. $K[X]$ es un dominio principal si, y sólo si, K es un cuerpo. (En efecto, si K es un cuerpo existe entonces en $K[X]$ un algoritmo de división, y el mismo razonamiento utilizado en **Z**, permite probar que todo ideal de $K[X]$ es principal. Recíprocamente, si K no es cuerpo entonces posee un ideal L, $0 \neq L \neq K$.

Sea $a \in L$, $0 \neq a$ y sea $J = \langle a, X \rangle$ = el ideal de $K[X]$ generado por a y X. Afirmamos que J no es principal. Para demostrarlo, sea $p(X)$ un generador de J, $p(X) = a_n X^n + \ldots + a_1 X + a_0$.

$$a \in J \Rightarrow a = p(X) \cdot t(X)$$

$$X \in J \Rightarrow X = p(X) \cdot u(X)$$

Por razones de grado (gr)

$$0 = \mathrm{gr}(a) = \mathrm{gr}(p(X)) + \mathrm{gr}(t(X)),$$

$p(X)$ posee grado cero, es decir $p(X) = a_0$. Si ahora $u(X) = bX + c$ debe ser $c = 0$ y, además, $b \cdot a_0 = 1$. Esto último dice que a es una unidad en K, por lo tanto el ideal $L = K$, lo cual es una contradicción.

Ejemplo 2. Sea K un cuerpo y sea $\mathbf{M}_n(K)$ el anillo completo de matrices de n filas por n columnas. Es posible demostrar que todo ideal a la izquierda (o a la derecha) es principal y de la forma $\langle e \rangle$, donde e es idempotente, o sea $e^2 = e$. Por ejemplo, sea U un subconjunto de

$[\![1, n]\!]$. Sea J_U el ideal a la izquierda de $\mathbf{M}_n(K)$ formado por todas las matrices cuyas columnas

$$\begin{vmatrix} a_{11} \\ \cdot \\ \cdot \\ \cdot \\ a_{n1} \end{vmatrix}$$

son todos ceros si $i \notin U$. Sea $e = e_U$ la matriz cuyos coeficientes son

$$e_{ij} = \delta_{ij} \quad \text{si} \quad i, j \in U$$
$$e_{ij} = 0 \quad \text{si} \quad i \notin U \text{ ó } j \notin U$$

Se verifica

$$J_U = \langle e \rangle \quad \text{y} \quad e^2 = e.$$

Por ejemplo, si $n = 2$, los ideales del tipo J_U son

$$J_1 = \left\{ \begin{Vmatrix} a & 0 \\ a' & 0 \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} \right\rangle, \quad J_2 = \left\{ \begin{Vmatrix} 0 & b \\ 0 & b' \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 0 & 0 \\ 0 & 1 \end{Vmatrix} \right\rangle$$

$$J_{12} = \left\{ \begin{Vmatrix} a & b \\ a' & b' \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} \right\rangle$$

Si $n = 3$, los ideales del tipo J_U son

$$J_1 = \left\{ \begin{Vmatrix} a & 0 & 0 \\ a' & 0 & 0 \\ a'' & 0 & 0 \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{Vmatrix} \right\rangle, \quad J_2 = \left\{ \begin{Vmatrix} 0 & b & 0 \\ 0 & b' & 0 \\ 0 & b'' & 0 \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{Vmatrix} \right\rangle$$

$$J_3 = \left\{ \begin{Vmatrix} 0 & 0 & c \\ 0 & 0 & c' \\ 0 & 0 & c'' \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{Vmatrix} \right\rangle, \quad J_{1,2} = \left\{ \begin{Vmatrix} a & b & 0 \\ a' & b' & 0 \\ a'' & b'' & 0 \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{Vmatrix} \right\rangle$$

$$J_{1,3} = \left\{ \begin{Vmatrix} a & 0 & c \\ a' & 0 & c' \\ a'' & 0 & c'' \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{Vmatrix} \right\rangle, \quad J_{2,3} = \left\{ \begin{Vmatrix} 0 & b & c \\ 0 & b' & c' \\ 0 & b'' & c'' \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{Vmatrix} \right\rangle$$

$$J_\emptyset = \left\{ \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{Vmatrix} \right\}, J_{1,2,3} = \left\{ \begin{Vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{Vmatrix} \right\} = \left\langle \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{Vmatrix} \right\rangle$$

Nota. El lector no debe creer que los ideales a la izquierda de $\mathbf{M}_2(K)$ y $\mathbf{M}_3(K)$ enumerados son *todos* los ideales a la izquierda de dichos anillos. Son sólo una familia de ideales a la izquierda. Si, por ejemplo, $K = \mathbf{R}$ el cuerpo real, entonces hay infinitos ideales a la izquierda

en $\mathbf{M}_n(\mathbf{R})$, $1 < n$. Lo que es posible probar es que todo ideal a la izquierda de $\mathbf{M}_n(K)$ es isomorfo a uno del tipo J_U.

Ejemplo 3. Sea $\mathbf{C}$ el cuerpo de números complejos, sea $x \to \bar{x}$ la conjugación en $\mathbf{C}$, y $\mathbf{C}[X]$ el anillo de polinomios en X.

Sea $R = \mathbf{C}[X]$ dotado de la suma ordinaria de polinomios, pero con producto inducido por las relaciones

$$\forall\, a \in \mathbf{C},\quad \bar{a} \cdot X = X \cdot a.$$

Se deja a cargo del lector probar que R, con las operaciones de suma y producto enunciadas, es un anillo con identidad principal, sin divisores de cero $\neq 0$, a la izquierda y a la derecha. Más aún, se puede probar que existen algoritmos de división a la izquierda y a la derecha. (El lector también se encargará de precisar estos conceptos). Este ejemplo admite una generalización importante que consiste en reemplazar $\mathbf{C}$ por un cuerpo K, y la conjugación en $\mathbf{C}$ por un automorfismo de K.

Definición 2.1.4. Un R-módulo a la izquierda A se dice *noetheriano* si todo submódulo de A es de tipo finito.

Es claro que todo R-módulo noetheriano es de tipo finito, pero la recíproca es falsa, como se vio en $\mathbf{R}^{[0,1]}$.

Ejemplo. Si R es un dominio principal, entonces R (considerado como R-módulo sobre sí mismo) es un módulo noetheriano.

30 Nota. Un módulo puede tener todos sus submódulos propios de tipo finito y no ser noetheriano. En efecto, $\mathbf{Z}_{p^\infty}$, p primo, tiene esa propiedad pero no es noetheriano porque $\mathbf{Z}_{p^\infty}$ no es de tipo finito.

2. PROPIEDADES FUNDAMENTALES

Proposición 2.2.5. Sea la siguiente sucesión exacta corta de R-módulos

$$0 \to A' \xrightarrow{i} A \xrightarrow{p} A'' \to 0$$

Entonces

a) Si A es de tipo finito, así lo es A'';

b) Si A' y A'' son de tipo finito, así lo es A;

a') Si A es noetheriano, así lo es A'';

b') Si A' y A'' son noetherianos, así lo es A.

Demostración. a) Si $A = \langle a_1, \ldots, a_n \rangle$, entonces fácilmente se ve que $A'' = p(A) = \langle p(a_1), \ldots, p(a_n) \rangle$.

b) Sea $A' = \langle a'_1, \ldots, a'_r \rangle$ y $A'' = \langle a''_1, \ldots, a''_s \rangle$. Siendo p sobre, existen $a_i \in A$ $i = 1, \ldots, s$, tales que $p(a_i) = a''_i$.

Afirmación. $A = \langle i(a'_1), \ldots, i(a'_r), a_1, \ldots, a_s \rangle$.

En efecto, si $a \in A$, se tiene

$$p(a) = \sum_{i=1}^{s} r_i \cdot a''_i, \qquad r_i \in R$$

Además

$$p\Big(\sum_{i=1}^{s} r_i \cdot a_i\Big) = \sum_{i=1}^{s} r_i \cdot a_i'$$

y por lo tanto

$$a - \sum_{i=1}^{s} r_i \cdot a_i \in i(A')$$

o sea

$$i(x) = a - \sum_{i=1}^{s} r_i \cdot a_i \quad \text{con } x \in A'.$$

Sea $x = \sum_{i=1}^{r} s_i \cdot a_i'$, $s_i \in R$

entonces

$$a = \sum_{i=1}^{s} r_i \cdot a_i + \sum_{j=1}^{r} s_j \cdot i(a_j')$$

lo que prueba nuestra afirmación.

a') es consecuencia inmediata de a), y b') lo es de b). La proposición queda probada.

Probemos ahora el siguiente resultado de importancia.

Teorema 2.2.6. Sea A un R-módulo. Las propiedades siguientes son todas equivalentes entre sí.

a) A es noetheriano.

b) Si $\mathcal{F}$ es una familia no vacía de submódulos de A, $\mathcal{F}$ posee un elemento maximal en el orden parcial dado por la inclusión conjuntista. Es decir existe $T \in \mathcal{F}$ tal que no existe $H \in \mathcal{F}$ con $T \subset H$ y $T \neq H$.

c) Sea $N_1 \subset N_2 \subset \ldots$ una cadena creciente de submódulos de A. Entonces dicha cadena es ***estacionaria***, es decir existe $k \in N$ tal que $N_k = N_{k+1} = \ldots = N_{k+t}$, cualquiera que sea $t \in N$.

Demostración. a) $\Rightarrow$ c). Sea $N = \cup_i N_i$ la unión de la familia $\{N_i\}$. Por hipótesis N es de tipo finito, o sea $N = \langle a_1, \ldots, a_m \rangle$. Como

$$a_1 \in N = \cup_i N_i$$

se tiene

$$a_1 \in N_{i_1},\ a_2 \in N_{i_2}, \ldots, a_m \in N_{i_m}.$$

Pero si $t \in N$ es tal que $i_1 \leq t,\ i_2 \leq t, \ldots, i_m \leq t$, entonces $\langle a_1, a_2, \ldots, a_m \rangle \subset N_t$, con lo que

$$N = \langle a_1, \ldots, a_m \rangle \subset N_t \subset N$$

es decir $N = N_t$; por lo tanto, para todo t

$$N_t \subset N_{t+1} \subset N = N_t$$

o sea

$$N_t = N_{t+1}$$

y la cadena $N_1 \subset N_2 \subset \ldots$ es estacionaria.

c) $\Rightarrow$ b). Sea $\mathcal{I}$ una familia no vacía de submódulos de A. Supongamos que $\mathcal{I}$ *no* posee elementos maximales. Esto significa que dado $T \in \mathcal{I}$ existe $S \in \mathcal{I}$ tal que $T \subset S$ y $T \neq S$.

Entonces, construiremos inductivamente una cadena

$$N_1 \subset N_2 \subset \ldots$$

como sigue. Sea N_1 arbitrario en $\mathcal{I}$. Existe entonces $N_2 \in \mathcal{I}$, tal que $N_1 \subset N_2$ y $N_1 \neq N_2$.

Si $N_n \in \mathcal{I}$, existe $N_{n+1} \in \mathcal{I}$, tal que $N_n \subset N_{n+1}$ y $N_n \neq N_{n+1}$. Se tiene entonces una cadena $N_1 \subset N_2 \subset \ldots$ estrictamente creciente. Dado que la misma no puede ser estacionaria, se ha llegado a una contradicción.

b) $\Rightarrow$ a). Sea $N \subset A$. Probaremos que N es de tipo finito. Sea $\mathcal{I}$ la familia de submódulos de A *contenidos* en N y de tipo finito. $\mathcal{I} \neq \emptyset$, dado que $0 \subset N$ es de tipo finito. Sea, por hipótesis, $N' \in \mathcal{I}$ maximal. Si $N' = N$, entonces N es de tipo finito y no hay nada que probar. Si $N' \neq N$, sea $x \in N$, $x \notin N'$. Entonces

$$N' + \langle x \rangle$$

es de tipo finito, contenido en N y contiene estrictamente a N'. Es decir, $N' + \langle x \rangle \in \mathcal{I}$ y es tal que $N' \subset N' + \langle x \rangle$, $N' \neq N' + \langle x \rangle$, lo que es un absurdo.

El teorema queda probado.

Teorema 2.2.7. Sea R un anillo noetheriano (a la izquierda). Entonces todo R-módulo (a la izquierda) de tipo finito es noetheriano.

Demostración. Vamos a demostrar que si R es noetheriano, entonces todo submódulo de un R-módulo A de tipo finito, es de tipo finito. Razonemos inductivamente sobre el número de generadores de A. Si $A = \langle a \rangle$, entonces A es isomorfo a un cociente R/I de R por un ideal (a la izquierda) I de R. O sea, se puede considerar A como una imagen homomórfica de R, como R-módulos. Como R es noetheriano, se sigue de 2.1.5 que A es noetheriano. Sea $A = \langle a_1, \ldots, a_n, a_{n+1} \rangle$, y supongamos que todo R-módulo generado por n elementos es noetheriano. Sea $A' = \langle a_1, \ldots, a_n \rangle$. Se tiene la sucesión exacta

$$0 \to A' \xrightarrow{i} A \xrightarrow{p} A/A' \to 0$$

A/A' es cíclico, pues está generado por $p(a_{n+1})$.

Como A' y A/A' son noetherianos, resulta de 2.2.5 b') que A es noetheriano. El teorema resulta ahora del principio de inducción.

3

SUMA DIRECTA Y PRODUCTO DIRECTO

1. DEFINICIONES

Este capítulo generaliza nociones introducidas en el capítulo 1. Si bien el tratamiento es en gran parte formal y tal vez un poco tedioso, está encarado desde un punto de vista moderno y forma parte del lenguaje cotidiano del álgebra, por lo que se aconseja al lector armarse de una buena dosis de paciencia ya que, a la postre, saldrá beneficiado.

R denota un anillo con identidad $1 \neq 0$.

A denota un R-módulo a la izquierda, como siempre unitario, es decir $1 \cdot x = x$ para todo x en A.

Si $\{A_\alpha\}_{\alpha \in I}$ denota una familia de submódulos de A, con $\sum_{\alpha \in I} A_\alpha$ (o, simplemente, $\sum_\alpha A_\alpha$) entenderemos la totalidad de sumas en A:

(s) $\sum_{\alpha \in I} a_\alpha$ (o, simplemente, $\sum_\alpha a_\alpha$) con $a_\alpha \in A_\alpha$

tales que $a_\alpha = 0$ para *casi todo* índice $\alpha \in I$.

Esto significa que existe a lo sumo un número finito de índices α tales que $a_\alpha \neq 0$. Por lo tanto, a pesar del abuso de notación al escribir una suma con un número arbitrario de sumandos, (s) define unívocamente un elemento de A. Por supuesto, si I es finito, no es necesario restricción alguna. Si $I = [\![1, n]\!]$, escribimos también

$$A_1 + \ldots + A_n = \sum_{i=1}^{n} A_i$$

y sus elementos en la forma

$$a_1 + \ldots + a_n = \sum_{i=1}^{n} a_i, \quad a_i \in A_i.$$

Sea

$$x = \sum_\alpha x_\alpha \in \sum_\alpha A_\alpha$$

Proposición 3.1.1. $\sum_\alpha A_\alpha$ es submódulo de A.

Demostración. $0 \in \sum_\alpha A_\alpha$, por lo tanto $\sum_\alpha A_\alpha \neq \emptyset$. Sean

$$x = \sum_\alpha x_\alpha \text{ y } S(x) = \{\alpha / x_\alpha \neq 0\}$$

$$y = \sum_{\alpha} y_\alpha \text{ y } S(y) = \{\alpha / y_\alpha \neq 0\}.$$

Afirmamos que la familia de elementos

$$x_\alpha - y_\alpha$$

está formada por 0 para casi todo índice $\alpha \in I$. En efecto,

$$x_\alpha - y_\alpha = 0 \text{ si } \alpha \notin S(x) \cup S(y)$$

y $S(x) \cup S(y)$ es un conjunto finito. Por lo tanto

$$x - y = \sum_{\alpha} (x_\alpha - y_\alpha) \in \sum_{\alpha} A_\alpha.$$

De modo análogo probamos que si $x \in \sum_{\alpha} A_\alpha$ y $k \in R$, entonces $k \cdot x \in \sum_{\alpha} A_\alpha$, con lo que concluye la demostración de 3.1.1.

Definición 3.1.2. $\sum_{\alpha} A_\alpha$ se denomina el (sub)módulo *suma* de la familia $\{A_\alpha\}_\alpha$.

Ejemplo 1. Para todo R-módulo A, $A = 0 + A = A + A = \sum_{a \in A} \langle a \rangle$.

Ejemplo 2. En $\mathbf{Z} = R = A$,

$$\langle m_1 \rangle + \langle m_2 \rangle + \ldots + \langle m_h \rangle = \langle (m_1, m_2, \ldots, m_h) \rangle$$

donde $(m_1, m_2, \ldots, m_h)$ denota el máximo común divisor de $m_1, m_2, \ldots, m_h$.

Ejemplo 3. Sea I un conjunto no vacío cualquiera. Sea $A_\alpha = A$ para todo $\alpha \in I$. Se deja a cargo del lector verificar que $\sum_{\alpha} A_\alpha = A$.

Ejemplo 4. Sea A un R-módulo y sea X un subconjunto de A, $X \neq \emptyset$. Sea $\mathbf{P}_f(X)$ la familia de partes *finitas* de X. Si $H \in \mathbf{P}_f(X)$,

$$H = \{h_1, \ldots, h_r\},$$

podemos formar el submódulo A_H de A generado por H, esto es $A_H = \langle h_1, \ldots, h_r \rangle$. Sea

$$A_X = \sum_{H \in \mathbf{P}_f(X)} A_H.$$

A_X es un submódulo de A con las propiedades siguientes:

i) $X \subset A_X$. En efecto, si $x \in X$, $x \in \langle x \rangle = A_{\{x\}} \subset A_X$.

ii) Sea M submódulo de A tal que $X \subset M$. Afirmamos que

$$A_X \subset M$$

En efecto, sea $a \in A_X$. Existen, entonces, $H_1, \ldots, H_n \in \mathbf{P}_f(X)$ tales que

$$a \in A_{H_1} + \ldots + A_{H_n}.$$

Sea

$$H = H_1 \cup \ldots \cup H_n.$$

Entonces $H \in \mathbf{P}_f(X)$ y se tiene que

$$a \in A_{H_1} + \ldots + A_{H_n} \subset A_H.$$

Por otra parte, $H \subset X$ implica que $H \subset M$. Por ser M submódulo de A resulta la inclusión $A_H \subset M$, con lo que $a \in M$ y, en definitiva, se ha probado la inclusión $A_X \subset M$.

A_X se denomina el *submódulo de* A *generado por* X.

Definición 3.1.3. Sea $L = \sum_\alpha A_\alpha$ la suma de una familia de submódulos de A. Diremos que L es *suma directa* de $\{A_\alpha\}$ si se cumple la condición

$$0 = \sum_\alpha a_\alpha,\ a_\alpha \in A_\alpha \text{ si, y sólo si, } a_\alpha = 0 \text{ para todo índice } \alpha.$$

Proposición 3.1.4. Las propiedades siguientes son todas equivalentes entre sí. Sea $L = \sum_\alpha A_\alpha$:

i) L es suma directa de $\{A_\alpha\}_\alpha$.

ii) $0 = \sum_\alpha a_\alpha$, $a_\alpha \in A_\alpha$ implica $a_\alpha = 0$ para todo α.

iii) $\sum_\alpha x_\alpha = \sum_\alpha y_\alpha$ implica $x_\alpha = y_\alpha$ para todo $\alpha \in I$.

Demostración. i) es equivalente a ii) en virtud de la definición 3.1.3. ii) implica iii): si $\sum_\alpha x_\alpha = \sum_\alpha y_\alpha$, entonces $\sum_\alpha (x_\alpha - y_\alpha) = 0$, por lo que $x_\alpha = y_\alpha$. Por otra parte, iii) implica ii): si $0 = \sum_\alpha a_\alpha$ podemos escribir $0 = \sum_\alpha 0 \cdot a_\alpha$ y, por lo tanto, $0 = 0 \cdot a_\alpha = a_\alpha$.

Notación 3.1.5. Si L es suma directa de $\{A_\alpha\}$ escribimos

$$L = \sum_{\alpha \oplus} A_\alpha$$

Si el conjunto de índices I es finito, $I = [\![1, n]\!]$ escribimos también

$$L = \sum_{i=1}^{n \oplus} A_i = A_1 \oplus \ldots \oplus A_n.$$

Ejemplo 1. Para todo módulo A, $A = A \oplus 0$; sin embargo si $A \neq 0$, entonces $A \neq A \oplus A$ dado que si $0 \neq a \in A$, $0 = a + (-a)$ viola la propiedad ii) de 3.1.4.

Ejemplo 2. Sea $R = \mathbf{Z}$ y sea $A = \mathbf{Z}_n$ el grupo abeliano de restos módulo n. Sea $n = p_1^{i_1} \ldots p_k^{i_k}$, donde los p_j son primos distintos entre sí y los exponentes son enteros positivos. Vamos a probar la siguiente representación de $\mathbf{Z}_n$ como suma directa de subgrupos

$$\mathbf{Z}_n = \mathbf{Z}_{p_1^{i_1}} \oplus \ldots \oplus \mathbf{Z}_{p_k^{i_k}}$$

(Por ejemplo, $\mathbf{Z}_6 = \mathbf{Z}_2 \oplus \mathbf{Z}_3$, $\mathbf{Z}_{12} = \mathbf{Z}_3 \oplus \mathbf{Z}_4$, $\mathbf{Z}_{700} = \mathbf{Z}_4 \oplus \mathbf{Z}_{25} \oplus \mathbf{Z}_7$.)

Sea para cada índice j, $1 \leq j \leq k$

$$n_j = n/p_j^{i_j}$$

es decir el divisor de n que no contiene $p_j^{i_j}$. Es fácil ver que 1 es el divisor común a los $n_1, \ldots, n_k$, es decir

$$(n_1, \ldots, n_k) = \text{max. com. div. } \{n_1, \ldots, n_k\} = 1.$$

Por lo tanto, existen enteros $m_1, \ldots, m_k$, tales que

$$n_1 \cdot m_1 + \ldots + n_k \cdot m_k = 1. \tag{1}$$

Indiquemos con $\underline{a}$ la clase de $a \in \mathbf{Z}$, módulo n. Afirmamos que

$$\mathbf{Z}_n = \langle \underline{n_1} \rangle \oplus \ldots \oplus \langle \underline{n_k} \rangle.$$

Sea $x \in \mathbf{Z}$, entonces $x = (x \cdot m_1) \cdot n_1 + \ldots + (x \cdot m_k) \cdot n_k$ (según (1)) y tomando congruencia módulo n resulta

$$\underline{x} = (x \cdot m_1) \cdot \underline{n_1} + \ldots + (x \cdot m_k) \cdot \underline{n_k}$$

lo cual prueba que $\mathbf{Z}_n = \langle \underline{n_1} \rangle + \ldots + \langle \underline{n_k} \rangle$. Veamos que la suma es directa. Sea

$$0 = h_1 \cdot \underline{n_1} + \ldots + h_k \cdot \underline{n_k}, \quad h_i \in \mathbf{Z}$$

También se puede escribir (para $k > 1$)

$$(-h_1) \cdot \underline{n_1} = h_2 \cdot \underline{n_2} + \ldots + h_k \cdot \underline{n_k}$$

o sea (volviendo a $\mathbf{Z}$)

$$(-h_1) \cdot n_1 = h_2 \cdot n_2 + \ldots + h_k \cdot n_k + t \cdot n.$$

Puesto que $p_1^{i_1}$ divide a $n_2, \ldots, n_k$, n divide también al segundo miembro y, por lo tanto, al primero. Como $p_1^{i_1}$ es coprimo con n_1, $p_1^{i_1}$ divide a h_1, $h_1 = r \cdot p_1^{i_1}$. Pero, entonces

$$h_1 \cdot \underline{n_1} = r \cdot (p_1^{i_1} \cdot \underline{n_1}) = r \cdot \underline{n} = 0, \text{ (en } \mathbf{Z}_n)$$

En la misma forma probamos que $h_2 \cdot \underline{n}_2 = \ldots = h_k \cdot \underline{n}_k = 0$. La suma es pues directa. Resta ver que

$$\langle \underline{n}_j \rangle \simeq \mathbf{Z}_{p_j^{i_j}}$$

$\underline{n}_j$ = imagen de $n_j \in \mathbf{Z}$ en $\mathbf{Z}_n$, por el morfismo canónico $\mathbf{Z} \to \mathbf{Z}_n$. Se tiene

$$\langle \underline{n}_j \rangle \simeq \frac{\langle n_j \rangle}{\langle n \rangle} \simeq \mathbf{Z}_{\frac{n}{n_j}} = \mathbf{Z}_{p_j^{i_j}}$$

Nuestra afirmación queda probada.

Ejemplo 3. El ejemplo 2 admite la siguiente generalización. Sea $R = \mathbf{Z}$ y sea A un grupo abeliano *de torsión*, es decir para todo $a \in A$ existe $n \in \mathbf{N}$ tal que $n \cdot a = 0$. Sea para cada primo p:

$$A_p = \{x / x \in A \text{ y existe } m \in \mathbf{N} \text{ con } p^m \cdot a = 0\}$$

A_p es un subgrupo de A y se denomina la *componente p-primaria* de A. Entonces vale la siguiente representación de A

$$A = \sum_{p \in \mathbf{P}}^{\oplus} A_p$$

donde $\mathbf{P}$ denota el conjunto de primos racionales. La demostración de esta afirmación es enteramente análoga a la hecha en 2, por lo que la dejamos como ejercicio para el lector. Como aplicación importante se tiene la siguiente. Sea $A = \mathbf{Q}/\mathbf{Z}$. $\mathbf{Q}/\mathbf{Z}$ es un grupo de torsión. (Véase Estructuras Algebraicas, Parte I, pág. 71.) Entonces

$$\mathbf{Q}/\mathbf{Z} = \sum_{p \in \mathbf{P}}^{\oplus} (\mathbf{Q}/\mathbf{Z})_p.$$

Pero, según lo visto en 3.1.4, $(\mathbf{Q}/\mathbf{Z})_p$ se identifica a $\mathbf{Z}_{p^\infty}$. Se tiene entonces la importante igualdad

$$\boxed{\mathbf{Q}/\mathbf{Z} = \sum_{p \in \mathbf{P}}^{\oplus} \mathbf{Z}_{p^\infty}}$$

Ejemplo 4. Para el lector familiarizado con la teoría de espacios vectoriales. Sea $V = \mathbf{R}^2$ el espacio vectorial real de pares ordenados de números reales. Entonces los subespacios de $\mathbf{R}^2$ son del tipo

$$V' = 0, V' = \mathbf{R}^2 \text{ ó}$$

$$V'_{a,b} = \{(x, y) / a \cdot x + b \cdot y = 0\} \quad a, b \in \mathbf{R}.$$

Si $\mathbf{R}^2$ se representa en el plano ordinario y se fija un origen, los subespacios de V son $0, \mathbf{R}^2$ y las rectas por el origen. Se tiene

$$V = V_{a,b} \oplus V_{c,d} \text{ si, y sólo si, } a \cdot d - b \cdot c \neq 0.$$

En efecto, la condición $a \cdot d - b \cdot c \neq 0$ equivale a que las rectas $ax + by = 0$ y $cx + dy = 0$ *no* sean coincidentes. Es fácil ver que todo vector de $\mathbf{R}^2$

se escribe unívocamente como suma de vectores yacentes en dos rectas por el origen si, y sólo si, dichas rectas son distintas. La figura 2 ilustra esta propiedad.

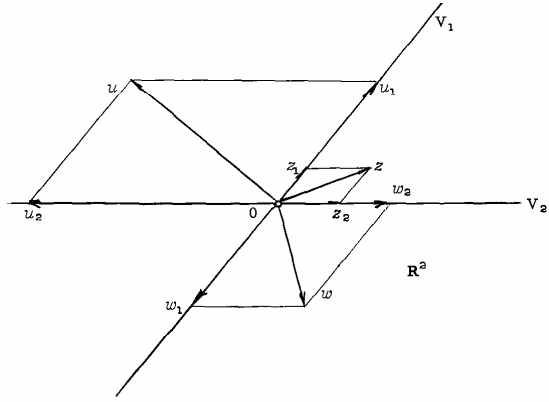


Fig. 2

38 **Proposición 3.1.6.** Sea $\{A_\alpha\}_{\alpha\in I}$ una familia de submódulos de A. Entonces $\sum_\alpha A_\alpha$ es directa si, y sólo si,

(1) $$\text{Para todo } \beta \in I, \quad (\sum_{\alpha\neq\beta} A_\alpha) \cap A_\beta = 0.$$

Demostración. Sea $\sum_\alpha A_\alpha$ directa, sea $\beta \in I$. Si

$$x \in (\sum_{\alpha\neq\beta} A) \cap A_\beta$$

se puede escribir

$$x = \sum_{\alpha\neq\beta} a_\alpha = -a_\beta$$

por lo tanto

$$0 = \sum_\alpha a_\alpha .$$

Se sigue $a_\alpha = 0$, cualquiera que sea $\alpha \in I$, o sea $x = 0$. Recíprocamente, supongamos (1) válida. Sea $\sum_\alpha a_\alpha = 0$, $a_\alpha \in A_\alpha$, si $\beta \in I$ resulta

$$- a_\beta = \sum_{\alpha\neq\beta} a_\alpha \in A_\beta \cap (\sum_{\alpha\neq\beta} A_\alpha) = 0$$

con lo que

$$a_\beta = 0.$$

La proposición queda probada.

Corolario 3.1.7. Sean A_1 y A_2 submódulos de A. Entonces

$$A = A_1 \oplus A_2$$

si, y sólo si,

$$A = A_1 + A_2 \text{ y } A_1 \cap A_2 = 0.$$

Nota. En el caso de $I = \{1, 2, 3\}$ la condición necesaria y suficiente para que $A = A_1 \oplus A_2 \oplus A_3$ es

$$\begin{cases} A = A_1 + A_2 + A_3 \\ A_1 \cap (A_2 + A_3) = A_2 \cap (A_1 + A_3) = A_3 \cap (A_1 + A_2) = 0. \end{cases}$$

Ejemplo. Sean en $V = R^2$ los siguientes submódulos

$$A_1 = \{(x, y)/x = y\}$$
$$A_2 = \{(x, y)/x = -y\}$$
$$A_3 = \{(x, y)/x = 3y\}$$

Dejamos a cargo del lector verificar que $A_i \cap A_j = 0$ si $i \neq j$, $V = A_1 + A_2 + A_3$, pero la suma *no es directa*.

2. SUMANDO DIRECTO

Definición 3.2.1. Sea A un R-módulo y sea A' un submódulo. Se dice que A' es *sumando directo* de A si existe un submódulo A'' de A tal que

$$A = A' \oplus A''.$$

Ejemplo 1. Para todo módulo A, A y 0 son sumandos directos.

Ejemplo 2. Si $V = \mathbf{R}^2$, todo submódulo de $\mathbf{R}^2$ es sumando directo. Este ejemplo muestra que para un submódulo A' de V pueden existir infinitos submódulos A'' con la propiedad $V = A' \oplus A''$.

Ejemplo 3. Sea $R = \mathbf{Z} = A$. Entonces $H = \langle m \rangle$ es sumando directo de $\mathbf{Z}$ si, y sólo si, $m = 0$ ó $m = 1$, es decir 0 y $\mathbf{Z}$ son los únicos sumandos directos. Esto es consecuencia inmediata del hecho que dos subgrupos H y K de $\mathbf{Z}$ tienen intersección 0 si, y sólo si, uno de ellos es 0.

Antes de continuar con los ejemplos, estableceremos un criterio útil para determinar la existencia de sumandos directos.

Proposición 3.2.2. Sea N y M, R-módulos a la izquierda. Entonces N es isomorfo a un sumando directo de M si, y sólo si, existen morfismos

$$N \xrightarrow{i} M \xrightarrow{p} N$$

tales que

$$p \cdot i = id_N$$

Resulta exactamente $M = Nu(p) \oplus i(N)$.

Demostración. Sea N isomorfo a un sumando directo de M, es decir sean N' y N'' submódulos de M tales que $M = N' \oplus N''$ e $i' : N \to N'$ un isomorfismo.

Si $x \in M$, podemos escribir unívocamente $x = x' + x''$, $x' \in N'$ y $x'' \in N''$, por lo tanto $p' : x \mapsto x'$ define un morfismo $p' : M \to N'$, el cual es epimorfismo y, además, $p'(x) = x$ si, y sólo si, $x \in N'$. p' se denomina *la proyección de* M *sobre* N' (*según* N'').

$$\underbrace{N \xrightarrow{i'} N' \subset M}_{i} \xrightarrow{i'^{-1} \cdot p'} \underbrace{N}_{p}$$

satisfacen, si $z \in N$

$$(p \cdot i)(z) = ((i'^{-1} \cdot p') \cdot i')(z) = i'^{-1}(p'(i'(z))) =$$
$$= i'^{-1}(i'(z)) \text{ pues } i'(z) \in N' =$$
$$= z$$

o sea $p \cdot i = id_N$, como se quería probar.

Recíprocamente, sean i, p los morfismos dados en las hipótesis. Nótese que i es un monomorfismo:

$$x \in N, i(x) = 0 \Rightarrow x = (p \cdot i)(x) = p(i(x)) = p(0) = 0.$$

Por lo tanto i induce un isomorfismo

$$i : N \to i(N) = N'.$$

Probaremos que N' es sumando directo de M. Sea $N'' = Nu(p)$.

a) $N' \cap N'' = 0$. En efecto, sea $x \in N' \cap N''$. Entonces

$$0 = p(x) \text{ y } x = i(z), \quad z \in N$$

por lo tanto

$$0 = p(x) = p(i(z)) = z \Rightarrow x = i(z) = 0.$$

b) $M = N' + N''$. En efecto, sea $x \in M$. Se tiene

$$p(x - i(p(x))) = p(x) - (p \cdot i)(p(x)) =$$
$$= p(x) - p(x) = 0$$

con lo que $x - i(p(x)) \in N''$. Por lo tanto

$$x = i(p(x)) + (x - i(p(x))).$$

Como $i(p(x)) \in i(N) = N'$, queda probado b). La proposición queda demostrada.

Corolario 3.2.3. Sea M un R-módulo a la izquierda. Entonces un submódulo N de M es sumando directo de M si, y sólo si, existe un endomorfismo $p : M \to M$ tal que

$$p^2 = p \cdot p = p, \text{ y}$$
$$N = p(M).$$

Tal morfismo se denomina un *proyector de* M *sobre* N.

Demostración. Si $M = N + N'$, entonces la proyección p de M sobre N según N' (véase 3.2.2) tiene las propiedades pedidas. Recíprocamente, sea p un proyector de M sobre N. Sea $i : N \subset M$ la inclusión, entonces

$$N \xrightarrow{i} M \xrightarrow{p} N.$$

Dado que $N = p(M)$ si $x \in N$, podemos escribir $x = p(z)$, $z \in M$. Por lo tanto

$$(p \cdot i)(x) = p(x) = p(p(z)) = p(z) = x$$

con lo que $p \cdot i = id_N$. El resultado sigue ahora en virtud de 3.2.2.

El corolario 3.2.3 muestra que hay correspondencia biyectiva entre sumandos directos de M y proyectores de M. En los ejemplos siguientes se determinará todos los proyectores en situaciones elementales.

Ejemplo 1. Sea M = R, de manera que los submódulos son los ideales a la izquierda de R. Sea p un proyector de R, entonces si $e = p(1)$, se tiene $e^2 = p(1)^2 = p(1) = e$, es decir p determina un elemento ídempotente. Recíprocamente, si $e \in R$ es ídempotente la aplicación $p : R \to R$, definida por $p(x) = x \cdot e$, es un morfismo y satisface $p^2(x) = p(p(x)) = (x \cdot e) \cdot e = x \cdot e^2 = x \cdot e = p(x)$, es decir es un proyector. Hemos probado pues que hay correspondencia biyectiva de proyectores de R e ídempotentes de R.

Puesto que, por ejemplo, en **Z** los únicos ídempotentes son 0 y 1, otra vez se tiene el resultado que los únicos sumandos directos de **Z** son 0 y **Z**.

Dejamos a cargo del lector probar la siguiente propiedad: si e es ídempotente en R, entonces $1 - e$ es ídempotente y

$$R = \langle e \rangle \oplus \langle 1 - e \rangle.$$

Dètermínese también el proyector de R sobre $\langle 1 - e \rangle$.

Ejemplo 2. Sea D un dominio de integridad. Entonces los únicos ídempotentes son 0 y 1. En efecto, sea $e \in D$, $e^2 = e$. Por lo tanto, $0 = e^2 - e = e(e - 1)$, lo cual implica $e = 0$ ó $e - 1 = 0$.

Ejemplo 3. Sea **R** el cuerpo real. Vamos a determinar todos los ídempotentes del anillo $M_2(\mathbf{R})$. Sea

$$e = \begin{Vmatrix} a & b \\ c & d \end{Vmatrix}, \qquad e^2 = e.$$

Adviértase primeramente que si e es inversible (o sea existe $x \in M_2(\mathbf{R})$ tal que $e \cdot x = x \cdot e = 1$), entonces $e = I$, dado que es posible cancelar un e en cada miembro de $e^2 = e$. Por lo tanto, se puede considerar a e no inversible. Ello implica, como es fácil de verificar que

$$0 = a \cdot d - b \cdot c.$$

La relación $e^2 = e$ da lugar a las ecuaciones

1) $\quad a^2 + b \cdot c = a$

2) $\quad a \cdot b + b \cdot d = b$, o sea $b \cdot (a + d) = b$

3) $\quad c \cdot a + d \cdot c = c$, o sea $c \cdot (a + d) = c$

4) $\quad c \cdot b + d^2 = d.$

Si $a + d = 0$, entonces $b = c = d = a = 0$, y entonces $e = 0$. Sea $a + d \neq 0$. Dado que $a \cdot d = b \cdot c$, de 1) y 4) resultan las ecuaciones

$$a \cdot (a + d) = a$$

$$d \cdot (a + d) = d.$$

Si $e \neq 0$, algún coeficiente será distinto de cero, por lo tanto se tiene que $a + d = 1$. Se ha probado pues que si e es ídempotente, entonces e está determinado por el valor $a + d$, que no es otra cosa que la traza de e, de la manera siguiente

$$\mathrm{Tr}(e) = a + d = 2, \text{ entonces } e = I$$

$$\mathrm{Tr}(e) = a + d = 1 \text{ y } a \cdot d = b \cdot c$$

$$\mathrm{Tr}(e) = a + d = 0, \text{ entonces } e = 0.$$

Recíprocamente, las matrices I, 0 y

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \text{ con } a + d = 1, \ a \cdot d = b \cdot c$$

son ídempotentes.

Ejemplo 4. Ídempotentes de $\mathbf{Z}_n$. Comencemos por recordar que los subgrupos de $\mathbf{Z}_n$ están en correspondencia biyectiva con los divisores de n. Sea $\mathbf{Z}_n = \mathbf{Z}_k \oplus \mathbf{Z}_h$. Afirmamos que $(k, h) = 1$. En efecto, sea $d = (k, h)$. Entonces, como d/k y d/h, existen en $\mathbf{Z}_k$ y $\mathbf{Z}_h$, respectivamente, subgrupos de orden d. Por lo tanto, en $\mathbf{Z}_n$ (que contiene a $\mathbf{Z}_k$ y $\mathbf{Z}_h$) existen por lo menos dos subgrupos de orden d, a saber

$$\mathbf{Z}_d + 0 \text{ y } 0 + \mathbf{Z}_d .$$

Esto es imposible, a menos que d sea 1. Nuestra primer afirmación queda probada. Recíprocamente sea $n = k \cdot h$ tal que $(h, k) = 1$. Entonces, si $1 = r \cdot h + s \cdot k$ resulta

$$r \cdot h = (r \cdot h)^2 + r \cdot s \cdot n$$

o sea

$$\underline{r} \cdot \underline{h} = (\underline{r} \cdot \underline{h})^2 \text{ en } \mathbf{Z}_n.$$

Análogamente

$$\underline{s} \cdot \underline{k} = (\underline{s} \cdot \underline{k})^2 \text{ en } \mathbf{Z}_n$$

y entonces

$$Z_n = \langle \underline{r} \cdot \underline{h} \rangle \oplus \langle \underline{s} \cdot \underline{k} \rangle$$

pero $\underline{h} = \underline{h} \cdot (\underline{r} \cdot \underline{h})$ con lo que $\langle \underline{r} \cdot \underline{h} \rangle = \langle \underline{h} \rangle = \mathbf{Z}_k$, y análogamente, $\langle \underline{s} \cdot \underline{k} \rangle = \langle \underline{k} \rangle = \mathbf{Z}_h$. Se puede escribir entonces

$$\mathbf{Z}_n = \mathbf{Z}_k \oplus \mathbf{Z}_h.$$

Hemos probado pues que los sumandos directos de $\mathbf{Z}_n$ están unívocamente determinados por los divisores k de n, tales que

$$\left(k, \frac{n}{k}\right) = 1.$$

Además, hemos calculado explícitamente los ídempotentes. En efecto, si $1 = s \cdot k + r \cdot \left(\frac{n}{k}\right)$, entonces la clase de $\underline{s} \cdot \underline{k}$ módulo n es ídempotente. Recíprocamente, si $e \in \mathbf{Z}_n$ es ídempotente, afirmamos que es de la forma $s \cdot k$. En efecto, $\mathbf{Z}_n = \langle e \rangle \oplus \langle 1 - e \rangle = \mathbf{Z}_h \oplus \mathbf{Z}_k$ con $k \cdot h = n$ y $(k, h) = 1$, donde $\langle e \rangle = \mathbf{Z}_h$, por lo tanto $e = \underline{s} \cdot \underline{k}$. Restaría por ver un detalle. Dado k/n con $\left(k, \frac{n}{k}\right) = 1$, ¿cómo determinar s? Notemos para ello que

$$1 = s \cdot k + r \cdot \frac{n}{k}$$

por lo tanto

$$1 \equiv s \cdot k \bmod\left(\frac{n}{k}\right)$$

y así se obtiene s determinando el inverso de k en $Z_{\frac{n}{k}}$.

Ilustremos con algunos ejemplos.

Ídempotentes de Z_{12}:

$$12 = 3 \cdot 4 = 1 \cdot 12$$

$3 \cdot 3 \equiv 1 \bmod(4)$, por lo tanto $\underline{3} \cdot \underline{3} = \underline{9}$ es ídempotente en $\mathbf{Z}_{12}$: $(\underline{9}^2 = \underline{81} = \underline{9}$ en $\mathbf{Z}_{12})$.

$\underline{4} \cdot \underline{1} \equiv 1 \bmod(3)$, por lo tanto $\underline{4} \cdot \underline{4} = \underline{4}$ es ídempotente en $\mathbf{Z}_{12}$.

Los ídempotentes son 0, 1 (correspondientes a la factorización $12 = 1 \cdot 12$) y $\underline{9}, \underline{4}$ (correspondientes a la factorización $12 = 3 \cdot 4$). Se deja a cargo del lector la demostración de la siguiente afirmación: Si $n =$

$= p_1^{i_1}, \ldots, p_k^{i_k}$, con p_i primos distintos entre sí, entonces el número de ídempotentes de $\mathbf{Z}_n$ es 2^k. (Recuérdese que los ídempotentes se obtienen factorizando $n = t \cdot h$ con $(t,h) = 1$ y recuérdese también que el número total de partes de un conjunto de k elementos es 2^k). Se deduce de este resultado que si $n = p^i$, $\mathbf{Z}_n$ posee dos ídempotentes (0 y 1), lo cual es claro pues los subgrupos de $\mathbf{Z}_{p^i}$ están totalmente ordenados por inclusión

$$\mathbf{Z}_p \subset \mathbf{Z}_{p^2} \subset \ldots \subset \mathbf{Z}_{p^i}.$$

Una última observación. En realidad, hemos determinado los sumandos directos de $\mathbf{Z}_n$ como $\mathbf{Z}_n$-módulo en virtud de que no hay distinción entre subgrupo de $\mathbf{Z}_n$ e ideal de $\mathbf{Z}_n$ al igual que en $\mathbf{Z}$.

3. PRODUCTO DIRECTO Y SUMA DIRECTA EXTERNA

A. Producto Directo

Sea I un conjunto de índices y $\{M_\alpha\}_{\alpha \in I}$ una familia de R-módulos (a la izquierda). Sea

$$U = \bigcup_{\alpha \in I} M_\alpha$$

la unión de la familia $\{M_\alpha\}_\alpha$, o sea un conjunto definido por la propiedad

$$x \in U \Leftrightarrow \text{existe } \alpha \in I \text{ tal que } x \in M_\alpha.$$

Definición 3.3.1. Se llama *función selectora* de la familia $\{M_\alpha\}_\alpha$, o simplemente función selectora, a toda aplicación

$$f : I \to U$$

tal que para todo

$$\alpha \in I, \quad f_\alpha = f(\alpha) \in M.$$

Si f es una función selectora, se escribe también

$$f = \{f_\alpha\}_\alpha.$$

Sea

$$\Pi_\alpha M_\alpha$$

la totalidad de funciones selectoras de la familia $\{M_\alpha\}_{\alpha \in I}$. Nótese que, $\Pi_\alpha M_\alpha \neq \emptyset$, pues $f : I \to U$ definida por $f(i) = 0$, cualquiera que sea $i \in I$, es una función selectora. Por la misma definición de función resulta:

si $f, g \in \Pi_\alpha M_\alpha$, entonces $f = g$ si, y sólo si, $f_\alpha = g_\alpha$ cualquiera que sea $\alpha \in I$.

$\Pi_\alpha M_\alpha$ se convierte en forma natural en un grupo abeliano definiendo

$$\begin{aligned} f + g &= \{f_\alpha + g_\alpha\}_\alpha \\ 0 &= \{f_\alpha\}_\alpha \text{ con } f_\alpha = 0 \text{ para todo } \alpha \in I \\ -f &= \{-f_\alpha\}_\alpha. \end{aligned}$$

Sea $k \in R$, definimos $k \cdot f$, si $f \in \Pi_\alpha M_\alpha$ por

$$k \cdot f = \{k \cdot f_\alpha\}_\alpha .$$

Es un ejercicio sencillo verificar que, en esas condiciones, $\Pi_\alpha M_\alpha$ queda dotado de una estructura de R-módulo (a la izquierda).

Definición 3.3.2. Se llama *producto directo* de la familia $\{M_\alpha\}_{\alpha \in I}$ al conjunto ΠM_α dotado de la estructura de R-módulo definida ya.

Sea para cada $\beta \in I$

$$p_\beta : \Pi_\alpha M_\alpha \to M_\beta$$

la aplicación

$$p_\beta(f) = f_\beta .$$

p_β satisface las propiedades siguientes

i) p_β es sobre

ii) $p_\beta(f + g) = p_\beta\{f_\alpha + g_\alpha\} = f_\beta + g_\beta = p_\beta(f) + p_\beta(g)$

iii) $p_\beta(k \cdot f) = p_\beta\{k \cdot f_\alpha\} = k \cdot f_\beta$ si $k \in R$

es decir, p_β es un epimorfismo.

Definición 3.3.3. Llamaremos a p_β la proyección sobre M_β o también la β-*proyección* de $\Pi_\alpha M_\alpha$.

Sea, por otra parte, para cada $\beta \in I$

$$i_\beta : M_\beta \to \Pi_\alpha M_\alpha$$

la aplicación definida por

$$i_\beta(x) = f \text{ con}$$
$$f_\alpha = 0, \text{ si } \alpha \neq \beta$$
$$f_\beta = x$$

i_β es un monomorfismo que satisface además

$$p_\beta \cdot i_\beta = id_\beta, \text{ donde } id_\beta = id_{M_\beta}$$
$$p_\alpha \cdot i_\beta = 0, \text{ si } \alpha \neq \beta .$$

Definición 3.3.4. Llamaremos al morfismo i_β la β-*inclusión canónica.*

Ejemplo. Sea $I = [\![1, n]\!]$. Sea $\{M_j\}_{j \in I}$. El producto directo de M_j consiste en la totalidad de funciones f que se pueden escribir

$$f = (f_1, f_2, \ldots, f_n),\ f_i \in M_i$$

y que llamaremos *n-uplas*. Las operaciones de R-módulo en ΠM_i son

$$f + g = (f_1 + g_1, f_2 + g_2, \ldots, f_n + g_n)$$

$$k \cdot f = (k \cdot f_1, k \cdot f_2, \ldots, k \cdot f_n)$$

En vez de $\Pi_i M_i$, escribiremos indistintamente

$$\Pi_{i=1}^{n} M_i = M_1 \times \ldots \times M_n.$$

El teorema que sigue ilustra un tipo de situación corriente en álgebra abstracta: un cierto objeto queda determinado en virtud de ser solución de un "problema de tipo universal". El lector tendrá oportunidad de encontrar muchos ejemplos al respecto. Un caso en donde ha mostrado gran utilidad es el del producto tensorial (véase (3c) ó (5)).

Teorema 3.3.5. Sea $\{M_\alpha\}_{\alpha \in I}$ una familia de R-módulos. Entonces

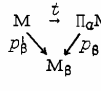
$$\langle \Pi_\alpha M_\alpha; p_\alpha \rangle$$

es el único objeto (salvo isomorfismos) con la siguiente propiedad: Cualquiera que sea el objeto

$$\langle M; p'_\alpha, \ \alpha \in I \rangle = \langle M; p'_\alpha \rangle$$

formado por un R-módulo M y morfismos $p'_\alpha : M \to M_\alpha$ existe un *único* morfismo $t : \mathbf{M} \to \Pi_\alpha M_\alpha$ tal que (para todo $\beta \in I$) el diagrama

(d)



es conmutativo.

Demostración. Probemos primero que $\langle \Pi_\alpha M_\alpha; p_\alpha \rangle$ posee la propiedad enunciada. Sea $m \in M$, entonces

$$\alpha \mapsto p'_\alpha(m)$$

define una función selectora $t(m)$ de la familia $\{M_\alpha\}$, o sea

$$t(m) \in \Pi_\alpha M_\alpha$$

Además, para todo m

$$p_\alpha t(m) = p'_\alpha(m)$$

o sea

$$p_\alpha \cdot t = p'_\alpha$$

la cual hace conmutativo el diagrama (d). Por otra parte, si $t' : M \to \Pi_\alpha M_\alpha$ es otro morfismo que hace conmutativo (d), se tiene para todo m,

$$p_\beta(t'(m)) = (p_\beta \cdot t')(m) = p'(m) = (p_\beta \cdot t)(m) = p_\beta(t(m))$$

lo cual demuestra que para $m \in M$

$$t'(m) = t(m)$$

o sea $t = t'$.

Consideremos la cuestión de unicidad. Vamos a probar que si

$$\langle P; \bar{p}_\beta : P \to M_\beta \rangle$$

tiene las propiedades enunciadas en el teorema, entonces existe un isomorfismo $\theta : \Pi M \to P$ tal que el diagrama

$$\begin{array}{ccc} \Pi_\alpha M_\alpha & \xrightarrow{\theta} & P \\ & {\scriptstyle p_\beta}\searrow \quad \swarrow{\scriptstyle \bar{p}_\beta} & \\ & M_\beta & \end{array}$$

es conmutativo.

Aplicando la parte ya demostrada del teorema se pueden definir morfismos que hacen conmutativos los diagramas.

$$\begin{array}{ccc} \Pi_\alpha M_\alpha & \xrightarrow{\theta} & P \\ & {\scriptstyle p_\beta}\searrow \quad \swarrow{\scriptstyle \bar{p}_\beta} & \\ & M_\beta & \end{array} \qquad \begin{array}{ccc} P & \xrightarrow{\theta'} & \Pi_\alpha M_\alpha \\ & {\scriptstyle \bar{p}_\beta}\searrow \quad \swarrow{\scriptstyle p_\beta} & \\ & M_\beta & \end{array}$$

Además

$$p_\beta \cdot (\theta' \cdot \theta) = (p_\beta \cdot \theta') \cdot \theta = \bar{p}_\beta \cdot \theta = p_\beta$$

$$\bar{p}_\beta \cdot (\theta \cdot \theta') = (\bar{p}_\beta \cdot \theta) \cdot \theta' = p \cdot \theta' = \bar{p}_\beta$$

lo cual dice que los diagramas siguientes son conmutativos

$$\begin{array}{ccc} \Pi_\alpha M_\alpha & \xrightarrow{\theta' \cdot \theta} & \Pi_\alpha M_\alpha \\ & {\scriptstyle p_\beta}\searrow \quad \swarrow{\scriptstyle p_\beta} & \\ & M_\beta & \end{array} \qquad \begin{array}{ccc} P & \xrightarrow{\theta \cdot \theta'} & P \\ & {\scriptstyle \bar{p}_\beta}\searrow \quad \swarrow{\scriptstyle \bar{p}_\beta} & \\ & M_\beta & \end{array}$$

pero, trivialmente, se tienen también los diagramas conmutativos

$$\begin{array}{ccc} \Pi M & \xrightarrow{\mathrm{id}} & \Pi M \\ & {\scriptstyle p_\beta}\searrow \quad \swarrow{\scriptstyle p_\beta} & \\ & M_\beta & \end{array} \qquad \begin{array}{ccc} P & \xrightarrow{\mathrm{id}} & P \\ & {\scriptstyle \bar{p}_\beta}\searrow \quad \swarrow{\scriptstyle \bar{p}_\beta} & \\ & M_\beta & \end{array}.$$

Por la unicidad establecida en el teorema

$$\theta' \cdot \theta = \mathrm{id} \quad \text{y} \quad \theta \cdot \theta' = \mathrm{id}$$

lo cual prueba que θ es un isomorfismo con las propiedades pedidas. El teorema queda completamente demostrado.

B. Suma Directa Externa

Sea $\{M_\alpha\}_{\alpha \in I}$ una familia de R-módulos y $\Pi_\alpha M_\alpha$ su producto directo. Sea S el siguiente subconjunto de $\Pi_\alpha M_\alpha$

$$f \in S \Leftrightarrow f_\alpha = 0 \text{ para } \textit{casi todo } \alpha \in I$$

Por ejemplo

$$\begin{cases} 0 \in S \\ \text{para todo } \beta \in I,\ x \in M_\beta,\ i_\beta(x) \in S. \end{cases}$$

Nótese que si I es finito, entonces $S = \Pi M_\alpha$, y recíprocamente, si $S = \Pi_\alpha M_\alpha$, I debe ser finito ó $M_\alpha = 0$ para casi todo $\alpha \in I$. Las siguientes propiedades son válidas en S

$$f, g \in S \rightarrow f - g \in S$$
$$k \in R,\ f \in S \rightarrow k \cdot f \in S$$

de manera que S es un submódulo de $\Pi_\alpha M_\alpha$.

Definición 3.3.6. Se llama *suma directa externa,* o simplemente *suma directa* de la familia $\{M_\alpha\}_{\alpha \in I}$, al conjunto S con la estructura de R-módulo definida ya. Escribiremos

$$S = \oplus_\alpha M_\alpha$$

y si $I = [\![1, n]\!]$ es finito

$$S = \oplus_{i=1}^{n} M_i = M_1 \oplus \ldots \oplus M_n.$$

Propiedad 3.3.7. Sea $m \in \oplus_\alpha M_\alpha$. Entonces $m = \{m_\alpha\} = \sum_\alpha i_\alpha(m_\alpha)$. En efecto, para todo $\beta \in I$

$$m_\beta = p_\beta(\{m_\alpha\})$$

y además

$$m_\beta = p_\beta \cdot i_\beta(m_\beta) = p_\beta\Big(\sum_\alpha i_\alpha(m_\alpha)\Big) \quad (\text{pues } p_\beta \cdot i_\alpha = 0, \text{ si } \beta \neq \alpha)$$

por lo tanto

$$m = \sum_\alpha i_\alpha(m_\alpha)$$

dado que tienen las mismas proyecciones.

Probemos un teorema análogo al 3.3.5.

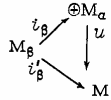
Teorema 3.3.8. Sea $\{M_\alpha\}_{\alpha \in I}$ una familia de R-módulos. Entonces

$$\langle \oplus_\alpha M_\alpha, i_\alpha \rangle$$

es el único objeto (salvo isomorfismos) con la siguiente propiedad: Cualquiera que sea el objeto

$$\langle M, i'_\alpha \rangle,\ i'_\alpha : M_\alpha \rightarrow M$$

existe un único morfismo $u : \oplus_\alpha M_\alpha \rightarrow M$, tal que, para todo $\beta \in I$, el diagrama



es conmutativo.

Demostración. Sea $f \in \oplus_\alpha M_\alpha$, entonces $f_\alpha = 0$ para casi todo $\alpha \in I$ por lo que

$$u(f) = \sum_\alpha i'_\alpha(f_\alpha)$$

está bien definido en M. De esta manera

$$\{f_\alpha\} \mapsto u(f)$$

define un morfismo

$$u : \oplus_\alpha M_\alpha \to M$$

que satisface, para todo $\beta \in I$, $m \in M_\beta$,

$$u(i_\beta(m)) = \sum_\alpha i'_\alpha((i_\beta(m))_\alpha) = i'_\beta(m)$$

es decir

$$u \cdot i_\beta = i'_\beta$$

como se quería probar. Si $u' : \oplus_\alpha M_\alpha \to M$ es otro morfismo que hace conmutativo el diagrama se tiene, para todo $f \in \oplus_\alpha M_\alpha$,

$$\begin{aligned} u(f) = \sum_\alpha i'_\alpha(f) &= \sum_\alpha u' \cdot i_\alpha(f_\alpha) = \\ &= u'(\sum_\alpha i_\alpha(f_\alpha)) = \\ &= u'(f) \quad \text{(por 3.3.7)} \end{aligned}$$

con lo que $u = u'$.

La unicidad del objeto, salvo isomorfismos, se prueba de la misma forma que en 3.3.5.

Ejemplo. Sea M un R-módulo y sea $\{M_\alpha\}_\alpha$ una familia de *sub*módulos de M. Sea $I' : M_\alpha \to M$ la inclusión natural. Existe entonces un (único) morfismo $u : \oplus_\alpha M_\alpha \to M$, tal que $u \cdot i_\beta = i'_\beta$. Se verifica

a) $u(\oplus M_\alpha) = \sum_\alpha M_\alpha$ (submódulo suma de $\{M_\alpha\}$)

b) $\sum_\alpha M_\alpha$ es directa si, y sólo si, u es monomorfismo.

En efecto, a) está claro. b) Si u es monomorfismo y $0 = \sum_\alpha m_\alpha$ con $m_\alpha \in M_\alpha$ y $m_\alpha = 0$ para casi todo α, entonces $m = \{m_\alpha\} \in \oplus_\alpha M_\alpha$ y

$$u(m) = \sum_\alpha i'_\alpha(m_\alpha) = \sum_\alpha m_\alpha = 0,$$

como u es monomorfismo se tiene que $m = 0$, o sea $m_\alpha = 0$ para todo α. Recíprocamente, sea $f = \{f_\alpha\}_\alpha \in \oplus_\alpha M_\alpha$ con $u(f) = 0$. Entonces por la propiedad 3.2.2 $f = \sum_\alpha i_\alpha(f)$, con lo que $0 = u(f) = \sum_\alpha u(i_\alpha(f_\alpha)) = \sum_\alpha i'_\alpha(f_\alpha)$.

Como $\sum_{\alpha} M_\alpha$ es directa, es $i'_\alpha(f_\alpha) = 0$ para todo α, o sea $f_\alpha = 0$ para todo α, y así $f = 0$, lo cual prueba que u es un monomorfismo.

En particular, si

$$M = \sum_{\alpha \oplus} M_\alpha$$

se tiene un isomorfismo

$$\boxed{\oplus_\alpha M_\alpha \simeq \sum_{\alpha \oplus} M_\alpha}$$

lo cual muestra que ambos conceptos de suma directa (interna y externa) se relacionan naturalmente.

C. Hom, $\oplus$ y Π

Sea $M = \oplus_\alpha M_\alpha$ y N un R-módulo. Sean

$$\mathrm{Hom}_R(M,N) \text{ y la familia}$$
$$\{\mathrm{Hom}_R(M_\alpha, N)\}_{\alpha \in I}.$$

La inclusión canónica $i : M_\alpha \to M$ induce un morfismo de grupos abelianos

$$p'_\alpha : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M_\alpha, N),\ p'_\alpha(f) = f \cdot i_\alpha.$$

Por lo tanto, de acuerdo con 3.3.5, existe un morfismo $t : \mathrm{Hom}_R(M, N) \to \Pi_\alpha \mathrm{Hom}_R(M_\alpha, N)$ tal que el diagrama

$$\begin{array}{ccc} \mathrm{Hom}_R(M, N) & \xrightarrow{t} & \Pi_\alpha \mathrm{Hom}_R(M_\alpha, N) \\ & {\scriptstyle p'_\alpha} \searrow \quad \swarrow {\scriptstyle p_\alpha} & \\ & \mathrm{Hom}_R(M_\alpha N) & \end{array}$$

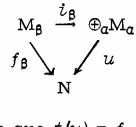
es conmutativo.

Proposición 3.3.9. t es un isomorfismo.

Demostración. Sea $f \in \mathrm{Hom}_R(M, N) \cdot (tf)_\alpha = p'_\alpha(f) = f \cdot i_\alpha$. Luego $t(f) = 0$ si, y sólo si, para todo $\alpha \in I$, $(tf)_\alpha = 0$. Si $t(f) = 0$, entonces $p'_\alpha(f) = 0$ para todo $\alpha \in I$, por lo tanto los diagramas siguientes son conmutativos

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle i_\alpha} \uparrow & \nearrow {\scriptstyle p'_\alpha} & \\ M_\alpha & & \end{array} \qquad \begin{array}{ccc} M & \xrightarrow{0} & N \\ {\scriptstyle i_\alpha} \uparrow & \nearrow {\scriptstyle p'_\alpha} & \\ M_\alpha & & \end{array}$$

Pero, en virtud de 3.3.8, debe ser $f = 0$ por razones de unicidad, lo cual prueba que t es un monomorfismo. Recíprocamente, sea $f = \{f_\alpha\}$, $f_\alpha : M_\alpha \to N$. Existe, en virtud de 3.3.8, un (único) morfismo $u : \oplus_\alpha M_\alpha \to N$, tal que el diagrama



es conmutativo. Afirmamos que $t(u) = f$. En efecto,

$$p_\alpha\{t(u)\} = p'_\alpha(u) = u \cdot t_\alpha = f_\alpha = p_\alpha(f)$$

para todo $\alpha \in I$. Por lo tanto, $t(u) = f$, como se quería probar.

Nota. La afirmación de la proposición 3.3.9 se puede escribir en la forma

$$\boxed{\mathrm{Hom}_R(\oplus_\alpha M_\alpha, N) \simeq \Pi_\alpha \mathrm{Hom}_R(M_\alpha, N)}$$

Se deja a cargo del lector demostrar en forma análoga

$$\boxed{\mathrm{Hom}_R(M, \Pi_\alpha N_\alpha) \simeq \Pi_\alpha \mathrm{Hom}_R(M, N_\alpha)}$$

Se suele decir entonces que Hom *conmuta* con sumas directas en la primer variable y con productos directos en la segunda. Pero no dejemos de notar en el primer caso que $\oplus$ no sale de Hom como tal, sino como producto directo.

Si el conjunto de índices es finito, entonces $\Pi_\alpha M_\alpha = \oplus_\alpha M_\alpha$ por lo tanto 51

$$\mathrm{Hom}_R(M, \oplus_{i=1}^n N_i) \simeq \oplus_{i=1}^n \mathrm{Hom}_R(M, N_i).$$

Veamos una aplicación. Sea para cada $n \in N$

$$\oplus^n \mathbf{Z} = \mathbf{Z}^n = \mathbf{Z} \oplus \ldots \oplus \mathbf{Z} \quad (n \text{ copias de } \mathbf{Z})$$

Proposición 3.3.10. $\mathbf{Z}^n \simeq \mathbf{Z}^m \Leftrightarrow n = m$.

Demostración. Sea en efecto, $f : \mathbf{Z}^n \to \mathbf{Z}^m$ un isomorfismo. Entonces f induce un isomorfismo $f_* = \mathrm{Hom}_{\mathbf{Z}}(f, \mathbf{Z}_p)$

$$f_* : \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}^m, \mathbf{Z}_p) \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}^n, \mathbf{Z}_p)$$

donde p es un número primo.

Pero dado que

$$\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}^m, \mathbf{Z}_p) \simeq \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_p) \oplus \ldots \oplus \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_p) \quad (m \text{ copias}) =$$
$$= \oplus^m \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_p)$$

(donde por $\oplus^m \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_p)$ no se entiende otra cosa que la suma directa de $m$copias isomorfas a $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_p)$)se tiene, recordando que $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_p) \simeq \mathbf{Z}_p$, un isomorfismo

$$\underbrace{\mathbf{Z}_p \oplus \ldots \oplus \mathbf{Z}_p}_{m \text{ copias}} \simeq \underbrace{\mathbf{Z}_p \oplus \ldots \oplus \mathbf{Z}_p}_{n \text{ copias}}$$

Pero ambos grupos ya escritos son *finitos* de orden

$$p^n \text{ y } p^n$$

respectivamente. Puesto que un isomorfismo preserva la cardinalidad debe verificarse

$$p^n = p^n$$

con lo que $n = m$.

Ejemplo 1. Sea $\mathbf{P}$ el conjunto de números primos racionales. Sea $\mathbf{P} = \mathbf{P}_1 \cup \mathbf{P}_2$ una partición de $\mathbf{P}$.

Sea A_1 la totalidad de racionales que admiten una representación irreducible $\frac{a}{b}$, $a, b \in \mathbf{Z}$, tal que $p \in \mathbf{P}_1 \Rightarrow p \nmid b$. Análogamente se define A_2. Se tiene entonces la sucesión exacta

$$0 \to \mathbf{Z} \xrightarrow{u} A_1 \oplus A_2 \xrightarrow{v} \mathbf{Q} \to 0$$

donde $u(m) = (m, m)$ y $v(a_1, a_2) = a_1 - a_2$. Se deja a cargo del lector probar que la sucesión exacta anterior no es equivalente a la sucesión exacta trivial

$$0 \to \mathbf{Z} \xrightarrow{j} \mathbf{Z} \oplus \mathbf{Q} \xrightarrow{t} \mathbf{Q} \to 0$$

$s(n) = (n, 0)$, $t(n, q) = q$. Un ejercicio interesante es hallar sucesiones exactas

$$0 \to \mathbf{Z} \to A \to \mathbf{Q} \to 0$$

con la propiedad de que A sea un grupo abeliano indescomponible, es decir no es posible representar A en la forma $A = A_1 \oplus A_2$, con $A_1 \neq 0 \neq A_2$.

Ejemplo 2. Sea R un anillo conmutativo. Sea $A^* = \mathrm{Hom}_R(A, R)$ el módulo dual de A (véase 1.5.7, ejemplo 2). Entonces A^* se puede "sumergir" en forma natural en un producto directo de copias de R. Dicho en forma más precisa, existe un monomorfismo $A^* \to \Pi_I R$, de A en un producto directo de I-copias de R (considerado como R-módulo). En efecto, sea I = A, entonces es fácil verificar que

$$f \to \{f(a)\}_{a \in A}$$

es un monomorfismo de A^* en $\Pi_A R$.

Ejemplo 3. Sea R un anillo conmutativo y sea $A = A_1 \oplus A_2$, suma directa de R-módulo. Entonces se verifica la igualdad

$$A^* = A_1^* \oplus A_2^*$$

lo cual se expresa diciendo que la dualidad de módulos conmuta con sumas directas *finitas*. Es fácil ver que la dualidad no conmuta con sumas directas infinitas. En efecto

$$(\oplus \mathbf{Z})^* \simeq \Pi \mathbf{Z} \text{ (no numerable)}$$

en tanto que $\oplus \mathbf{Z}^* \simeq \oplus \mathbf{Z}$ (numerable). $\Pi \mathbf{Z}$ y $\oplus \mathbf{Z}$ denotan producto y suma directa, respectivamente, de un conjunto infinito numerable de copias del grupo $\mathbf{Z}$.

4

MÓDULOS LIBRES

1. DEFINICIÓN Y EJEMPLOS

Sea A un R-módulo a la izquierda.

Definición 4.1.1. Se dice que un subconjunto B de A, determinado por un conjunto de índices $B = \{b_\alpha\}_{\alpha \in I}$, $b_\alpha \in A$ es una *base* de A como R-módulo, o simplemente es una base de A si

B1) B es un sistema de generadores de A, es decir para todo $x \in A$ existe $\{r_\alpha\}_\alpha$, $r_\alpha \in R$, tales que $r_\alpha = 0$ para casi todo $\alpha \in I$ y

$$x = \sum_\alpha r_\alpha \cdot b_\alpha.$$

B2) B es un conjunto R-linealmente independiente, es decir si $0 = \sum_\alpha r_\alpha \cdot b_\alpha$; $r_\alpha \in R$, $r_\alpha = 0$ para casi todo $\alpha \in I$, entonces

$$r_\alpha = 0, \quad \textit{para todo } \alpha \in I.$$

Las condiciones B1) y B2) son equivalentes a la siguiente condición

$$A = \sum_{\alpha \oplus} \langle b_\alpha \rangle$$

como el lector puede verificar simplemente repasando la definición de suma directa interna.

Definición 4.1.2. Un R-módulo se dice *libre* si posee una base.

Ejemplo 1. 0 es un módulo libre, por definición.

Ejemplo 2. Sea R un anillo con identidad 1. Entonces R es un módulo libre a la izquierda (y a la derecha). Una base la constituye el conjunto $B = \{1\}$. Por ejemplo en el caso de los enteros racionales **Z**, las únicas bases de **Z**, como **Z**-módulo, son $B = \{1\}$ y $B = \{-1\}$.

Es fácil ver cuando un subconjunto $B = \{u\}$ del anillo R es base de R. La afirmación es la siguiente: $B = \{u\}$ es base de R, como R-módulo a la izquierda, si, y sólo si, u es inversible. Probemos esta afirmación:

i) Sea u inversible. Entonces, si $x \in R$, podemos escribir

$$x = (x \cdot u^{-1}) \cdot u \quad \text{con lo que} \quad R = \langle u \rangle.$$

Debemos probar que $\{u\}$ es linealmente independiente. Sea

$$y \cdot u = 0, \; y \in R$$

entonces $y = y \cdot (u \cdot u^{-1}) = (y \cdot u) \cdot u^{-1} = 0$, como se quería probar.

ii) Sea $\{u\}$ base de R. Entonces $1 = v \cdot u$, y así u posee un inverso a la izquierda. Debemos probar que $u \cdot v = 1$. Para ello notemos que

$$(u \cdot v - 1) \cdot u = u \cdot (v \cdot u) - u = u - u = 0$$

y como u es una base debe ser $u \cdot v = 1$. Nuestra afirmación queda probada.

Ejemplo 2'. El ejemplo 2) admite la siguiente generalización. Sea I un conjunto no vacío. Sea $\{R_\alpha\}_{\alpha \in I}$ la familia de R-módulos a la izquierda definida así: para todo $\alpha \in I$, $R \simeq R_\alpha$ como R-módulos. Formemos

$$\bigoplus_{\alpha \in I} R_\alpha$$

la suma directa de la familia $\{R_\alpha\}$. Esta suma directa la denotaremos también por

$$\oplus^I R.$$

El conjunto $B = \{e_\alpha\}$, donde $e_\alpha = i_\alpha(1_\alpha)$, 1_α denota la imagen de 1 en el isomorfismo $R \simeq R_\alpha$, e i_α la inclusión canónica $R_\alpha \to \bigoplus_\alpha R_\alpha$, es una base de $\oplus^I R$, llamada la *base canónica*.

54 Si $I = [\![1, n]\!]$ entonces escribiremos

$$R^n = \oplus^n R = \oplus^{[\![1,n]\!]} R = R \oplus \ldots \oplus R$$

indistintamente. La base canónica de R^n se escribe así

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0) \\ &\cdots\cdots \\ e_i &= (0, \ldots, \overset{i}{1}, \ldots 0) \\ &\cdots\cdots \\ e_n &= (0, \ldots, 0, 1). \end{aligned}$$

Si I = N (el conjunto de número naturales), la base canónica de

$$\oplus^N R$$

se escribe así

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0, \ldots) \\ e_2 &= (0, 1, 0, \ldots, 0, \ldots) \\ e_3 &= (0, 0, 1, 0, \ldots, 0, \ldots) \\ &\cdots\cdots \end{aligned}$$

en general e_n es la sucesión que tiene todos ceros, salvo en el lugar n-ésimo donde tiene un 1.

Ejemplo 3. Sea $R = \mathbf{Z}$ y $A = \mathbf{Z} \oplus \mathbf{Z}$. A es un módulo libre y su base canónica es $B = \{(1, 0), (0, 1)\}$. En este ejemplo vamos a determinar

todas las bases de $\mathbf{Z}^2 = \mathbf{Z} \oplus \mathbf{Z}$. Primeramente probamos que

$$b_1 = (x_1, y_1), \quad b_2 = (x_2, y_2)$$

es una base de A si, y sólo si, $x_1 \cdot y_2 - y_1 \cdot x_2 = \pm 1$. En efecto, $\{b_1, b_2\}$ es base de A $\Leftrightarrow$ Para todo $(x, y) \in \mathbf{Z} \oplus \mathbf{Z}$ existen únicos $r_1, r_2 \in \mathbf{Z}$, tales que $(x, y) = r_1 \cdot b_1 + r_2 \cdot b_2$ $\Leftrightarrow$ Para todo $(x, y) \in \mathbf{Z} \oplus \mathbf{Z}$ el sistema lineal

$$(1) \qquad \begin{aligned} r_1 \cdot x_1 + r_2 \cdot x_2 &= x \\ r_1 \cdot y_1 + r_2 \cdot y_2 &= y \end{aligned}$$

admite solución única r_1, r_2 en $\mathbf{Z} \Leftrightarrow x_1 \cdot y_2 - x_2 \cdot y_1 = \pm 1$.

Justifiquemos la última equivalencia. Operando sobre (1) se obtiene

$$(2) \qquad \begin{aligned} (x_1 \cdot y_2 - y_1 \cdot x_2) \cdot r_2 &= x_1 \cdot y - y_1 \cdot x \\ (x_1 \cdot y_2 - y_1 \cdot x_2) \cdot r_1 &= x \cdot y_2 - y \cdot x_2. \end{aligned}$$

Por lo tanto, si $x_1 \cdot y_2 - y_1 \cdot x_2 = \pm 1$, los valores de r_1, r_2 se obtienen inmediatamente de (2), al igual que la unicidad. Recíprocamente, supongamos que (1) admite solución única cualquiera que sea $(x, y) \in \mathbf{Z} \oplus \mathbf{Z}$. Eligiendo $(x, y) = (0, 0)$, la unicidad de la solución $r_1 = 0$, $r_2 = 0$ implica que $x_1 \cdot y_2 - y_1 \cdot x_2 \neq 0$. Eligiendo $(x, y) = (1, 0)$, $(0, 1)$, se sigue de (2) que

$$x_1 \cdot y_2 - y_1 \cdot x_2 \text{ divide a } x_1, y_1, x_2, y_2$$

dado que las soluciones r_1, r_2 son números enteros. Si

$$x_1 \cdot y_2 - y_1 \cdot x_2 \neq \pm 1$$

entonces el máximo común divisor de x_1, x_2, y_1, y_2 es un número d, $1 < d$. Pero entonces alguno de los sistemas

$$\begin{cases} r_1 \cdot x_1 + r_2 \cdot x_2 = \dfrac{x_1}{d} \\ r_1 \cdot y_1 + r_2 \cdot y_2 = \dfrac{y_1}{d} \end{cases} \qquad \begin{cases} r_1 \cdot x_1 + r_2 \cdot x_2 = \dfrac{x_2}{d} \\ r_1 \cdot y_1 + r_2 \cdot y_2 = \dfrac{y_2}{d} \end{cases}$$

no admite solución, dado que los miembros izquierdos son divisibles por d pero no así algún miembro derecho. Esto contradice la hipótesis, por lo tanto $x_1 \cdot y_2 - y_1 \cdot x_2 = \pm 1$. Nuestra afirmación queda probada.

Notemos que en $\mathbf{Z} \oplus \mathbf{Z}$ toda base tiene dos elementos. En efecto, si $B = \{b\}_{\alpha \in I}$ es una base de $\mathbf{Z} \oplus \mathbf{Z}$, entonces

$$(3) \qquad \oplus^2 \mathbf{Z} = \mathbf{Z}^2 = \oplus_{\alpha \in I} \langle b_\alpha \rangle \simeq \oplus^I \mathbf{Z}$$

(donde $\oplus^I \mathbf{Z}$ denota la suma directa de una familia $\{M_\alpha\}_{\alpha \in I}$ de $\mathbf{Z}$-módulos, todos isomorfos a $\mathbf{Z}$).

Aplicando $\mathrm{Hom}_{\mathbf{Z}}(\ , \mathbf{Z}_p)$, con p primo, a (3) se tiene

$$\mathbf{Z}_p \oplus \mathbf{Z}_p \simeq \Pi^I \mathbf{Z}_p.$$

Por razones de cardinalidad I debe ser finito y contener dos elementos. Nuestra afirmación queda probada.

Sea $(u, v) \in \mathbf{Z} \oplus \mathbf{Z}$. Nos preguntamos: ¿En qué condiciones existe (u', v') en $\mathbf{Z} \oplus \mathbf{Z}$, tal que $\{(u, v), (u', v')\}$ constituya una base de $\mathbf{Z} \oplus \mathbf{Z}$. Una condición suficiente es que existan enteros u', v', tales que $u \cdot v' - v \cdot u' = \pm 1$, pues entonces (u, v), (u', v') tiene las propiedades pedidas. La condición es evidentemente necesaria según el criterio probado al principio de este ejemplo. Ahora la condición $u \cdot v' - v \cdot u' = \pm 1$ implica que u y v son coprimos (o primos entre sí). Recíprocamente, si u y v son coprimos existen enteros u', v', tales que $u \cdot v' + v \cdot u' = 1$, o también $u \cdot v' - v \cdot (-u') = 1$.

Por lo tanto, (u, v) se extiende a una base de $\mathbf{Z} \oplus \mathbf{Z}$ si, y sólo si, u y v son coprimos. Esta misma condición es necesaria y suficiente para que el elemento (u, v) genere un sumando directo de $\mathbf{Z} \oplus \mathbf{Z}$. Por ejemplo,

$$\mathbf{Z} \oplus \mathbf{Z} = \langle (1, 3) \rangle \oplus \langle (4, 11) \rangle = \langle (1, 1) \rangle \oplus \langle (6, 7) \rangle.$$

Ejemplo 4. Sea $\mathbf{Z}^n = \mathbf{Z} \oplus \ldots \oplus \mathbf{Z}$ (n copias). Sea $a = (a_1, \ldots, a_n) \in \mathbf{Z}^n$, $a \neq 0$. Entonces a genera un sumando directo de $\mathbf{Z}^n$, si, y sólo si, el máximo común divisor de $\{a_1, \ldots, a_n\} = 1$. En efecto, si el máximo común divisor de $\{a_1, \ldots, a_n\} = 1$, existen entonces enteros $r_1, \ldots, r_n$, tales que

$$\sum_{i=1}^{n} r_i \cdot a_i = 1.$$

La aplicación $p : \mathbf{Z}^n \to \mathbf{Z}^n$ definida por $p(x_1, \ldots, x_n) = (\sum_i r_i \cdot x_i) \cdot (a_1, \ldots, a_n)$

es un proyector de $\mathbf{Z}^n$ sobre $\langle a \rangle$. Para ello obsérvese que $p(a) = (\sum_i r_i \cdot a_i) \cdot a = a$. Recíprocamente, si p es un proyector de $\mathbf{Z}^n$ sobre $\langle a \rangle$, $e_1 = (1, 0, \ldots, 0), \ldots e_n = (0, \ldots, 1)$ es la base canónica de $\mathbf{Z}^n$ y $p(e_i) = r_i \cdot a$, entonces

$$a = p(a) = (\sum_i r_i \cdot a_i) \cdot a, \text{ o sea}$$

$$(1 - \sum_i r_i \cdot a_i) \cdot a = 0$$

con lo que (si $a \neq 0$)

$$1 = \sum_{i=1}^{n} r_i \cdot a_i$$

lo cual prueba que los a_i son coprimos, como se quería demostrar.

Ejemplo 5. Sea D un dominio de integridad. Entonces todo ideal principal es un módulo libre. En efecto, si $\mathcal{J} = \langle a \rangle$, entonces la aplicación $g : \mathcal{J} \to D$ definida por $g(r \cdot a) = r$ es un isomorfismo. Como D es libre, $\mathcal{J}$ es libre. Recíprocamente, si $\mathcal{J}$ es un ideal de D que es libre como D-módulo, entonces debe ser principal, pues si b_1, b_2 pertenecen a I, resultan dependientes sobre D, en efecto

$$(b_2) \cdot b_1 + (-b_1) \cdot b_2 = 0$$

con lo cual una base no puede tener más de un elemento. Por lo tanto, se deduce que en un dominio de integridad D todo ideal es un módulo libre si, y sólo si, D es un dominio principal.

2. PROPIEDADES IMPORTANTES

Teorema 4.1.3. Sea A un R-módulo *libre* y sea $B = \{b_\alpha\}_{\alpha \in I}$ una base de A. Sea M un R-módulo y $\varphi' : B \to M$ una "aplicación" de conjuntos. Entonces existe un único morfismo $\varphi : A \to M$ que extiende a φ', es decir

$$\varphi'(b_\alpha) = \varphi(b_\alpha)$$

para todo α.

Demostración. Sea $a = \sum_\alpha r_\alpha \cdot b_\alpha \in A$, $r_\alpha \in R$, $r_\alpha = 0$ para casi todo $\alpha \in I$. Dado que dicha representación de a en términos de la base B es única, cabe asociar al elemento a un único elemento determinado por los coeficientes r_α, a saber

$$a \mapsto \sum_\alpha r_\alpha \cdot \varphi'(b_\alpha)$$

queda así definido un morfismo $\varphi : A \to M$ que, evidentemente, extiende a φ'. Si $\varphi'' : A \to M$ es otro morfismo que extiende a φ', se tiene

$$\varphi(a) = \varphi(\sum_\alpha r_\alpha \cdot b_\alpha) =$$

$$= \sum_\alpha r_\alpha \cdot \varphi'(b_\alpha) = \sum_\alpha r_\alpha \cdot \varphi''(b_\alpha) = \varphi''(\sum_\alpha r_\alpha \cdot b_\alpha) = \varphi''(a)$$

con lo que $\varphi(a) = \varphi''(a)$ y así $\varphi = \varphi''$, por lo tanto la unicidad solicitada.

Corolario 4.1.4. Sea A un módulo libre y sea B una base de A.

a) Si $\varphi : A \to M$ es un morfismo de módulos y

$$\varphi(b) = 0 \text{ si } b \in B$$

entonces

$$\varphi = 0.$$

b) Sean φ y ρ morfismos de A en un módulo M. Entonces

$$\varphi = \rho \text{ si, y sólo si, } \varphi(b) = \rho(b) \text{ si } b \in B.$$

c) Sea $\varphi : A \to A$ un endomorfismo. $\varphi = id_A$ si, y sólo si, $\varphi(b) = b$ para todo $b \in B$.

Nota. De acuerdo con el teorema 4.1.3 se dice que un morfismo definido sobre un módulo libre está unívocamente determinado por los valores que toma sobre una base. El lector familiarizado con la teoría de espacios vectoriales recordará que ésta es una propiedad típica de las transformaciones lineales.

Ejemplo. A manera de aplicación probaremos *que no existe ningún epimorfismo de* **Z** *sobre* $Z \oplus Z$.

Razonando por el absurdo, supóngase que exista un epimorfismo $\Psi : \mathbf{Z} \to \mathbf{Z} \oplus \mathbf{Z}$, Sea $\{b_1, b_2\}$ una base de $\mathbf{Z} \oplus \mathbf{Z}$. Siendo Ψ un epimorfismo, existen m_1, m_2 en $\mathbf{Z}$, tales que

$$\Psi(m_1) = b_1, \quad \Psi(m_2) = b_2 .$$

Por el teorema 4.1.3 existe un morfismo $\varphi : \mathbf{Z} \oplus \mathbf{Z} \to \mathbf{Z}$, tal que $\varphi(b_1) = m_1$, $\varphi(b_2) = m_2$. Adviértase que Ψ es un monomorfismo dado que

$$\varphi \cdot \Psi = \mathrm{id}_{\mathbf{Z} \oplus \mathbf{Z}}$$

por lo tanto si $x, y \in \mathbf{Z} \oplus \mathbf{Z}$ satisfacen $\Psi(x) = \Psi(y)$, entonces

$$x = \varphi \cdot \Psi(x) = \varphi \cdot \Psi(y) = y.$$

Por otra parte

$$\begin{aligned} \Psi(m_2 \cdot b_1 - m_1 \cdot b_2) &= m_2 \cdot \Psi(b_1) - m_1 \cdot \Psi(b_2) \\ &= m_2 \cdot m_1 - m_1 \cdot m_2 \\ &= 0 \end{aligned}$$

con lo que

$$0 = m_2 \cdot b_1 - m_1 \cdot b_2 = m_2 \cdot b_1 + (-m_1) \cdot b_2 .$$

Siendo b_1, b_2 base de $\mathbf{Z} \oplus \mathbf{Z}$, debe ser $m_1 = m_2 = 0$, un absurdo. Por lo tanto, no existe ningún epimorfismo de $\mathbf{Z}$ sobre $\mathbf{Z} \oplus \mathbf{Z}$.

58 A manera de ejercicio, se propone al lector dé otra demostración de la no existencia de epimorfismos $\mathbf{Z} \to \mathbf{Z} \oplus \mathbf{Z}$, utilizando, por ejemplo, el hecho que $\mathbf{Z}$ es un módulo cíclico.

Corolario 4.1.5. Sean A y L, R-módulos, $\varphi : A \to L$ un epimorfismo. Entonces, si L es libre, existe un monomorfismo $\epsilon : L \to A$, tal que $\varphi \cdot \epsilon = \mathrm{id}_L$. Por lo tanto, L es isomorfo a un sumando directo de A. Exactamente, $A = \mathrm{Nu}(\varphi) \oplus \epsilon(L)$.

Demostración. Sean $B = \{b_\alpha\}_\alpha$ una base de L. Sea para cada α, $a_\alpha \in A$, tal que $\varphi(a_\alpha) = b_\alpha$ (*)

$$\epsilon' : B \to A$$

la aplicación definida por

$$\epsilon'(b_\alpha) = a_\alpha.$$

Entonces, por 4.1.4, se puede extender ϵ' a un morfismo

$$\epsilon : L \to A$$

que tiene las propiedades pedidas. La segunda parte del corolario es consecuencia de 3.2.2.

Nota. Se suele decir, en las condiciones del corolario 4.1.5, que el morfismo φ es *partible*. La razón de esta denominación es que en esas condiciones $A = \mathrm{Nu}(\varphi) \oplus \epsilon(L)$, y por lo tanto, φ se expresa unívocamente como la suma del morfismo nulo sobre $\mathrm{Nu}(\varphi)$ con el morfismo ϵ^{-1} sobre $\epsilon(L)$.

(*) Esta simple afirmación utiliza el llamado axioma de elección.

Nota. Sea $\Pi\mathbf{Z}$ (respectivamente, $\oplus\mathbf{Z}$) el producto directo (respectivamente, la suma directa) de una familia infinita *numerable* de copias de $\mathbf{Z}$. Valen las siguientes afirmaciones

1) Sea $f \in (\Pi\mathbf{Z})^*$. Considerando a $\oplus\mathbf{Z}$ como subgrupo de $\Pi\mathbf{Z}$, $f\,|\oplus\mathbf{Z} = 0$ si, y sólo si, $f = 0$. O equivalentemente

$$\mathrm{Hom}(\Pi\mathbf{Z}/\oplus\mathbf{Z}, \mathbf{Z}) = 0.$$

2) $(\Pi\mathbf{Z})^* \simeq \oplus\mathbf{Z}$, con lo que $(\Pi\mathbf{Z})^*$ es un grupo libre.

(Las demostraciones de 1) y 2) pueden consultarse en (7a), Ths. 47.2 y 47.3).

Utilizando 2) es posible demostrar las afirmaciones siguientes:

a) $\Pi\mathbf{Z}$ no es un grupo abeliano libre. En efecto, si lo fuera podría escribirse como suma directa

$$\Pi\mathbf{Z} \simeq \oplus^I\mathbf{Z}$$

donde el conjunto I de índices *no* es numerable. Tomando dual resulta

$$\oplus\mathbf{Z} \simeq (\Pi\mathbf{Z})^* \simeq (\oplus^I\mathbf{Z})^* \simeq \Pi^1\mathbf{Z}$$

lo cual es un absurdo, pues el grupo de la izquierda es numerable, pero no así el de la derecha. 59

b) $\oplus\mathbf{Z}$ no es sumando directo de $\Pi\mathbf{Z}$. En efecto, supongamos

$$\Pi\mathbf{Z} = \oplus\mathbf{Z} \oplus L$$

entonces, tomando dual resulta

$$\oplus\mathbf{Z} \simeq (\Pi\mathbf{Z})^* \simeq \Pi\mathbf{Z} \oplus L^*$$

lo cual es un absurdo por razones de cardinalidad, como en a).

c) $\Pi\mathbf{Z}$ y $\oplus\mathbf{Z}$ son módulos reflexivos. En efecto

$$(\Pi\mathbf{Z})^{**} \simeq (\oplus\mathbf{Z})^* \simeq \Pi\mathbf{Z}$$
$$((\oplus\mathbf{Z})^{**} \simeq (\Pi\mathbf{Z})^* \simeq \oplus\mathbf{Z}$$

(Bien entendido que se trata de suma y producto directo de una familia *numerable* de copias de $\mathbf{Z}$. Ignoramos si idénticos resultados valen en el caso no numerable.)

5

ESPACIOS VECTORIALES

Este capítulo constituye una revisión de la teoría de espacios vectoriales, y la razón de su inclusión es la de completar la exposición. Un espacio vectorial sobre un cuerpo K no es otra cosa que un K-módulo. En realidad, no es necesario que K sea conmutativo, se puede desarrollar la teoría suponiendo que K es un anillo de división. La teoría estructural de espacios vectoriales es fácil de describir: Todo espacio vectorial es un módulo libre y todas las bases de un espacio vectorial tienen el mismo número de elementos (la dimensión del espacio). Por ejemplo, si un espacio vectorial posee una base finita es isomorfo a un, y sólo a un, K^n.

Nos vamos a limitar aquí a estudiar los espacios vectoriales de tipo finito. Para el caso infinito recomendamos la lectura de (13) volumen II.

Proposición 5.1.1. Sea V un espacio vectorial de tipo finito. Entonces V es un módulo libre.

Demostración. Vamos a demostrar la proposición razonando inductivamente sobre el número de elementos de un sistema de generadores. La afirmación inductiva es la siguiente: Si un espacio vectorial de tipo finito posee un sistema de generadores de n elementos, entonces es libre.

Notemos primeramente que si $V = 0$, V es libre, y si $V = \{v\} \neq 0$, entonces cualquier elemento de V no nulo es una base de V (adviértase que, en este caso, V es isomorfo (como K-módulo) a K). Sea V un espacio vectorial con un sistema de generadores

$$v_1, \ldots, v_n, v_{n+1}. \tag{1}$$

Si existe un índice $i \in [\![1, n+1]\!]$, tal que v_i es combinación lineal de los restantes v_j, entonces $\{v_j\}_{j \neq i}$ es un sistema de generadores de V con n elementos. La hipótesis inductiva permite concluir que V es libre. Es posible suponer entonces que ningún v_i es combinación lineal de los restantes v_j. Esto implica que (1) es una base. En efecto, es un sistema de generadores. Bastará demostrar que (1) es un conjunto linealmente independiente. Sea pues

$$k_1 \cdot v_1 + \ldots + k_n \cdot v_n + k_{n+1} \cdot v_{n+1} = 0.$$

Si algún coeficiente k_i es distinto de cero, entonces por ser K un anillo de división, k_i es inversible en K y podremos escribir

$$v_i = - \sum_{j \neq i} (k_i^{-1} \cdot k_j) \cdot v_j$$

que contradice nuestra suposición que ningún v_i es combinación lineal de los restantes. La proposición queda probada.

Teorema 5. 1. 2. *(de la dimensión).* Sea $0 \neq V$ un espacio vectorial de dimensión finita. Entonces dos bases cualesquiera de V poseen el mismo número de elementos.

Sea $e_1, \ldots, e_n$ una base de V y sea $f_1, \ldots, f_m$ otra base de V, tal que $n < m$. El conjunto $f_1, \ldots, f_{m-1}$ genera un subespacio $\langle f_1, \ldots, f_{m-1} \rangle \neq V$. Algún $e_i \notin \langle f_1, \ldots, f_{m-1} \rangle$, pues si todo e_i pertenece a dicho subespacio, como $e_1, \ldots, e_n$ es base, resultaría que $V \subset \langle f_1, \ldots, f_{m-1} \rangle \subset V$ y así $V = \langle f_1, \ldots, f_{m-1} \rangle$, lo cual hemos excluido. Sea, para fijar las ideas, $e_1 \notin \langle f_1, \ldots, f_{m-1} \rangle$. Afirmamos que

(1) $$e_1, f_1, \ldots, f_{m-1}$$

es una base de V. Podemos escribir (por ser $f_1, \ldots, f_m$ una base de V)

$$e_1 = \sum_{j=1}^{m} k_j \cdot f_j$$

con el coeficiente $k_m \neq 0$, pues de ser cero e_1 pertenecería a $\langle f_1, \ldots, f_{m-1} \rangle$. Podemos entonces despejar f_m en términos de (1) y se sigue inmediatamente que (1) es un sistema de generadores de V. Por otra parte

$$k \cdot e_1 + \sum_{i=1}^{m-1} k_i \cdot f_i = 0$$

62 implica $k = 0$, pues de otro modo e_1 pertenecería $\langle f_1, \ldots, f_{m-1} \rangle$. Como los f_i son linealmente independiente se tiene $k_i = 0$. Por lo tanto, se ha probado que (1) es un conjunto linealmente independientey, finalmente, una base de V.

Repitiendo el razonamiento con las bases

$$e_1, \ldots, e_n \quad \text{y} \quad e_1, f_1, \ldots, f_{m-1}$$

se tiene que, para algún e_i, $i \neq 1$

$$e_i, e_1, f_1, \ldots, f_{m-2}$$

es base de V. Y así sucesivamente vamos formando bases de V, donde cada f_j se reemplaza por un e_h. Puesto que $n < m$, por hipótesis se agotarán primero los e_j y llegaremos a construir una base

$$e_1, \ldots, e_n, f_1, \ldots, f_{m-n}, \quad \text{con } 0 < m - n,$$

lo cual es un absurdo dado que $e_1, \ldots, e_n$ es ya una base de V y el agregado de cualquier elemento de V destruye la independencia lineal. Se sigue que $n < m$ es imposible. Por simetría también es imposible que $m < n$. Por lo tanto, $n = m$. El teorema queda probado.

Definición 5. 1. 3. El invariante definido por 5. 1. 2 se denomina la *dimensión de* V, y se denota por $\dim_K V$. Si $V = 0$ fijamos en 0 su dimensión.

Corolario 5. 1. 4. $\dim_K K^n = n$.

Demostración. En efecto, la base canónica posee n elementos.

Corolario 5.1.5. $K^n \simeq K^m$ si, y sólo si, $n = m$.

Demostración. "Si" es trivial. Sea θ: $K^n \to K^m$ un isomorfismo. Entonces, si B es una base de K^n, $\theta(B)$ es base de K^m. Por lo tanto, B posee el mismo número de elementos de $\theta(B)$, es decir m. Por lo tanto, K^n posee dimensión m. Pero, por 5.1.4, $n = m$.

Lema 5.1.6. Sea V un espacio vectorial de dimensión finita. Entonces todo subespacio de V es sumando directo de V.

Demostración. Sea V' subespacio de V. Siendo V de tipo finito, el espacio vectorial cociente V/V' es de tipo finito, por lo tanto libre según 5.1.1. Esto implica, por el corolario 4.1.5, que el morfismo canónico $V \to V/V'$ es partible, por lo tanto $V = V' \oplus V''$. El lema queda probado.

Corolario 5.1.7. Sea V un espacio vectorial de dimensión finita. Entonces todo subespacio de V es de dimensión finita.

Demostración 1. Sea V' subespacio de V. V' es sumando directo y, por lo tanto, existe un proyector de V sobre V'. Como V es de tipo finito, así lo es V'.

Demostración 2. K es un anillo de división y por lo tanto posee dos únicos ideales a la izquierda, y por lo tanto K es noetheriano a la izquierda. Siendo V de tipo finito, es también un módulo noetheriano, con lo que todo submódulo es de tipo finito.

Corolario 5.1.8. Sea V un espacio vectorial de dimensión finita y sea $V = V' \oplus V''$. Entonces

$$\dim_K(V) = \dim_K(V') + \dim_K(V'') \tag{1}$$

Demostración. Notemos que por 5.1.7, $\dim_K(V')$ y $\dim_K(V'')$ están bien definidos. Sea B' base de V' y B'' base de V''. Entonces $B' \cup B''$ es base de V y como $B' \cap B'' = \emptyset$, la igualdad (1) es inmediata.

Corolario 5.1.9. Sea V un espacio vectorial de dimensión finita. Sea $v_1, \ldots, v_h$ un conjunto linealmente independiente. Existe entonces una base B de V, tal que $v_i \in B$, si $i = 1, \ldots, h$.

Demostración. $v_1, \ldots, v_h$ es base del subespacio $V' = \langle v_1, \ldots, v_h \rangle$. Sea $V = V' \oplus V''$. Si B'' es una base de V'', entonces

$$B = \{v_1, \ldots, v_h\} \cup B''$$

es una base de V con las propiedades pedidas.

Corolario 5.1.10. $V = 0$ si, y sólo si, $\dim_K V = 0$.

Demostración. Si $V = 0$ ya hemos fijado su dimensión en 0. Si $\dim_K V = 0$, entonces $V = 0$, pues de ser $V \neq 0$ cualquier $0 \neq v \in V$ puede, según 5.1.9, extenderse a una base de V, con lo que $\dim_K(V) \geq 1$.

Corolario 5.1.11. Sea V un espacio vectorial de dimensión finita y sea V' un subespacio de V. Entonces

i) $$\dim_K(V') \leq \dim_K(V)$$

ii) Vale la igualdad en i) si, y sólo si, $V = V'$.

Demostración. Sea, por 5.1.6, $V = V' \oplus V''$. Por 5.1.8 resulta

$$\dim_K(V) = \dim_K(V') + \dim_K(V''), \text{ y}$$

tratándose de números enteros no negativos $\dim_K(V') \leq \dim_K(V)$, lo cual prueba i). $\dim_K(V') = \dim_K(V)$ si, y sólo si, $\dim_K(V'') = 0$. Pero, por 5.1.10, $\dim_K(V'') = 0$ equivale a $V'' = 0$. ii) queda probado.

Corolario 5.1.12. Sea V un espacio vectorial de dimensión finita n. Entonces, si $v_1, \ldots, v_h$ es un conjunto de elementos de V linealmente independiente, es $h \leq n$. Por lo tanto, m elementos de V con $n < m$ son siempre linealmente dependientes.

Demostración. $v_1, \ldots, v_h$ genera un subespacio de dimensión h, por lo tanto $h \leq n$.

Corolario 5.1.13. Todo sistema lineal

$$\begin{cases} a_{11} \cdot X_1 + \ldots + a_{1n} \cdot X_n = 0 \\ \\ a_{m1} \cdot X_1 + \ldots + a_{mn} \cdot X_n = 0 \end{cases}$$

donde los coeficientes $a_{ij} \in K$, en las indeterminadas

$$X_1, \ldots, X_n$$

admite una solución $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ $x_i \in K$, si $m < n$.

Demostración. Sea K^n el conjunto de elementos (vectores columnas)

$$v_1 = (a_{11}, \ldots, a_{m1})$$

$$v_n = (a_{1n}, \ldots, a_{mn}).$$

Como $m < n$, dicho conjunto es linealmente dependiente en R^n, por lo que existen $x_1, \ldots, x_n \in K$ *no todos ceros*, tales que $0 = \sum_{i=1}^{n} x_i \cdot v_i$. Escribiendo esta última igualdad en términos de las coordenadas a_{ij} de los v_j, se obtiene que $(x_1, \ldots, x_n)$ es solución del sistema.

6

MÓDULOS SOBRE UN DOMINIO DE INTEGRIDAD. DOMINIOS PRINCIPALES

1. DOMINIOS DE INTEGRIDAD

Recordemos que un anillo D es de integridad si es conmutativo, con identidad $1 \neq 0$ y donde

$$x, y \in D,\ x \cdot y = 0 \Leftrightarrow x = 0 \text{ ó } y = 0.$$

Esta propiedad equivale a la ley cancelativa:

$$0 \neq a,\ a \cdot x = a \cdot y \Rightarrow x = y.$$

Una de las propiedades importantes de los dominios de integridad es la de inmersión en un cuerpo, llamado cuerpo de cocientes (véase Estructuras Algebraicas, Parte I, pág. 112). Dicho en forma precisa, si D es un dominio de integridad, existe un cuerpo Q, tal que D se identifica a un subanillo de Q y todo elemento de Q es expresable en forma de fracción $\frac{p}{q}$, con

$$\frac{p}{q} = p \cdot q^{-1}$$

con $p, q \in D$ y $q \neq 0$. Además, el par $D \subset Q$ resuelve el siguiente problema de tipo universal: Para todo morfismo $f : D \to R$ de anillos con identidad y $f(1) = 1$ y tal que

$$\forall\ 0 \neq d \in D,\ f(d) \text{ es inversible en R}$$

existe un único morfismo $\theta : Q \to R$ tal que el diagrama

es conmutativo.

Sean $a, b \in D$, $a \neq 0$. Diremos que a *divide* a b (en D) si existe $x \in D$, tal que $b = x \cdot a$. En esta situación se dice también que b es múltiplo de a, o que a es divisor de b, etc. y se indica con la notación a/b. Por ejemplo,

$$\forall a \in D,\ 1/a \text{ y } a/a \text{ si } a \neq 0.$$

La negación de a/b se denota por $a \not| b$.

En general, si U(D) denota el grupo de unidades de D, es decir, el grupo de elementos de D inversibles (en D), se tiene

$$\forall u \in U(D),\ \forall a \in D : u/a \text{ y } u \cdot a/a, \text{ si } a \neq 0.$$

Así U(D) define una relación de equivalencia en $D^* = D - \{0\}$

(X) $$a \; X \; b \Leftrightarrow a = u \cdot b \text{ con } u \in U(D)$$

(la verificación correspondiente queda a cargo del lector).

Las clases de equivalencia son

$$\underline{a} = U(D) \cdot a, \; a \in D.$$

Notemos que (X) es equivalente a la relación (en D^*)

$$a \sim b \Leftrightarrow a/b \text{ y } b/a.$$

Los elementos equivalentes se denominarán *asociados*. Así, en Z, los asociados de a son a y $-a$. En el anillo de enteros de Gauss (véase Estructuras Algebraicas, Parte I, pág. 48) los asociados de $a \in \mathbf{Z}[t]$ son a, $-a$, $t \cdot a$ y $-t \cdot a$.

La relación de divisibilidad a/b induce en el conjunto cociente $D^*/(X)$ una relación de orden parcial. En efecto, denotemos los elementos de $D^*/(X)$ con la notación

$$\underline{a} = U(D) \cdot a \text{ y } \underline{1} = U(D)$$

podemos entonces definir la relación en $D^*/(X)$

$$\underline{a}/\underline{b} \text{ si, y sólo si, } a/b.$$

La misma verifica los axiomas de orden parcial

Reflexividad	$\underline{a}/\underline{a}$
Antisimetría	$\underline{a}/\underline{b}$ y $\underline{b}/\underline{a} \Rightarrow \underline{a} = \underline{b}$
Transitividad	$\underline{a}/\underline{b}$ y $\underline{b}/\underline{c} \Rightarrow \underline{a}/\underline{c}$

Notemos que cualquiera que sea $a \in D^*$

$$\underline{1}/\underline{a} \text{ y } \underline{a}/\underline{a}.$$

Definición 6.1.1. Se dice que $a \in D^*$ es *extremal* (o también *irreducible*) si $\underline{a} \neq \underline{1}$, y además

$$\forall \, x \in D^*, \; \underline{x}/\underline{a} \Rightarrow \underline{x} = \underline{1} \text{ ó } \underline{x} = \underline{a}.$$

Con P se denota la totalidad de elementos extremales de D.

Ejemplo 1. En el anillo D de enteros racionales los elementos extremales son los números primos.

Ejemplo 2. En el anillo de polinomios $K[X]$, K un cuerpo, los elementos extremales son los polinomios irreducibles.

Ejemplo 3. Sea $D = \mathbf{Z}[t]$ el anillo de enteros de Gauss. Calculemos algunos elementos extremales de D. Recordemos (Véase Estructuras Algebraicas, Parte I, pág. 48) la existencia de una aplicación $N : \mathbf{Z}[t] \to$

$\to \mathbf{Z} \geq 0$ denominada la *norma*, con la propiedad multiplicativa $N(z \cdot z') = N(z) \cdot N(z')$. Sea $z \in D$. Si $N(z)$ es primo, entonces z es extremal. En efecto, $z = z' \cdot z''$ implica $N(z) = N(z') \cdot N(z'')$, por lo tanto $N(z') = 1$ ó $N(z'') = 1$, o sea z' es inversible o z'' es inversible. z es, pues, extremal. No es cierto, en general, que si z es extremal, entonces $N(z)$ sea primo en $\mathbf{Z}$. En efecto, $3 = 3 + 0 \cdot i \in D$ posee $N(3) = 9$. Probemos que 3 es extremal en $Z[i]$. Sea $3 = (a + b \cdot i) \cdot (c + d \cdot i)$. Tomando norma resulta:

$$3^2 = (a^2 + b^2) \cdot (c^2 + d^2)$$

lo cual implica

$$3 = a^2 + b^2 = c^2 + d^2.$$

Esto es un absurdo, pues si a es par (impar) y b es impar (par), entonces $a^2 + b^2 \equiv 1 \bmod(4)$ en tanto que $3 \equiv 3 \bmod(4)$. No hay otra posibilidad.

Notemos, finalmente, que los primos racionales no son necesariamente elementos extremales en $\mathbf{Z}[i]$. Por ejemplo, $5 = 5 + 0 \cdot i = (2 + i) \cdot (2 - i)$. Un resultado clásico (véase por ejemplo, Hardy-Wright, Teorema 366) establece que un primo impar p es suma de dos cuadrados en $\mathbf{Z}$ si, y sólo si, p es de la forma $4m + 1$. Basándose en este resultado es fácil ver cuáles son los primos racionales que son elementos extremales en $\mathbf{Z}[i]$. Afirmamos que $p \neq 2$, primo racional es extremal en $\mathbf{Z}[i]$ si, y sólo si, p es de la forma $4m + 3$. En efecto, sea $p = 4m + 3$. Si p no es extremal en $\mathbf{Z}[i]$, se tiene $p = (a + b \cdot i) \cdot (c + d \cdot i)$, y tomando norma resulta $p^2 = (a^2 + b^2) \cdot (c^2 + d^2)$ con lo cual $p = a^2 + b^2$, pero, por el resultado mencionado antes, p es de la forma $4k + 1$ una contradicción. Recíprocamente, sea p primo extremal en $\mathbf{Z}[i]$, siendo p impar, $p = 4k + 1$ ó $p = 4m + 3$. Si $p = 4m + 1$, entonces por el resultado a que se ha hecho referencia, $p = c^2 + d^2$, por lo tanto

$$p = (c + d \cdot i) \cdot (c - d \cdot i)$$

con $N(c + d \cdot i) = p \neq 1$. Esto contradice el carácter extremal de p. Por lo tanto, $p = 4m + 3$. Nuestra afirmación queda probada.

Notemos finalmente que 2 no es extremal en $\mathbf{Z}[i]$; en efecto, podemos escribir $2 = (1 + i) \cdot (1 - i)$.

Ejemplo 4. Sea p un primo racional. Sea $\mathbf{Z}_{(p)}$ la localización de $\mathbf{Z}$ en el ideal primo $\langle p \rangle$. Calculemos los elementos extremales de $\mathbf{Z}_{(p)}$. Sea $a/b \in \mathbf{Z}_{(p)}$, $a, b \in \mathbf{Z}$, $p \nmid b$. Es claro que (siendo a y a/b asociados, por ser b unidad) a es extremal si, y sólo si, a/b es extremal. Se trata pues de hallar los enteros racionales que sean extremales en $\mathbf{Z}_{(p)}$. Pero, si un entero racional es extremal en $\mathbf{Z}_{(p)}$, lo es *a fortiori* en $\mathbf{Z} \subset \mathbf{Z}_{(p)}$, por lo tanto es primo racional. En resumen, los elementos extremales de $\mathbf{Z}_{(p)}$ son asociados a primos racionales. Pero si q es primo racional y es distinto de p, es inversible en $\mathbf{Z}_{(p)}$. Por lo tanto, entre los primos debemos descartar los que son distintos de p. En definitiva, se puede afirmar que un elemento $a \in \mathbf{Z}_{(p)}$ es extremal si, y sólo si, $a = u \cdot p$, $u \in U(\mathbf{Z}_{(p)})$, es decir es asociado a p.

Esto significa también que el conjunto cociente $\mathbf{Z}^*_{(p)}/(X)$ contiene dos elementos: 1 y p.

Los siguientes tipos de dominios de integridad son de gran importancia en el álgebra conmutativa y en la teoría algebraica de números.

Definición 6.1.2. Un dominio D se dice *principal*, si todo ideal α de D es principal, es decir $\alpha = \langle a \rangle$, para algún $a \in D$.

Definición 6.1.3. Un dominio D se dice *euclidiano*, si está dada una aplicación $\delta : D \to \mathbf{Z} \geq 0$, tal que

(E1) $\delta(a) = 0$ si, y sólo si, $a = 0$

(E2) Para todo par a, b, $a \neq 0$, existen $q, r \in D$, tales que $b = q \cdot a + r$ con $\delta(r) < \delta(a)$.

En esas condiciones se dice también que D posee un *algoritmo euclidiano de división*.

Definición 6.1.4. Un dominio D se dirá *factorial* (o también un *dominio de factorización única*) si

(F1) $\forall a \in D$, $a \neq 0$ y $a \notin U(D)$

existen elementos extremales en un número finito $\pi_2, \ldots, \pi_h$, tales que $a = \prod_{i=1}^{h} \pi_i$

(F2) Si $\pi_1, \ldots, \pi_h$ y $\nu_1, \ldots, \nu_h$

son sucesiones finitas de elementos extremales, tales que

$$\prod_{i=1}^{h} \pi_i = \prod_{j=1}^{l} \nu_j$$

entonces $h = l$, y además, cada π_i es asociado a un ν_j y viceversa.

Las jerarquías correspondientes a estas definiciones son

$$DE \Rightarrow DP \Rightarrow DF$$

(donde DE = dominio euclidiano, DP = dominio principal y DF = dominio de factorización única).

La demostración de la implicación DE $\Rightarrow$ DP es similar al caso del anillo de enteros racionales, y puede ser un buen ejercicio para el lector elaborar una demostración. En lo que sigue se probará la implicación DP $\Rightarrow$ DF. La misma estará precedida de resultados parciales que muestran propiedades típicas de los dominios principales. Estas propiedades son análogas a los resultados válidos en el anillo $\mathbf{Z}$. Es, pues, importante que el lector piense en términos de este ejemplo.

Proposición 6.1.5. Sea D un dominio principal. Entonces $a \in D$ es extremal si, y sólo si, el ideal $\langle a \rangle$ es primo (véase Estructuras Algebraicas, Parte I, pág. 109).

Demostración. Sea $\langle a \rangle$ un ideal primo. Entonces, si $a = x \cdot y$ en D, se tiene $x \cdot y \in \langle a \rangle$, por lo tanto $x \in \langle a \rangle$ ó $y \in \langle a \rangle$, es decir $x = r \cdot a$ ó $y = s \cdot a$. Analicemos el caso $x = r \cdot a$. Entonces $a = x \cdot y = r \cdot a \cdot y$ y así $a \cdot (1 - r \cdot y) = 0$. Esto implica $1 - r \cdot y = 0$, o sea $y \in U(D)$ y $r \in U(D)$. Por lo tanto, x e y son divisores impropios de a, con lo cual a es extremal.

Sea a extremal en D. Vamos a probar que $D/\langle a \rangle$ es un dominio de integridad (véase Estructuras Algebraicas, Parte I, pág. 109). Sean $x, y \in D$, tales que $\underline{x} \cdot \underline{y} = 0$ en $D/\langle a \rangle$, $\underline{y} \neq 0$. El anulador $An(\underline{y})$ de $\underline{y}$ en $D/\langle a \rangle$ es un ideal $\neq D/\langle a \rangle$, pues $\underline{1} \cdot \underline{y} = \underline{y} \neq 0$. Sea J un ideal en D, tal que $\langle a \rangle \subset J$, $\theta(J) = An(\underline{y})$, $\theta : D \to D/\langle a \rangle$ el morfismo canónico. $J = \langle j \rangle$, por ser D dominio principal. $\langle a \rangle \subset J$ implica $a = j \cdot r$. Pero, siendo a extremal, caben dos posibilidades: i) j es asociado con a. Esto equivale a $J = \langle a \rangle$, y por lo tanto, $0 = \theta(\langle a \rangle) = \theta(J) = An(\underline{y})$, con lo que $\underline{x} = 0$ (pues $\underline{x} \cdot \underline{y} = 0$). ii) j es una unidad. Esto equivale a $J = D$, por lo tanto $An(\underline{y}) = \theta(J) = D/\langle a \rangle$, lo cual es una contradicción. $D/\langle a \rangle$ es un dominio de integridad y así $\langle a \rangle$ es un ideal primo.

Proposición 6.1.6. Sea D un dominio principal. Las afirmaciones siguientes son equivalentes entre sí: Sea $0 \neq a \in D$

i) a es extremal

ii) $\langle a \rangle$ es un ideal primo

iii) $\langle a \rangle$ es un ideal maximal.

Demostración. La equivalencia i) $\Leftrightarrow$ ii) fue probada en 6.1.5. La implicación iii) $\Rightarrow$ ii) es fácil de ver. En efecto, $\langle a \rangle$ maximal es equivalente a que $D/\langle a \rangle$ sea un cuerpo, por lo tanto un dominio de integridad, y así $\langle a \rangle$ es un ideal primo. La implicación ii) $\Rightarrow$ iii) se prueba utilizando las ideas de la demostración de la parte "sólo si" de 6.1.5, y se deja como ejercicio para el lector. Una consecuencia de 6.1.6 es la siguiente. Un dominio principal D es un cuerpo si, y sólo si, $P = \emptyset$. En efecto, si D es un cuerpo, entonces $U(D) = D^* = D - \{0\}$, de manera que no hay elementos extremales. Recíprocamente, si $P = \emptyset$, entonces 0 es un ideal maximal, por lo tanto D es un cuerpo.

Proposición 6.1.7. (Existencia de un máximo común divisor). Sea D un dominio principal. Para todo par a, b de elementos (no simultáneamente 0) de D existe $d \in D$, con las propiedades siguientes

M.1) d/a y d/b

M.2) Si k/a y k/b, entonces k/d

M.3) Existen $r, s \in D$, tales que $d = r \cdot a + s \cdot b$.

Demostración. Sea $J = \langle a \rangle + \langle b \rangle$ el ideal suma de $\langle a \rangle$ y $\langle b \rangle$. Por ser D principal existe $d \in D$, tal que $J = \langle d \rangle$. Como $\langle a \rangle \subset J$, $\langle b \rangle \subset J$,

se tiene que d/a y d/b. Además, k/a y k/b implica que $\langle a\rangle \subset \langle k\rangle$ y $\langle b\rangle \subset \langle k\rangle$, con lo que $J = \langle a\rangle + \langle b\rangle \subset \langle k\rangle$ y así k/d. Finalmente, por pertenecer d a $\langle a\rangle + \langle b\rangle$, se puede escribir $d = r\cdot a + s\cdot b$, con $r, s \in D$. La proposición queda probada.

Definición 6.1.8. Cualquier elemento d con las mismas propiedades de 6.1.7 se denomina (un) máximo común divisor de a y b. Lo denotamos genéricamente con (a, b). Si $(a, b) = 1$, se dice que a y b son *coprimos* (o primos entre sí).

Es claro que a y b son coprimos si, y sólo si, existen $r, s \in D$, tales que $1 = r\,.\,a + s\,.\,b$.

Si $a, b \in D$ se puede definir el *mínimo común múltiplo* como cualquier k tal que $\langle k\rangle = \langle a\rangle \cap \langle b\rangle$. Se dejan los detalles a cargo del lector. Lo denotamos genéricamente con corchetes $[a, b]$.

Proposición 6.1.9. Sea π extremal. Entonces $\pi/a\,.\,b$, $a, b \in D$ si, y sólo si, π/a ó π/b.

Demostración. Parte "si" es trivial. Sea $\pi/a\,.\,b$. Si $\pi\not/a$, entonces π y a son coprimos. Existen así $r, s \in D$, tales que $1 = r\,.\,a + s\,.\,\pi$. También se tiene $b = r\,.\,a\,.\,b + s\,.\,\pi\,.\,b$. Como π divide al miembro derecho, divide también al izquierdo, es decir π/b. La proposición queda probada.

Teorema 6.1.10. Sea D un dominio principal. Entonces D es un dominio factorial.

Demostración. Sea $a \in D$, $a \neq 0$ y $a \notin U(D)$. La familia F de ideales propios de D que contienen al ideal $\langle a\rangle$ es no vacía: $\langle a\rangle \in F$. (Nótese que dado que $a \notin U(D)$, $\langle a\rangle \neq D$). Por ser D noetheriano, existe un ideal maximal propio J, tal que $\langle a\rangle \subset J$. Pero $J = \langle \pi\rangle$, y así π/a con π extremal. Hemos probado que a es divisible por un elemento extremal. Sea H la totalidad de *productos finitos de elementos extremales, que dividen a* a. Acabamos de probar que $H \neq \emptyset$. Formemos la familia F_H de todos los ideales del tipo $\langle \frac{a}{k}\rangle$ con $k \in H$. Por la noetherianidad de D existe en F_H un elemento *maximal* $\langle \frac{a}{k}\rangle$, con $k = \prod \pi_i$ producto finito de elementos extremales de D. Si $\langle \frac{a}{k}\rangle = D$ entonces $1 = r\,.\,\frac{a}{k}$ y así $r \in U(D)$, $a = r^{-1}\cdot \prod \pi_i$, con lo que a es asociado a un producto de elementos extremales. Si $\langle \frac{a}{k}\rangle \neq D$ entonces existe un ideal maximal propio $\langle \pi\rangle$, tal que $\langle \frac{a}{k}\rangle \subset \langle \pi\rangle$ con π extremal. Se tiene $\frac{a}{k} = t\cdot \pi$. Ahora, $k\cdot \pi \in H$ y así

$$\langle t\rangle = \langle \frac{a}{k\cdot \pi}\rangle \in F_H\,.$$

Además

$$\langle \frac{a}{k}\rangle \subset \langle \frac{a}{k\cdot \pi}\rangle \qquad (1)$$

y la inclusión es propia (pues de no ser así $\frac{a}{k}$ y $\frac{a}{k\cdot \pi} = t$ serían asociados, lo cual es un absurdo puesto que $\frac{a}{k} = t\cdot \pi$). Pero (1) contradice la

maximalidad de $\langle \frac{a}{h} \rangle$. En definitiva, hemos probado que todo elemento $a \in D$, $a \neq 0$, $a \notin U(D)$ es producto finito de elementos extremales de D.

Probemos ahora la unicidad. Sean $\pi_i \in P$, $i = 1, \ldots, h$; $\nu_j \in P$, $j = 1, \ldots, l$

$$u \cdot \prod_{i=1}^{h} \pi_i = \prod_{j=1}^{l} \nu_j, \quad u \in U(D). \tag{2}$$

Hagamos una inducción en h. Si $h = 1$.

$$u \cdot \pi_1 = \prod_{j=1}^{l} \nu_j .$$

Si l fuera mayor que 1, los ν_i serían divisores propios de π_1, lo cual es un absurdo. Por lo tanto $l = 1$ y así $\pi_1 \sim \nu_1$. Sea $1 < h$ y supongamos la unicidad para el caso de productos de extremales de $h - 1$ factores. π_1 divide al producto $\prod_{j=1}^{l} \nu_j$. Aplicando 6.1.9 un número finito de veces, se obtiene que π_1 divide a algún ν_j, por ejemplo ν_1. Siendo ν_1 extremal, se tiene que π_1 y ν_1 son asociados: $\pi_1 = u' \cdot \nu_1, u' \in U(D)$. Reemplazando en (2) y cancelando se obtiene

$$u'' \cdot \prod_{i=2}^{h} \pi_i = \prod_{j=2}^{l} \nu_j . \qquad u'' = u \cdot u'$$

Podemos utilizar ahora la hipótesis inductiva y concluir que $h = l$ y cada π_i es asociado a algún ν_j, y recíprocamente. En virtud del principio de inducción se tiene la unicidad de la descomposición en producto de elementos extremales en D.

2. UNA FAMILIA IMPORTANTE DE EJEMPLOS

En esta sección se darán ejemplos de los tipos de dominios de integridad considerados en la sección 1 de este capítulo. La finalidad es estudiar algunas nociones de la teoría algebraica de números, que es donde hoy día juega un papel fundamental la teoría de módulos.

Sea $\mathbf{Q}$ el cuerpo de números racionales. Sea $d \in \mathbf{Z}$. Consideraremos en lo que sigue las extensiones de $\mathbf{Q}$ determinadas por las soluciones complejas de la ecuación cuadrática

$$x^2 - d = 0. \tag{q}$$

Observemos primeramente que (q) posee solución en $\mathbf{Q}$ si, y sólo si, posee solución en $\mathbf{Z}$ (en virtud del Teorema de Gauss relativo a las soluciones racionales de ecuaciones algebraicas con coeficientes enteros). Ahora bien, es evidente que (q) posee solución en $\mathbf{Z}$ si, y sólo si, d es cuadrado en $\mathbf{Z}$. Por lo tanto, supondremos que d no es cuadrado en $\mathbf{Z}$. Incluso podemos suponer que d no *posee factores que sean cuadrados en* $\mathbf{Z}$, excepto 1. En efecto, si $d = m^2 \cdot h$, se puede reemplazar (q) por la ecuación equivalente (q') $X^2 - h = 0$ (r es solución de (q') si, y sólo si, $r \cdot m$ es solución de (q)).

La ecuación (q) posee soluciones en $\mathbf{C}$, el cuerpo complejo. Una solución no es otra cosa que una raíz cuadrada de d. Sea, por abuso de notación, $\sqrt{d} \in \mathbf{C}$ una solución de (q). El conjunto

$$\mathbb{Q}(\sqrt{d}) = \{r + s \cdot \sqrt{d} / r, s \in \mathbb{Q}\}$$

tiene las propiedades siguientes:

i) $\mathbb{Q}(\sqrt{d})$ es, respecto de la suma y producto de números complejos, un anillo con identidad

i') $\mathbb{Q}(\sqrt{d})$ es un cuerpo

ii) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d})$

ii') $\mathbb{Q}(\sqrt{d})$ es un $\mathbb{Q}$-espacio vectorial de dimensión 2.

iii) Los únicos automorfismos de $\mathbb{Q}(\sqrt{d})$ (como anillo) son $id_{\mathbb{Q}(\sqrt{d})}$ y la conjugación $a + b \cdot \sqrt{d} \to a - b \cdot \sqrt{d}$.

iv) $\mathbb{Q}(\sqrt{d}) \simeq \mathbb{Q}(\sqrt{d'})$ si, y sólo si, $d = d'$.

En efecto, i) se obtiene mediante una verificación de tipo computacional, que se deja a cargo del lector.

i') Probaremos que todo elemento no nulo de $\mathbb{Q}(\sqrt{d})$ es inversible en $\mathbb{Q}(\sqrt{d})$. Para ello definimos primero la *norma* de la extensión $\mathbb{Q}(\sqrt{d})$, es decir la aplicación

$$N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q} \text{ definida por}$$

$$N(r + s \cdot \sqrt{d}) = (r + s \cdot \sqrt{d})\ (r - s \cdot \sqrt{d}) = r^2 - d \cdot s^2.$$

La misma es multiplicativa, es decir $N(x \cdot y) = N(x) \cdot N(y)$, si $x, y \in \mathbb{Q}(\sqrt{d})$. Además

$$N(r + s \cdot \sqrt{d}) = 0 \Leftrightarrow r = s = 0.$$

En efecto, $r^2 - d \cdot s^2 = 0$, implica $s = r = 0$ ó $0 \neq s$, con lo que $d = \frac{r^2}{s^2}$ un cuadrado en $\mathbb{Q}$ (luego en $\mathbb{Z}$) un absurdo. Por lo tanto, debe ser $r = s = 0$.

Sea ahora $0 \neq z \in \mathbb{Q}(\sqrt{d})$. Entonces, si $z = r + s \cdot \sqrt{d}$, sea $\bar{z} = r - s \cdot \sqrt{d}$ (denominado el conjugado de z). Se tiene

$$z \cdot \bar{z} = N(z), \text{ y así } z \cdot \left(\frac{\bar{z}}{N(z)}\right) = 1$$

lo cual prueba que z es inversible en $\mathbb{Q}(\sqrt{d})$.

ii) los elementos de $\mathbb{Q}$ corresponden a los elementos de $\mathbb{Q}(\sqrt{d})$ de la forma $r + 0 \cdot \sqrt{d}$. La aplicación $r \to r + 0 \cdot \sqrt{d}$ de $\mathbb{Q}$ en $\mathbb{Q}(\sqrt{d})$ es un monomorfismo.

ii') de acuerdo con ii), $\mathbb{Q}(\sqrt{d})$ resulta ser un $\mathbb{Q}$-espacio vectorial de dimensión 2. En efecto, $\{1, \sqrt{d}\}$ es una base de $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$.

iii) Sea $\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ un automorfismo. Probemos que si $r \in \mathbb{Q}$, entonces $\sigma(r) = r$. En efecto, $\sigma(1) = 1$, implica $\sigma(m) = m$, si $m \in \mathbb{Z} \subset \mathbb{Q}$. Además si $m \neq 0$, $\sigma(1) = \sigma\left(\frac{m}{m}\right) = m\sigma\left(\frac{1}{m}\right)$, con lo que $\sigma\left(\frac{1}{m}\right) = \frac{1}{m}$. Se sigue de inmediato que $\sigma\left(\frac{n}{m}\right) = \frac{n}{m}$, como se quería probar. Entonces $\sigma(\sqrt{d}) =$

$= r + s \cdot \sqrt{d}$, con $s \neq 0$ (pues σ es biyectiva y $\sigma(r) = r$). Por lo tanto,

$$d = \sigma(d) = (\sigma(\sqrt{d}))^2 = r^2 + 2r \cdot s\sqrt{d} + d \cdot s^2.$$

La independencia lineal de 1 y $\sqrt{d}$ implica

$$2 \cdot r \cdot s = 0$$

$$r^2 + d \cdot s^2 = d.$$

Como $s \neq 0$, resulta $r = 0$ y $s^2 = 1$, o sea $s = \pm 1$. En definitiva σ es el morfismo identidad si $s = 1$ y la conjugación si $s = -1$.

iv) Sea $\mu : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d'})$ un isomorfismo. Por las mismas razones que en iii) se tiene $\mu(r) = r$, si $r \in \mathbb{Q}$. Por lo tanto,

$$\mu(\sqrt{d}) = r + s \cdot \sqrt{d'} \quad \text{con} \quad s \neq 0.$$

Elevando al cuadrado

$$d = \mu(d) = r^2 + 2 \cdot r \cdot s\sqrt{d'} + s^2 \cdot d'$$

por lo tanto, $r = 0$ y $d = r^2 + s^2 \cdot d'$, como en iii). Entonces

$$d = s^2 \cdot d'$$

y como d no posee factores cuadrados $\neq 1$, debe ser $s^2 = 1$ y así $d = d'$.

Definición 6.2.1. El cuerpo $\mathbb{Q}(\sqrt{d})$ se denominara la *extensión cuadrática de* $\mathbb{Q}$ asociada a la ecuación $X^2 - d = 0$.

Se dice que $\mathbb{Q}(\sqrt{d})$ es *real*, si $0 < d$, e *imaginaria*, si $d < 0$.

Proposición 6.2.2. Sea $z = r + s \cdot \sqrt{d}$. Entonces z es raíz de una ecuación cuadrática

$$X^2 + b \cdot X + c = 0.$$

Demostración. En efecto, la ecuación

$$(X - (r + s \cdot \sqrt{d})) \cdot (X - (r - s \cdot \sqrt{d})) =$$

$$= X^2 - (2 \cdot r) \cdot X + (r^2 - d \cdot s^2) = 0$$

tiene sus coeficientes en $\mathbb{Q}$ y sus raíces son z y $\bar{z}$.

Definición 6.2.3. Si $z = r + s \cdot \sqrt{d}$, se llama *traza de* z a $\mathrm{Tr}(z) = 2r$, y se llama ecuación característica de z a la ecuación

$$X^2 - \mathrm{Tr}(z) \cdot X + \mathrm{N}(z) = 0.$$

Es claro, según 6.2.2, que *z es raíz de su ecuación característica.*

Definición 6.2.4. Se llama *entero algebraico* de $\mathbb{Q}(\sqrt{d})$ a todo elemento cuya ecuación característica posea coeficientes enteros. Con A se denota la totalidad de elementos algebraicos de $\mathbb{Q}(\sqrt{d})$.

Nótese que si $m \in \mathbf{Z}$, entonces $\mathrm{Tr}(m) = 2m$ y $\mathrm{N}(m) = m^2$, de manera que

$$\mathbf{Z} \subset \mathrm{A}.$$

Además, si $z \in \mathrm{Q}(\sqrt{d})$ es tal que existe un polinomio $f(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$ *mónico*, tal que $f(z) = 0$, entonces $z \in \mathrm{A}$. En efecto, sin pérdida de generalidad cabe suponer que $f(\mathrm{X})$ posee grado mínimo entre los polinomios $g(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$ mónicos, tales que $g(z) = 0$. Esto implica que $f(\mathrm{X})$ es irreducible en $\mathbf{Z}[\mathrm{X}]$ (es decir, no es posible escribir $f(\mathrm{X}) = h(\mathrm{X}) \cdot t(\mathrm{X})$, con $h(\mathrm{X}), t(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$, ambos con grado estrictamente menor que el grado de $f(\mathrm{X})$). Nótese que si $z \in \mathbf{Q}$, entonces $z \in \mathbf{Z}$, pues las raíces racionales de un polinomio mónico con coeficientes enteros son números enteros (Teorema de Gauss). En este caso, no hay nada que probar, pues $\mathrm{Z} \subset \mathrm{A}$. Sea pues $z \notin \mathrm{Q}$. El polinomio característico $\mathrm{X}^2 - \mathrm{Tr}(z) \cdot \mathrm{X} + \mathrm{N}(z)$ anula a z y es el polinomio con coeficientes racionales de menor grado que anula a z. Por lo tanto, $f(z) = 0$ implica que $f(\mathrm{X})$ es divisible en $\mathrm{Q}[\mathrm{X}]$ por $\mathrm{X}^2 - \mathrm{Tr}(z) \cdot \mathrm{X} + \mathrm{N}(z)$. Si $f(\mathrm{X})$ tiene grado 2, entonces coincide con el característico, con lo que $\mathrm{Tr}(z)$ y $\mathrm{N}(z)$ pertenecen a Z y z es un entero algebraico. Si $f(\mathrm{X})$ tiene grado mayor que 2, entonces es factorizable propiamente en $\mathbf{Q}[\mathrm{X}]$. Se deja a cargo del lector probar que en estas condiciones $f(\mathrm{X})$ es factorizable propiamente en $\mathbf{Z}[\mathrm{X}]$, lo cual es una contradicción. (Si el lector no logra probar lo propuesto, puede consultar en cualquier texto de álgebra la teoría de polinomios primitivos, sin embargo, creemos que es un ejercicio interesante de resolver por sí mismo). En fin, nuestra afirmación inicial queda probada.

Teorema 6.2.5. A es un anillo (es decir un subanillo de $\mathbf{Q}(\sqrt{d})$).

Demostración. Sean $z = r + s \cdot \sqrt{d}$, $z' = r' + s' \cdot \sqrt{d} \in \mathrm{A}$. Debemos probar que

$$\mathrm{Tr}(z + z'),\ \mathrm{Tr}(z \cdot z'),\ \mathrm{N}(z + z'),\ \mathrm{N}(z \cdot z')$$

son enteros racionales. Notemos que

$$\mathrm{Tr}(z + z') = \mathrm{Tr}(z) + \mathrm{Tr}(z') \in \mathbf{Z} \quad \text{y}$$
$$\mathrm{N}(z \cdot z') = \mathrm{N}(z) \cdot \mathrm{N}(z') \in \mathbf{Z}.$$

Ahora $\mathrm{N}(z + z') = (r + r')^2 - d \cdot (s + s')^2 = \mathrm{N}(z) + \mathrm{N}(z') + 2rr' - 2dss'$

$$\mathrm{Tr}(z \cdot z') = \mathrm{Tr}(rr' + dss' + (rs' + sr')\sqrt{d}) = 2rr' + 2dss'.$$

Por lo tanto, será suficiente probar que

$$\alpha = 2rr' \pm 2dss' \in \mathbf{Z}.$$

Observemos que $2r \in \mathbf{Z}$

i) $r \in \mathbf{Z} \Rightarrow s \in \mathbf{Z}$. En efecto, $r^2 - d \cdot s^2 = m \in \mathbf{Z}$, luego $d \cdot s^2 \in \mathbf{Z}$ y si $s = \frac{u}{v}$, $u, v \in \mathbf{Z}$, u, v coprimos entonces v^2/d, lo cual es posible sólo si $v^2 = 1$.

ii) $r = \frac{t}{2}$, t impar $\Rightarrow s = \frac{u}{2}$, u impar, y además, $d \equiv 1 \bmod(4)$. En efecto, sea $r^2 - d \cdot s^2 = m \in \mathbf{Z}$. Entonces $t^2 - 4ds^2 = 4m$, o también si $t = 2h + 1$

$$4(h^2 + h) + 1 - 4ds^2 = 4m.$$

Obviamente s no puede ser entero, sea $s = \frac{u}{v}$ con $(u, v) = 1$, $1 < v$.

$$4(h^2 + h) + 1 - 4 \cdot d \cdot \frac{u^2}{v^2} = 4m \tag{1}$$

siendo $4 \cdot d \cdot \frac{u^2}{v^2}$ entero, v divide a $4d$, y como d no posee factores cuadrados, $v/4$, por lo tanto $v^2 = 4$, o sea $v = 2$. Notemos que u debe ser impar, pues v es par y $(u, v) = 1$. Se sigue que d debe ser $\equiv 1 \bmod(4)$, pues tomando congruencia módulo 4 en (1) resulta

$$0 + 1 - (d \cdot u^2) \equiv 0 \mod(4)$$

y como u es impar, $d \equiv 1 \bmod(4)$.

Estamos en condiciones de probar que $\alpha = 2rr' + 2dss' \in \mathbf{Z}$.

1) si r y r' son enteros, entonces $\alpha \in \mathbf{Z}$ (por i)).

2) si $r = \frac{u}{2}$, u impar y r' entero, entonces $2rr' \in \mathbf{Z}$ y lo mismo $2dss' \in \in \mathbf{Z}$ (por 1) e ii)), por lo que $\alpha \in \mathbf{Z}$.

3) si $r = \frac{u}{2}$, $r' = \frac{u'}{2}$, u y u' impares, resulta $s = \frac{t}{2}$, $s' = \frac{t'}{2}$ con t y t' impares. Por lo tanto,

$$\alpha = \frac{uu' \pm d \cdot tt'}{2}. \tag{2}$$

Como $d \equiv 1 \bmod(4)$, d es impar. Por lo tanto, el numerador de (2) es *par* y así $\alpha \in \mathbf{Z}$.

Nuestra afirmación queda probada, así como también la proposición.

Teorema 6.2.6. Sea A el anillo de enteros algebraicos de $\mathbf{Q}(\sqrt{d})$. Entonces

1) $$A = \{r + s\sqrt{d} / r, s \in Z\}$$
$$\text{si } d \equiv 2, \text{ ó } d \equiv 3 \bmod(4)$$

2) $$A = \{\tfrac{1}{2}(r + s \cdot \sqrt{d}) / r, s \in Z \text{ y } r \equiv s \bmod(2)\}$$

(o sea r y s son simultáneamente pares o impares) si $d \equiv 1 \bmod(4)$.

Demostración. En ambos casos, 1) y 2), valen las inclusiones $\supset$ por la simple verificación que los elementos en cuestión tienen traza y norma en Z. Veamos la inclusión opuesta.

1) $d \equiv 2$ ó $d \equiv 3 \bmod(4)$. En este caso si $z = r + s \cdot \sqrt{d} \in A$ debe ser r (y s) entero, pues de no serlo, d sería congruente a 1 módulo 4, según el mismo argumento utilizado en ii) de 6.2.5.

2) $d \equiv 1 \bmod(4)$. Sea $z = r + s\sqrt{d}$ entero algebraico en $\mathbf{Q}(\sqrt{d})$. Si r es entero entonces s es entero y no hay nada que probar. Sea $r = \frac{u}{2}$, u impar. Entonces de $r^2 + d \cdot s^2 = m \in \mathbf{Z}$, resulta

$$u^2 + 4 \cdot d \cdot s^2 = 4m.$$

Si s fuera entero, tomando congruencia mod(4) resultaría

$$1 + 0 \equiv 0 \mod(4)$$

un absurdo. Por lo tanto, $s = \frac{u}{2}$, u impar.

El teorema queda probado.

Ejemplo 1. Si $d = -1$, entonces $d \equiv 3 \mod(4)$, por lo tanto el anillo de enteros algebraicos de $\mathbf{Q}(i)$ es el anillo $\mathbf{Z}[i]$ de enteros de Gauss.

Ejemplo 2. Si $d = 2$, entonces $d \equiv 2 \mod(4)$ y el anillo de enteros algebraicos de $\mathbf{Q}(\sqrt{2})$ es el conjunto $m + n \cdot \sqrt{2}$, $m, n \in \mathbf{Z}$.

Ejemplo 3. Si $d = 5$, entonces $d \equiv 1 \mod(4)$, por lo tanto el anillo de enteros algebraicos de $\mathbf{Q}(\sqrt{5})$ es el conjunto $\frac{1}{2}(r + s\sqrt{5})$, con r, s enteros simultáneamente pares o simultáneamente impares.

Veamos a continuación algunas propiedades de los anillos de enteros algebraicos de extensiones cuadráticas de $\mathbf{Q}$.

Proposición 6.2.7. Para todo d, el anillo de enteros de $\mathbf{Q}(\sqrt{d})$ es un anillo noetheriano.

Demostración. Observemos que el anillo A de enteros algebraicos es un $\mathbf{Z}$-módulo libre de rango 2. En efecto

$$1, \sqrt{d} \text{ es una base si } d \equiv 2 \text{ ó } d \equiv 3 \mod(4)$$

$$1, \tfrac{1}{2}(1 + \sqrt{d}) \text{ es una base, si } d \equiv 1 \mod(4)$$

Por lo tanto, A como $\mathbf{Z}$-módulo es noetheriano. Puesto que todo ideal de A es un $\mathbf{Z}$-módulo, A es noetheriano.

Proposición 6.2.8. Todo ideal primo no nulo de A es maximal.

Demostración. Sea $\mathcal{P}$ un ideal primo no nulo de A, entonces $A/\mathcal{P}$ es dominio de integridad. Debemos probar que es además un cuerpo. Sea pues $z \in A$ tal que $\underline{z} \neq 0$ ($\underline{z}$ denota la imagen de z por el morfismo $A \to A/\mathcal{P}$). La intersección $\mathbf{Z} \cap \mathcal{P}$ es un ideal primo de $\mathbf{Z}$.

Veamos que $0 \neq \mathbf{Z} \cap \mathcal{P}$. Si $0 \neq r + s \cdot \sqrt{d} \in \mathcal{P}$, entonces

$$0 \neq r^2 - d \cdot s^2 = (r + s \cdot \sqrt{d})\ (r - s \cdot \sqrt{d}) \in \mathcal{P} \cap \mathbf{Z}.$$

Sea pues $\mathbf{Z} \cap \mathcal{P} = \langle p \rangle$, p primo racional. La inclusión $\mathbf{Z} \to A$ induce un monomorfismo $\mathbf{Z}/\langle p \rangle \to A/\mathcal{P}$ por el cual identificamos $\mathbf{Z}_p$ a un subanillo de $A/\mathcal{P}$

$$\mathbf{Z}_p \subset A/\mathcal{P}.$$

La ecuación característica $z^2 - \mathrm{Tr}(z) \cdot z + \mathrm{N}(z) = 0$ induce en $A/\mathcal{P}$ la ecuación $\underline{z}^2 - \underline{\mathrm{Tr}(z)} \cdot \underline{z} + \underline{\mathrm{N}(z)} = \underline{0}$, o también

$$\underline{z} \cdot (\underline{z} - \underline{\mathrm{Tr}(z)} \cdot \underline{1}) = \underline{-\mathrm{N}(z)}.$$

Recordemos que $\mathrm{Tr}(z)$ y $\mathrm{N}(z)$ son enteros. Si $\mathrm{N}(z)$ no es divisible por p, entonces $-\mathrm{N}(z)$ es inversible en $\mathbf{Z}_p$, y por lo tanto, lo es $\underline{z}$. Si $\mathrm{N}(z)$ es divisible por p, resulta $\underline{z} \cdot (\underline{z} - \underline{\mathrm{Tr}(z)} \cdot \underline{1}) = 0$. Como $A/\mathcal{P}$ es un dominio de integridad, $z \neq 0$ implica

$$\underline{z} = \underline{\mathrm{Tr}(z)} \cdot \underline{1}$$

por lo tanto si $p \nmid \mathrm{Tr}(z)$, $\underline{\mathrm{Tr}(z)}$ es inversible en $\mathbf{Z}_p$ y también $\underline{z}$ es inversible en $A/\mathcal{P}$. Si $p/\mathrm{Tr}(z)$, entonces (como $p/\mathrm{N}(z)$) resulta que

$$p/z^2 \text{ en } A$$

por lo tanto $\underline{z}^2 = 0$ en $A/\mathcal{P}$. Pero esto implica $z = 0$, un absurdo. La proposición queda probada.

Proposición 6.2.9. Sea A el anillo de enteros algebraicos de $\mathbf{Q}(\sqrt{d})$. Sean $z \in \mathbf{Q}(\sqrt{d})$ y $f(X) \in A[X]$ *mónico*, tal que

$$f(z) = 0.$$

Entonces $z \in A$.

Demostración. Notemos primeramente la propiedad siguiente general

$$A \cap \mathbf{Q} = \mathbf{Z}$$

es decir los enteros de $\mathbf{Q}(\sqrt{d})$ que son racionales son exactamente los enteros racionales. Esto es consecuencia del Teorema de Gauss relativo a las raíces racionales de un polinomio con coeficientes enteros, o también puede probarse directamente con facilidad. Lo dejamos a cargo del lector.

Sea entonces $f(X) \in A[X]$ mónico, tal que $f(z) = 0$. Sea σ el automorfismo de conjugación en $\mathbf{Q}(\sqrt{d})$. Entonces si f^σ denota el polinomio cuyos coeficientes son los conjugados de f, o sea, si

$$f = \sum_{i=1}^{n} a_i \cdot X^i, \quad f^\sigma = \sum_{i=1}^{n} \sigma(a_i) \cdot X^i$$

se tiene que z también es raíz del polinomio

$$f \cdot f^\sigma = a_0 \cdot \sigma(a_0) + (a_0 \cdot \sigma(a_1) + \sigma(a_0) \cdot a_1) \cdot X + \ldots$$

cuyos coeficientes son dejados fijos por σ. Pero observemos que en $\mathbf{Q}(\sqrt{d})$

$$\sigma(x) = x \text{ si, y sólo si, } x \in \mathbf{Q}$$

por lo tanto los coeficientes de $f \cdot f^\sigma$ están en $\mathbf{Q}$. Pero también están en A, puesto que si a es entero algebraico, $\sigma(a)$ también lo es. En definitiva, los coeficientes de $f \cdot f^\sigma$ están en $\mathbf{Z} = A \cap \mathbf{Q}$. Como z es raíz de $f \cdot f^\sigma$, se tiene que $z \in A$, como quería probar.

Definición 6.2.10. Sea D un dominio de integridad y Q su cuerpo de cocientes. Un elemento $z \in Q$ se dice *entero* sobre D si z satisface una

ecuación polinomial $P(z) = 0$ con $P(X) \in D[X]$ *mónico*. Se dice que D es *integralmente cerrado* (en Q), si todo elemento de Q entero sobre D pertenece a D.

Definición 6.2.11. Un dominio D de integridad se denomina un *dominio de Dedekind* si se verifican las tres condiciones siguientes: d1) D es noetheriano, d2) todo ideal primo no nulo es maximal, d3) D es integralmente cerrado.

Los anillos de Dedekind constituyen la generalización más importante del anillo de enteros racionales. La fuente más abundante de ejemplos se halla en la teoría algebraica de números. Para un tratamiento sistemático de la teoría de dominios de Dedekind consúltese (24).

Se sigue de 6.2.7-6.2.9 y de las definiciones 6.2.10 y 6.2.11 el teorema siguiente.

Teorema 6.2.12. El anillo de enteros algebraicos de $\mathbf{Q}(\sqrt{d})$ es un dominio de Dedekind.

Se deja a cargo del lector probar que todo dominio principal es un dominio de Dedekind. La recíproca no es cierta. En efecto,

Ejemplo. Sea $\mathbf{Z}[\sqrt{-5}]$ el anillo de enteros algebraicos de $\mathbf{Q}(\sqrt{-5})$. Mostremos que $\mathbf{Z}[\sqrt{-5}]$ no es dominio de factorización única. Por lo tanto, no puede ser un dominio principal. Se tiene

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})\ (1 - \sqrt{-5}).$$

Veamos que 2 no es asociado ni de $1 + \sqrt{-5}$, ni de $1 - \sqrt{-5}$.

$$N(2) = 4,\ N(1 - \sqrt{-5}) = 1 - (\sqrt{-5})^2 = 6 = N(1 + \sqrt{-5})$$

Es interesante investigar las propiedades de ser DE, DF, DP en los anillos de enteros algebraicos de extensiones cuadráticas $\mathbf{Q}(\sqrt{d})$. Nos limitaremos a enunciar algunos resultados, ya que las demostraciones necesitan de recursos de mayor nivel que los de esta monografía. A los efectos, se recomienda la lectura de (11) de Hardy-Wright y (23) de Weiss para profundizar el estudio de cuerpos cuadráticos.

Resultado 6.2.13. $\mathbf{Q}(\sqrt{d})$ es euclidiano en los casos siguientes:

caso real: $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$

caso imaginario: $d = -1, -2, -3, -7, -11$

Otro resultado interesante es la existencia de un cuerpo cuadrático cuyo anillo de enteros es principal, pero no euclidiano. Se trata de $\mathbf{Q}(\sqrt{23})$. Una propiedad, cuya demostración no es muy difícil, es que si el anillo de enteros algebraicos es de factorización única, entonces es principal. O sea, DF y DP son propiedades equivalentes para los anillos de enteros algebraicos.

Ejemplo. Sea $z = r + s \cdot \sqrt{d} \in \mathbf{Q}(\sqrt{d})$. Sea $u = a + b \cdot \sqrt{d}$ entero algebraico $\neq 0$. Entonces

(1) $$N(z-u) = (r-a)^2 - d\cdot(s-b)^2.$$

Sea d cualquiera de los enteros -2, -1, 2, 3. Se afirma que cualquiera que sea $z \in \mathbf{Q}(\sqrt{d})$, existe $u \in A$, tal que $|N(z-u)| < 1$. Puesto que los d dados son $\not\equiv 1 \bmod(4)$, si $u = a + b\cdot\sqrt{d} \in A$, entonces a y b son enteros. Siendo $r, s \in \mathbf{Q}$ existen enteros a y b, tales que $\varepsilon = |r-a| \le \frac{1}{2}$, $\delta = |s - b| \le \frac{1}{2}$. Por lo tanto, de (1) resulta (si $u = a + b\cdot\sqrt{d}$)

$$|\varepsilon^2 - d\cdot\delta^2| = |N(z-u)|$$

si $d = -2, -1$ se tiene $|N(z-u)| = \varepsilon^2 + (-d)\delta^2 \le \frac{1+(-d)}{4} < 1$, si $d = 2, 3$ se tiene $|N(z-u)| = |\delta^2 d - \varepsilon^2| \le \delta^2 d \le \frac{d}{4} < 1$.

Nuestra afirmación queda probada. Con este resultado parcial probamos la siguiente propiedad: Si $d \in \{-2, -1, 2, 3\}$ el anillo de enteros algebraicos de $\mathbf{Q}(\sqrt{d})$ es euclidiano. Sea

$$\mu : A \to \mathbf{Z} \text{ definida por } \mu(z) = |N(z)|$$

Sean $0 \neq u \in A$, $z \in A$. Por lo que se acaba de ver existe $v \in A$, tal que

$$\frac{z}{u} - v = v' \text{ con } \mu(v') = |N(v')| < 1.$$

Por lo tanto

$$z = v\cdot u + (v'\cdot u) \text{ con}$$

$$\mu(v'\cdot u) = |N(v'\cdot u)| = |N(v')\cdot N(u)| < |N(u)| = \mu(u).$$

Puesto que v y $(v'\cdot u)$ pertenecen a A, se tiene así un algoritmo euclidiano de división en A.

3. UN TEOREMA DE DIAGONALIZACIÓN

En esta sección probaremos un resultado sobre diagonalización de matrices, que será útil en el cálculo de los factores invariantes de un módulo de tipo finito sobre un dominio principal. En esta sección, D denota un dominio principal, $\mathbf{M}_n(D)$ el anillo de matrices de n filas por n columnas con coeficientes en D.

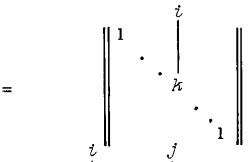
Definición 6.3.1. Se llaman matrices elementales de $\mathbf{M}_n(D)$ a las matrices de los tipos siguientes:

$P^{ij} =$

	i	j
1		
.		
.		
i	0	1
j	1	0
		.
		.
		1

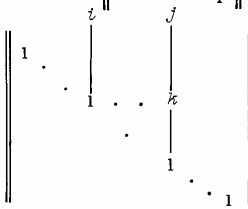
(O sea, la matriz obtenida a partir de la matriz identidad I_n permutando las filas i y j).

$k \in U(D)$, $m^i(k) =$



(O sea, la matriz obtenida multiplicando el coeficiente (i,i) de I_n por k)

$i \neq j$, $t^{ij}(k) =$



(O sea, la matriz $I_n + k \cdot E^{ij}$, donde E^{ij} es la matriz con 0, excepto en la posición (i,j) que posee 1)

Estas matrices elementales poseen las siguientes propiedades:

E1) son inversibles en $\mathbf{M}_n(D)$. En efecto,

$$(p^{ij})^{-1} = p^{ij}$$

$$(m^i(k))^{-1} = m^i(k^{-1})$$

$$(t^{ij}(k))^{-1} = t^{ij}(-k)$$

Nótese asimismo que las inversas de las matrices elementales son también matrices elementales.

E2) Sea $a \in \mathbf{M}_n(D)$. La multiplicación de a por una matriz elemental produce los siguientes efectos

$p^{ij} \cdot a$: permuta las filas i, j de a, y deja invariantes a las restantes

$a \cdot p^{ij}$: permuta las columnas i, j, y deja invariantes a las restantes

$m^i(k) \cdot a$: multiplica la i-sima fila de a por k, y deja invariantes a las restantes

$a \cdot m^i(k)$: multiplica la i-sima columna de a por k, y deja invariantes a las restantes

$t^{ij}(k) \cdot a$: suma *a la i-sima* fila de a, la fila j multiplicada por k, y deja invariantes a las filas restantes

$a \cdot t^{ij}(k)$: suma *a la j-sima columna* de a, la i-sima columna multiplicada por k, y deja invariantes a las restantes.

Definición 6.3.2. Se llaman *operaciones elementales* sobre una matriz a las operaciones efectuadas sobre filas o columnas que resultan de multiplicar la matriz por matrices elementales. Estas operaciones son: permutar dos filas (o columnas), multiplicar una fila (o columna) por una unidad de D, sumar a una fila (o columna) otra distinta multiplicada por un elemento cualquiera de D.

Definición 6.3.3. Se dice que dos matrices a y $b \in \mathbf{M}_n(D)$ son *equivalentes*, si existen matrices *inversibles* u y $v \in \mathbf{M}_n(D)$ tales que

$$a = u \cdot b \cdot v$$

Proposición 6.3.4. La equivalencia definida en 6.3.3 es una relación de equivalencia en $\mathbf{M}_n(D)$.

Demostración. Es inmediata.

El resultado fundamental a probar es que toda matriz de $\mathbf{M}_n(D)$ es equivalente a una matriz diagonal. Si, en particular, D es un cuerpo, resulta que toda matriz es equivalente a una, y sólo una, de las matrices diagonales siguientes

$$\text{diag}(0,0,\ldots,0),\ \text{diag}(1,0,\ldots,0),\ldots,\ \text{diag}(1,1,\ldots,1)$$

O sea, el conjunto cociente de $\mathbf{M}_n(D)$ por la relación de equivalencia 6.3.3 está caracterizado por las $n+1$ matrices diagonales mencionadas. En rigor, el conjunto cociente provee de una definición de *rango* en $\mathbf{M}_n(D)$, D un cuerpo: $a \in \mathbf{M}_n(D)$ posee rango r, $0 \leq r \leq n$ si, y sólo si, a es equivalente a la matriz diagonal $\text{diag}(1,1,\ldots,1,0,\ldots,0)$ (r unos y $n-r$ ceros). Si D es un dominio euclidiano (en particular si D es un cuerpo, definimos pues $\delta: D \to Z_{\geq 0}$ por $\delta(0) = 0$, y $\delta(x) = 1$ si $x \neq 0$) se puede demostrar que toda matriz es equivalente a una diagonal por sucesivas operaciones elementales de filas y columnas, o como suele decirse, toda matriz se puede llevar a la forma diagonal por operaciones elementales de filas y columnas. En efecto, sea $a \in \mathbf{M}_n(D)$, D un dominio euclidiano. Notemos que si $n = 1$, entonces a es una matriz diagonal. Sea pues $1 < n$. Si $a = 0$, a es diagonal y no hay nada que probar. Sea pues $a \neq 0$. Si $a_{ij} \neq 0$ se procede a determinar los restos de la división euclidiana de los elementos de la fila i y columna j por el elemento a_{ij}. Se tiene

$$\text{(fila } i) \qquad a_{is} = a_{ij} \cdot q_s + r_{is} \text{ con } \delta(r_{is}) < \delta(a_{ij}) \qquad s = 1,\ldots,n$$

$$\text{(columna } j) \qquad a_{tj} = a_{ij} \cdot q_t + r_{tj} \text{ con } \delta(r_{tj}) < \delta(a_{ij}) \qquad t = 1,\ldots,n.$$

Adviértase que no hay ambigüedad en la designación de los $r:(t,s) = (t,j)$ si, y sólo si, $t = t$, $s = j$ y, en ese caso, $r_{ij} = r_{ij}$. Vamos a efectuar ahora operaciones de filas y columnas a fin de obtener una matriz equivalente a a cuya fila i y columna j sean, respectivamente,

$$r_{i1} r_{i2} \cdots r_{in}$$

$$r_{1j} r_{2j} \cdots r_{nj}$$

para ello debemos sucesivamente

multiplicar la fila i por $-q_s$ y sumarla a la fila s, $s \neq i$

multiplicar la columna j por $-k_t$ y sumarla a la columna t, $t \neq j$.

De esta manera, se obtiene una matriz equivalente a a tal que los coeficientes r_{is}, $s = 1, \ldots, n$, y r_{tj}, $t = 1, \ldots, n$ satisfagan $\delta(r_{is}) < \delta(a_{ij})$, $\delta(r_{tj}) < \delta(a_{ij})$. Puesto que los valores de δ son enteros no negativos, al cabo de un número finito de pasos se logrará una matriz a' equivalente a a, tal que si $a'_{ij} \neq 0$, entonces

$$\forall s \neq i \; a'_{is} = 0 \quad \text{y} \quad \forall t \neq j \; a'_{tj} = 0$$

(es decir con 0 en la fila i, columna j, excepto en la posición ij).

Permutando ahora filas y columnas convenientemente resulta una matriz diagonal

(d) $$\operatorname{diag}(d_1, d_2, \ldots, d_n)$$

equivalente a a.

Sea $d_1 \neq 0$. La matriz

$$\begin{Vmatrix} d_1 & d_2 & 0 & \ldots & 0 \\ 0 & d_2 & 0 & \ldots & 0 \\ 0 & 0 & d_3 & \ldots & 0 \\ \cdot & \cdot & , & \cdots & , \\ 0 & 0 & , & \ldots & d_n \end{Vmatrix}$$

es equivalente a (d) y luego a a.

Si d_1 no divide a d_2, repitiendo el proceso anterior se obtiene al cabo de un número finito de operaciones de filas y columnas una matriz diagonal

$$\operatorname{diag}(d'_1, d'_2, \ldots, d'_n) \quad \text{con} \quad \delta(d'_1) < \delta(d_1), d'_1 \neq 0.$$

Puesto que δ toma valores enteros no negativos, al cabo de un número finito de pasos se debe obtener una matriz diagonal, equivalente a a,

$$\operatorname{diag}(a_1, a_2, \ldots, a_n)$$

tal que si $a_i \neq 0$ entonces a_i / a_j si $i \leq j$.

Hemos pues probado el siguiente teorema.

Teorema 6.3.5. Sea $a \in \mathbf{M}_n(D)$, D un dominio euclidiano. Existen entonces elementos $d_1, \ldots, d_n$ en D tales que

$$d_i \neq 0, \; i \leq j \Rightarrow d_i / d_j$$

y la matriz a es equivalente (por operaciones elementales de filas y columnas) a la matriz diagonal

$$\operatorname{diag}(d_1, \ldots, d_n).$$

Corolario 6.3.6. Sea $u \in \mathrm{U}(\mathbf{M}_n(D))$. Entonces u es un producto de un número finito de matrices elementales.

Demostración. Sea $\operatorname{diag}(d_1, \ldots, d_n) = E_1 \ldots E_s \cdot u \cdot E_{s+1} \ldots E_t$, donde las matrices E_i son elementales. Puesto que el miembro derecho es inversible (por ser producto de elementos inversibles) así lo es el miembro izquierdo. Pero esto implica inmediatamente que los d_i son unidades en D. Por lo tanto

$$I_n = m^1(d_1^{-1}) \ldots m^n(d_n^{-1}) \cdot \operatorname{diag}(d_1, \ldots, d_n).$$

Podemos escribir entonces

$$I_n = L_1 \ldots L_s \cdot u \cdot L_{s+1} \ldots L_t$$

donde las matrices L_i son elementales. Ahora bien, puesto que si L es elemental L^{-1} así lo es, podemos despejar u y obtener

$$u = L_s^{-1} \ldots L_1^{-1} \cdot I_n \cdot L_t^{-1} \ldots L_{s+1}^{-1}$$

lo cual prueba nuestra afirmación.

Nota. Sea $u \in U(\mathbf{M}_n(D))$, D un dominio euclidiano. Si $E_1, \ldots, E_t$ son matrices elementales, tales que

$$I_n = E_1 \ldots E_s \cdot u \cdot E_{s+1} \ldots E_t$$

resulta

$$E_s^{-1} \ldots E_1^{-1} \cdot I_n = u \cdot E_{s+1} \ldots E_t = I_n \cdot E_s^{-1} \ldots E_1^{-1}$$

pues I_n conmuta con todas las matrices. Por lo tanto

(1) $$I_n = u \cdot E_{s+1} \ldots E_t \cdot E_1 \ldots E_s$$

lo cual expresa que u es equivalente a I_n por operaciones elementales de columnas.

Además se sigue de (1)

$$u^{-1} = I_n \cdot E_{s+1} \ldots E_t \cdot E_1 \ldots E_s$$

lo cual dice que *"las mismas"* operaciones de columnas que efectuadas sobre u "dan" I_n, efectuadas sobre I_n "dan" u^{-1}. Por ejemplo

$$u = \begin{Vmatrix} 1 & 2 \\ 1 & 3 \end{Vmatrix} \to \begin{Vmatrix} 1 & 0 \\ 1 & 2 \end{Vmatrix} \to \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} = I_2$$

$$I_2 = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} \to \begin{Vmatrix} 1 & -2 \\ 0 & 1 \end{Vmatrix} \to \begin{Vmatrix} 3 & -2 \\ -1 & 1 \end{Vmatrix} = u^{-1}$$

Un resultado idéntico es válido para filas. Constituye éste un método muy útil para determinar la inversa de una matriz $a \in U(\mathbf{M}_n(D))$, con D dominio euclidiano.

Ejemplo. Calculemos los divisores d_i de la matriz

$$\begin{Vmatrix} X-1 & -2 & 0 \\ 0 & X-2 & 0 \\ 2 & 2 & X+1 \end{Vmatrix} \in M_3(\mathbf{Q}[X])$$

Siendo $\mathbf{Q}[X]$ un dominio euclidiano, será posible lograr la diagonalización por operaciones elementales de filas y columnas. Puesto que 2 es unidad en $\mathbf{Q}[X]$ se puede multiplicar la fila 3 por $\frac{1}{2}$ y la columna 3 por 2. Resulta la matriz equivalente a la dada

$$\begin{Vmatrix} X-1 & -2 & 0 \\ 0 & X-2 & 0 \\ 1 & 1 & X+1 \end{Vmatrix}$$

A continuación se irán efectuando operaciones elementales, y a cargo del lector se deja justificar los respectivos pasos.

$$\begin{Vmatrix} X-1 & -2 & 0 \\ 0 & X-2 & 0 \\ 1 & 1 & X+1 \end{Vmatrix} \to \begin{Vmatrix} X-1 & -(X+1) & 0 \\ 0 & X-2 & 0 \\ 1 & 0 & X+1 \end{Vmatrix} \to \begin{Vmatrix} X-1 & -(X+1) & -(X^2-1) \\ 0 & X-2 & 0 \\ 1 & 0 & 0 \end{Vmatrix}$$

$$\to \begin{Vmatrix} 0 & X+1 & X^2-1 \\ 0 & X-2 & 0 \\ 1 & 0 & 0 \end{Vmatrix} \to \begin{Vmatrix} 0 & 3 & X^2-1 \\ 0 & X-2 & 0 \\ 1 & 0 & 0 \end{Vmatrix} \to \begin{Vmatrix} 0 & 1 & X^2-1 \\ 0 & X-2 & 0 \\ 1 & 0 & 0 \end{Vmatrix}$$

$$\to \begin{Vmatrix} 0 & 1 & X^2-1 \\ 0 & 0 & -(X-2)(X^2-1) \\ 1 & 0 & 0 \end{Vmatrix} \to \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X-2)(X^2-1) \end{Vmatrix}$$

Por lo tanto

$$d_1 = 1,\ d_2 = 1,\ d_3 = (X-2)(X^2-1).$$

Analizaremos a continuación el caso de un dominio principal D. El resultado sobre diagonalización existe, pero las operaciones elementales no son suficientes. En el caso de un dominio euclidiano, multiplicar una matriz a por una matriz inversible equivale a multiplicar a por matrices elementales, dado que toda matriz inversible es producto de matrices elementales, pero ignoramos si el resultado es válido para matrices sobre un dominio principal general. Demostraremos pues el siguiente teorema.

Teorema 6.3.7. Sea D un dominio principal. Sea $a \in \mathbf{M}_n(D)$. Existen entonces elementos $d_1, \ldots, d_n$ en D, tales que

$$d_i \neq 0,\ i \leq j \Rightarrow d_i / d_j$$

y la matriz a es equivalente a la matriz diagonal

$$\operatorname{diag}(d_1, \ldots, d_n)$$

Demostración. Si $n = 1$ el resultado está claro. Sea pues $1 < n$. Sea $a \neq 0$ (pues el caso $a = 0$ es trivial), existe un coeficiente $a_{ij} \neq 0$. Efectuando permutaciones de filas y columnas podemos suponer que $a_{11} \neq 0$. La idea de la demostración es bastante análoga a la utilizada en 6.3.5, pero al no disponer de un algoritmo de división, se recurre a un "invariante" en D, que es la unicidad de la representación de un elemento ($\neq 0$ y $\notin U(D)$) en producto de elementos extremales. Si a_{11} es una unidad en D, se obtiene por operaciones de filas y columnas una matriz equivalente a a del tipo

$$\begin{Vmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \square & \\ 0 & & & \end{Vmatrix}$$

donde el cuadro corresponde a una matriz de $(n-1) \times (n-1)$. Aplicando una hipótesis inductiva quedaría probada la afirmación. Análogamente, si a_{11} divide a todos los coeficientes a_{1i} y a_{j1}. Supongamos, entonces, que a_{11} no es unidad ni divide a a_{1j}. Sea d el máximo común divisor de a_{11} y a_{1j}. Existen entonces elementos $r, s \in D$ tales que $d = r \cdot a_{11} + s \cdot a_{1j}$. Sean $a'_{11} = \frac{a_{11}}{d}$ y $a'_{1j} = \frac{a_{1j}}{d}$. Resulta entonces $1 = r \cdot a'_{11} + s \cdot a'_{1j}$ y

$$\begin{Vmatrix} a'_{11} & a'_{1j} \\ s & -r \end{Vmatrix} \cdot \begin{Vmatrix} r & a'_{1j} \\ s & -a'_{11} \end{Vmatrix} = I_2$$

por lo tanto, si definimos

$$u = \begin{Vmatrix} s & 0 & \dots & a'_{1j} & \dots & 0 \\ \cdot & \cdot & \dots & \cdot & \dots & \cdot \\ r & 0 & & -a'_{11} & \dots & 0 \\ \cdot & \cdot & \dots & \cdot & \dots & \cdot \\ 0 & 0 & \dots & 0 & \dots & 1 \end{Vmatrix}$$

(con 1 sobre la diagonal, excepto en las posiciones 1 y j donde figuran s y $-a'_{11}$ respectivamente, con 0 fuera de la diagonal, excepto en las posiciones $1j$ y $j1$ donde figuran a'_{1j} y r respectivamente) se obtiene una unidad en $\mathbf{M}_n(D)$, tal que el producto $a \cdot u$ es de la forma

$$\begin{Vmatrix} d & \dots & 0 & \dots & a_{1n} \\ \cdot & \dots & \cdot & \dots & \cdot \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{Vmatrix}$$

Esta matriz es equivalente a a y habiendo supuesto que a_{11} no divide a a_{1j} y además a_{11} no es unidad, el coeficiente d en la posición 11 posee un número estrictamente menor de divisores primos que a_{11}. En esta

forma, imitando la demostración de 6.3.5 se llega a la forma diagonal pedida.

Nota. Es posible probar la unicidad de los d_i que aparecen en 6.3.5 y 6.3.7. La unicidad debe entenderse salvo en el caso de asociados, es decir que si $d_1', \ldots, d_n' \in D$ satisfacen 6.3.5 ó 6.3.7 entonces d_i es asociado a d_i' para todo $i = 1, \ldots, n$. Esto se verá en el capítulo siguiente.

4. MÓDULOS SOBRE UN DOMINIO DE INTEGRIDAD

Sea D un dominio de integridad y sea A un D-módulo.

Definición 6.4.1. Un elemento $a \in A$ se dice *de torsión* si existe $r \in D$, $r \neq 0$, tal que $r \cdot a = 0$.

Con tA denotamos la totalidad de elementos de torsión de A. Es fácil probar la siguiente proposición.

Proposición 6.4.2. 1) tA es submódulo de A

2) $t(A/tA) = 0$

3) Si C es submódulo de A entonces $tC = tA \cap C$.

Definición 6.4.3. Un módulo A se dice *sin torsión*, si $tA = 0$. Se dice *de torsión*, si $A = tA$.

Sea, para cada $r \in D$, $h_r : A \to A$ el endomorfismo multiplicación por r, o sea $h_r(a) = r \cdot a$. h_r se denomina la homotecia de A de razón r. Entonces A es sin torsión si, y sólo si, para todo $r \in D$ la sucesión

$$0 \to A \xrightarrow{h_r} A$$

es exacta, es decir h_r es un monomorfismo.

Ejemplo 1. Todo grupo abeliano finito es un $\mathbf{Z}$-módulo de torsión.

Ejemplo 2. Sea D un dominio de integridad y sea α un ideal de D. Entonces si $\alpha \neq 0$, el D-módulo D/α es de torsión. Como consecuencia

Ejemplo 3. Un dominio D tal que todo D-módulo es sin torsión es un cuerpo.

Ejemplo 4. Sea A un D-módulo sin torsión, entonces si $0 \neq r \in D$, A/rA es un módulo de torsión (en efecto, $r \cdot (A/rA) = 0$), donde $r \cdot A = h_r(A)$.

Definición 6.4.4. Un elemento $a \in A$ se dice *divisible* por $r \in D$, $r \neq 0$ si existe $a' \in A$ tal que $a = r \cdot a'$. Se dice que A es divisible por r, si todo elemento es divisible por r. Se dice que A es un *módulo divisible*, si es divisible por r para todo $r \in D$, $r \neq 0$.

Nota. La totalidad de elementos divisibles de un módulo A no tiene porqué ser un módulo divisible (en efecto, la suma de dos elementos

divisibles es divisible en A, pero puede no serlo en un submódulo contenido propiamente). No obstante los contraejemplos no son tan sencillos de dar. Para ello, el lector interesado puede consultar la referencia (7a).

Proposición 6.4.5. Sean A' y A'' submódulos de A, tales que A' y A'' son módulos divisibles. Entonces, A' + A'' es un módulo divisible. El mismo resultado es válido para una suma arbitraria de submódulos divisibles.

Demostración. Sea $a' + a'' \in A' + A''$ y sea $0 \neq r \in D$. Existen $a'_1 \in A'$, $a''_1 \in A''$, tales que $a' = r \cdot a'_1$ y $a'' = r \cdot a''_1$, por lo tanto $a' + a'' = r(a'_1 + a''_1)$ con $a'_1 + a''_1 \in A' + A''$.

Se sigue de 6.4.5 que en todo módulo A existe un submódulo δA divisible y maximal respecto de la inclusión. En efecto, sea $\{A^1_\alpha\}$ la familia de todos los submódulos A^1_α de A que son módulos divisibles (0 es un tal submódulo). La suma $\delta A = \sum_\alpha A^1_\alpha$ es un submódulo divisible y es maximal.

Definición 6.4.6. Un D-módulo A se dice ***reducido*** si $\delta A = 0$. Nótese que un módulo A es divisible si, y sólo si, $\delta A = A$. También en términos de homotecias es posible caracterizar a los módulos divisibles como aquellos para los cuales la sucesión

$$\forall r \neq 0, \qquad A \xrightarrow{h_r} A \to 0$$

es exacta, es decir h_r es un epimorfismo.

Nota. La importancia de la noción de módulo reducido se puede apreciar en el siguiente resultado. Sea D un dominio principal. Todo módulo A es *suma directa* de un módulo divisible y un módulo reducido. De esta manera, el estudio de los módulos sobre un dominio principal se puede restringir al de los divisibles y al de los reducidos.

Ejemplo 1. Sea Q el cuerpo de cocientes de D. Q es un D-módulo divisible.

Ejemplo 2. D es divisible como D-módulo si, y sólo si, D es un cuerpo. (En efecto, si D es D-divisible, la ecuación $a \cdot X = b$, $a \neq 0$, a y b en D admite solución en D. Esto equivale a que todo elemento no nulo de D sea inversible en D.)

Ejemplo 3. Sea A un módulo divisible. Si $f : A \to C$ es un morfismo, entonces $f(A)$ es un módulo divisible y $f(A) \subset \delta C$. Por lo tanto, Q/D es un módulo divisible. Si A es divisible y C es sumando directo, entonces, C es divisible. En efecto, es consecuencia de la existencia de un proyector $p : A \to C$. Puesto que para todo primo racional p, $\mathbf{Z}_{p^\infty}$ es sumando directo de $\mathbf{Q}/\mathbf{Z}$, se tiene que $\mathbf{Z}_{p^\infty}$ es divisible

Ejemplo 4. $\delta \mathbf{Z} = 0$. En efecto, todo elemento de $\mathbf{Z}$ que sea distinto de cero admite sólo un número finito de divisores. Se sigue que si A es divisible, el único morfismo de A en $\mathbf{Z}$ es el morfismo nulo (véase Estructuras Algebraicas, Parte I, pág. 26).

Ejemplo 5. Sea D un dominio de integridad y sea α un ideal de D no nulo. Entonces $\delta(D/\alpha) = 0$. En efecto, para todo $\underline{x} \in D/\alpha$ y todo $r \in \in \alpha$, $r \cdot \underline{x} = 0$, por lo tanto los elementos de D/α no son divisibles por los elementos de $\alpha \subset D$.

Ejemplo 6. Un dominio de integridad D es un cuerpo si, y sólo si, posee un módulo de tipo finito divisible no nulo. En efecto, sea A un módulo de tipo finito y divisible. $A = \langle a_1, \ldots, a_n \rangle$ con $a_1, \ldots, a_n$ un sistema *minimal* de generadores. Según 5) podemos suponer $1 < n$. El cociente $A/\langle a_2, \ldots, a_n \rangle$ es un módulo cíclico. Entonces, si A es divisible, así lo es $A/\langle a_2, \ldots, a_n \rangle$, que es $\neq 0$ y cíclico. Esto es imposible de acuerdo con 5). (Recuerde el lector que los módulos cíclicos son isomorfos a los módulos cocientes D/α de D por un ideal α de D.)

Ejemplo 7. Sean ΠZ y $\oplus Z$, respectivamente, el producto y la suma de un conjunto infinito numerable de copias de Z. Sea H el subgrupo de ΠZ formado por las sucesiones $\{a_i\}$, tales que para casi todo i, a_i es divisible por $i!$ (factorial de i). Entonces $\oplus Z \subset H$. Dejamos a cargo del lector demostrar que en el morfismo canónico $\Pi Z \to \Pi Z/\oplus Z$, H se aplica sobre un grupo divisible.

Veamos una propiedad interesante de los módulos divisibles.

Proposición 6.4.7. Sea D un dominio de integridad. Sea A un D-módulo. Consideremos la siguiente propiedad (relativa a A y D).

PI) Para todo ideal I de D y todo morfismo $\varphi' : I \to A$ existe una extensión a un morfismo $\varphi : D \to A$. Entonces,

1) Si A satisface PI), entonces A es divisible.

2) Si A es sin torsión, PI) equivale a ser A divisible.

3) Si D es dominio principal, entonces PI) equivale a que A sea divisible.

Demostración. 1) Sea $a \in A$ y sea $0 \neq r \in D$. El morfismo

$$\varphi' : \langle r \rangle \to A$$

del ideal $\langle r \rangle$ en A, definido por $\varphi'(x \cdot r) = x \cdot a$, puede extenderse a un morfismo $\varphi : D \to A$. Por lo tanto

$$a = \varphi'(r) = \varphi(r) = \varphi(r \cdot 1) = r \cdot \varphi(1)$$

lo cual prueba que a es divisible por r.

2) En virtud de 1) será suficiente probar que si A es sin torsión y divisible, entonces se satisface PI). Sea $z \in D$, supongamos $I \neq 0$, con lo que existe $0 \neq y \in I$. Entonces si $\varphi' : I \to A$ es un morfismo.

$$\varphi'(z \cdot y) = z \cdot \varphi'(y) = z \cdot a, \text{ si } \varphi'(y) = a.$$

Por ser A divisible existe $a' \in A$, tal que $z \cdot a = y \cdot a'$. Afirmamos que a' es único. En efecto, $z \cdot a = y \cdot a' = y \cdot a''$ implica $0 = y \cdot (a' - a'')$ y,

como A es sin torsión, resultará $a' = a''$. Sea $0 \neq y' \in I$. Se tiene, análogamente,

$$\varphi'(z \cdot y') = z \cdot \varphi'(y') = z \cdot b = y' \cdot b' \text{ si } \varphi'(y') = b$$

y entonces

$$\varphi'(z \cdot y \cdot y') = y \cdot y' \cdot b'$$
$$\varphi'(z \cdot y \cdot y') = y' \cdot y \cdot a'$$

con lo que $a' = b'$.

Se ha demostrado que si $z \in D$, existe un único $a' \in A$, tal que

$$\forall\, y \in I,\ \varphi'(z \cdot y) = y \cdot a'$$

por lo tanto podemos definir

$$\varphi : D \to A \text{ por } \varphi(z) = a'$$

φ extiende φ' y es trivialmente un morfismo. Se ha probado 2).

3) En virtud de 1) será suficiente probar que si A es divisible entonces (bajo la hipótesis de ser D principal) A satisface PI). Sea $\varphi' : I \to A$ un morfismo y sea $z \in D$. Supongamos $z \notin I$. Vamos a extender $\varphi' : I \to A$ a $\varphi'' : I + D \cdot z \to A$, donde $I + D \cdot z$ es el ideal generado por I y z, y es estrictamente más grande que I (dado que $z = 0 + 1 \cdot d \in I + D \cdot z$, pero $z \notin I$). Un elemento típico de $I + D \cdot z$ es de la forma $y + d \cdot z$, $y \in I$, $d \in D$. Sea $J = \{x / x \in D \text{ con } x \cdot z \in I\}$. J es un ideal de D, y siendo D principal, $J = \langle r \rangle$. Entonces $r \cdot z \in I$, con lo que está definido $\varphi'(r \cdot z)$. Por la divisibilidad de A, sea $a' \in A$, tal que

$$\varphi'(r \cdot z) = r \cdot a'.$$

Notas. Si se supone que $I \neq 0$, entonces $I \subset J$ no puede ser 0, con lo que $r \neq 0$. Además, a' no necesita ser único, como lo era en la demostración de 2). Por esta razón se introdujo la hipótesis de principalidad de D.

Vamos a probar que la correspondencia $y + d \cdot z \to \varphi'(y) + d \cdot a'$ está bien definida (de $I + D \cdot z$ en A). En efecto, sea

$$y + d \cdot z = y' + d' \cdot z.$$

Entonces

$$(d - d') \cdot z = y' - y \in I$$

lo cual implica

$$d - d' = s \cdot r,\ s \in D.$$

Por lo tanto

$$\begin{aligned}\varphi'(y) + d \cdot a' &= \varphi'(y - y') + \varphi'(y') + d \cdot a' = \varphi'((d' - d) \cdot z) + \varphi'(y') + d \cdot a' = \\ &= -s \cdot \varphi'(r \cdot z) + \varphi'(y') + d \cdot a' = -s \cdot r \cdot a' + \varphi'(y') + d \cdot a' = \\ &= (d' - d) \cdot a' + \varphi'(y') + d \cdot a' = \\ &= \varphi'(y') + d' \cdot a'.\end{aligned}$$

Esto prueba que la correspondencia $y + d \cdot z \to \varphi'(y) + d \cdot a'$ está bien definida y es una aplicación $\varphi'' : I + D \cdot z \to A$; y es además un morfismo, como es fácil de verificar. Extiende φ':

$$\text{Si } y \in I, \quad \varphi''(y) = \varphi''(y + 0 \cdot z) = \varphi'(y).$$

De esta forma obtenemos sucesivas extensiones $\varphi'', \varphi''', \ldots$, de φ'. Como estas extensiones son estrictas y D es noetheriano, al cabo de un número finito de pasos debemos lograr la extensión buscada a D.

7

MÓDULOS SOBRE UN DOMINIO PRINCIPAL

Este capítulo tratará sobre la teoría de módulos de tipo finito sobre un dominio principal. Como un caso particular se obtendrá la clasificación completa de grupos abelianos de tipo finito. Un resultado fundamental establece que un módulo A sobre un dominio principal se "parte" en suma directa $A = tA \oplus L$, de su submódulo de torsión tA, y en un submódulo L libre de tipo finito. La descomposición $A = tA \oplus L$ es única, salvo la posibilidad de escribir $A = tA \oplus L'$ con $L \simeq L'$. Este resultado divide el estudio de los módulos de tipo finito sobre un dominio principal en el estudio de módulos de torsión y módulos libres. Estos últimos quedan unívocamente determinados por su rango (concepto análogo al de dimensión en la teoría de espacios vectoriales). Los módulos de torsión se clasifican según sus factores invariantes o, equivalentemente, según sus divisores elementales. En esta forma, la teoría de estructura de módulos de tipo finito sobre un dominio principal está completamente determinada. Sin la condición de finitud no hay teoría completa, salvo en casos particulares. Aun en el caso de grupos abelianos no hay teoría general, y así ocurre, por ejemplo, en el caso de grupos abelianos sin torsión ($tA = 0$).

1. EXTENSIÓN DE MORFISMOS Y MÓDULOS DE TIPO FINITO SIN TORSIÓN

Sea D un dominio principal y sea Q su cuerpo de cocientes. Q es naturalmente un D-módulo y además un módulo divisible (es decir, dados $q \in Q$, $r \in D$, $0 \neq r$, existe $q' \in Q$ tal que $q = r \cdot q'$). Vamos a probar el siguiente teorema de extensión de morfismos. En el mismo, Q se puede reemplazar por cualquier módulo divisible. (Compárese con 6.4.7, 3).)

Teorema 7.1.1. Sea A un D-módulo de tipo finito y sea $\varphi' : A' \to Q$ un morfismo de un submódulo A' de A en Q. Entonces φ' se extiende a un morfismo $\varphi : A \to Q$.

Demostración. Sea $A' \neq A$ y sea $a \in A - A'$. Sea

$$I = \{k / k \in D \text{ y } k \cdot a \in A'\}.$$

Nótese que $0 \in I$, de modo que I no es vacío. Además

$$k', k'' \in I \Rightarrow k' - k'' \in I$$

$$r \in D, k \in I \Rightarrow r \cdot k \in I$$

de manera que I es un ideal de D, por lo tanto es de la forma

$$I = \langle t \rangle = D \cdot t.$$

Es claro que también $t \cdot a \in A'$. Sea $q \in Q$ con la propiedad

$$\varphi'(t \cdot a) = t \cdot q.$$

(Lector: Note que no es lícito escribir $\varphi'(t \cdot a) = t \cdot \varphi'(a)$, pues $a \notin A'$. Precisamente, el q elegido jugará un papel vital en la extensión del morfismo.)

La elección de q es posible gracias a la divisibilidad de Q. Sea

$$A'' = A' + D \cdot a = A' + \langle a \rangle$$

es decir, el submódulo de A generado por A' y a. Los elementos de A'' son de la forma $a' + k \cdot a$, $a' \in A'$ y $k \in D$. Además, si

$$a' + k \cdot a = a'_1 + k_1 \cdot a$$

$$a', a'_1 \in A' \text{ y } k, k_1 \in D$$

entonces

$$(k_1 - k) \cdot a = a' - a'_1 \in A'$$

lo cual implica que

$$k_1 - k \in I, \text{ o sea } k_1 - k = r \cdot t, \ r \in D.$$

Como consecuencia

$$\begin{aligned}
\varphi'(a') + k \cdot q &= \varphi'(a'_1 + (k_1 - k) \cdot a) + k \cdot q = \\
&= \varphi'(a'_1) + \varphi'((k_1 - k) \cdot a) + k \cdot q = \\
&= \varphi'(a'_1) + r \cdot \varphi'(t \cdot a) + k \cdot q = \\
&= \varphi'(a'_1) + r \cdot t \cdot q + k \cdot q = \\
&= \varphi'(a'_1) + (k_1 - k) \cdot q + k \cdot q = \\
&= \varphi'(a'_1) + k_1 \cdot q
\end{aligned}$$

Esto equivale a decir que a cada elemento $a' + k \cdot a \in A' + D \cdot a$ se le puede asignar unívocamente el elemento $\varphi'(a') + k \cdot q$, o sea

$$a' + k \cdot a \mapsto \varphi'(a') + k \cdot q$$

define una aplicación

$$\varphi'' : A'' \to Q$$

que posee las propiedades siguientes:

i) φ'' es un morfismo

ii) Si $a' \in A'$, entonces $\varphi'(a') = \varphi''(a')$.

(Se deja estas verificaciones a cargo del lector.) En definitiva, se ha construido una extensión de $\varphi' : A' \to Q$ a $\varphi'' : A'' \to Q$. Notemos que A'' es estrictamente más grande que A', dado que $a \notin A'$. De esta ma-

nera, repitiendo el proceso se logra extensiones sucesivas de $\varphi' : A' \to Q$:

$$A' \subset A'' \subset A''' \subset \ldots$$

Como D es un anillo noetheriano y A es de tipo finito, se sigue que A es un módulo noetheriano, por lo tanto toda cadena creciente de submódulos debe ser estacionaria al cabo de un número finito de pasos. Ahora bien, el módulo donde se estaciona la cadena no puede ser otro que A, pues si no fuera así construiríamos una extensión propia del mismo. El teorema queda probado.

Corolario 7.1.2. Sea A un D-módulo de tipo finito y sea $0 \neq a \in A$ un elemento *sin torsión*. Entonces existe un morfismo $\varphi : A \to Q$ tal que $\varphi(a) = 1$.

Demostración. Si a es sin torsión, entonces $\langle a \rangle = D \cdot a \simeq D$ por la aplicación $\varphi' : \langle a \rangle \to D$, $\varphi'(k \cdot a) = k$. Por 7.1.1 φ' se extiende a un morfismo $\varphi : A \to Q$ y, por lo tanto, $\varphi(a) = \varphi'(a) = \varphi'(1 \cdot a) = 1$ como se quería probar.

Corolario.7.1.3. Sea A un D-módulo de tipo finito. Entonces $\mathrm{Hom}_D(A, Q) \neq 0$ si, y sólo si, $A \neq tA$ (donde tA denota el submódulo de torsión de A).

Demostración. Se deja a cargo del lector.

El siguiente lema caracteriza los submódulos de tipo finito del cuerpo de cocientes de un dominio principal.

Lema 7.1.4. Sea Q el cuerpo de cocientes de un dominio principal D. Entonces todo submódulo A de Q de tipo finito es cíclico.

Demostración. Sea $\{x_1, \ldots, x_n\}$ un conjunto finito de generadores de A. Podemos escribir

$$x_i = \frac{p_i}{q_i}; \quad p_i, q_i \in D, \ q_i \neq 0$$

$$\text{si } i = 1, \ldots, n.$$

Sea $q = \Pi q_i$ producto de los denominadores q_i. Entonces $0 \neq q$ y $q \cdot x_i \in D$ cualquiera que sea i. Por lo tanto

$$q \cdot A \subset D$$

es un ideal de D, por lo tanto principal. Puesto que la multiplicación por q es un D-morfismo y, más aún, un isomorfismo

$$A \to q \cdot A = \langle t \rangle,$$

A resulta cíclico.

Probaremos ahora el importante teorema siguiente.

Teorema 7.1.5. Todo D-módulo A de tipo finito y sin torsión es libre.

Demostración. Sea $0 \neq A$ y sea $\varphi : A \to Q$ un morfismo no nulo de A en Q (corolario 7.1.3). Siendo $\varphi(A)$ un submódulo de Q de tipo finito, 7.1.4 implica que $\varphi(A) = D \cdot q = \langle q \rangle$, $q \neq 0$.

Por ser $\varphi(A) = \langle q \rangle$ libre, el morfismo $\varphi : A \to \langle q \rangle$ es partible y así podemos escribir

$$A = A_1 \oplus L \quad \text{con} \quad L \simeq \langle q \rangle,$$

por lo tanto

$$A = A_1 \oplus \langle e_1 \rangle .$$

Podemos repetir el razonamiento con A_1 (si es $\neq 0$, pues es un D-módulo de tipo finito y sin torsión) y obtener

$$A = A_2 \oplus \langle e_2 \rangle \oplus \langle e_1 \rangle .$$

De esta manera se obtiene una cadena creciente

$$\langle e_1 \rangle \subset \langle e_1 \rangle \oplus \langle e_2 \rangle \subset \ldots$$

de submódulos de A. Siendo A noetheriano debe existir $n \in N$ donde dicha cadena se estabiliza. Pero ello debe ocurrir cuando

$$A = \langle e_1 \rangle \oplus \langle e_2 \rangle \oplus \ldots \oplus \langle e_n \rangle .$$

Resulta entonces que $e_1, \ldots, e_n$ es una base de A y el teorema queda
94 probado.

Nota. Sin la hipótesis de finitud, el teorema 7.1.5 no es válido. Por ejemplo, en el caso del anillo **Z** de enteros racionales, el grupo **Q** de números racionales es sin torsión, pero no es libre. Su justificación se deja a cargo del lector y se le propone que pruebe el siguiente resultado más general: si D es un dominio, con $D \neq Q$ su cuerpo de cocientes, entonces 0 es el único módulo sobre D que es simultáneamente libre y divisible.

Corolario 7.1.6. Todo submódulo de un módulo libre de tipo finito sobre un dominio principal es libre.

Demostración. Se deja su demostración como ejercicio para el lector.

Nota. Se puede probar que 7.1.6 es válido sin condiciones de finitud, es decir: Todo submódulo de un módulo libre sobre un dominio principal es libre.

Teorema 7.1.7. Sea A un módulo de tipo finito sobre un dominio principal D. Existe entonces un módulo libre L, submódulo de A, tal que $A = tA \oplus L$.

Demostración. A/tA es sin torsión y finitamente generado y por lo tanto es libre. En consecuencia, el morfismo canónico $A \to A/tA$ es partible, con lo que podemos escribir

$$A = tA \oplus L, \quad L \simeq A/tA.$$

El teorema queda probado. En virtud de este teorema y como se dijo al iniciar este capítulo, la teoría de módulos de tipo finito sobre un dominio principal se divide en dos direcciones: módulos libres y módulos de torsión.

2. MÓDULOS LIBRES DE TIPO FINITO

Su teoría es completamente análoga a la teoría de espacios vectoriales de dimensión finita. En efecto,

Proposición 7.2.1. Sea A un módulo libre de tipo finito sobre un dominio principal D. Entonces dos bases de A poseen el mismo número de elementos.

Demostración. Sea $V = \mathrm{Hom}_D(A, Q)$, siendo Q el cuerpo de cocientes de D. Vamos a definir sobre V, en forma natural, una estructura de módulo sobre Q, es decir una estructura de Q-espacio vectorial: si $q \in Q$, $\varphi \in \mathrm{Hom}_D(A, Q)$ definimos $(q \cdot \varphi)(a) = q \cdot \varphi(a)$ cualquiera que sea $a \in A$.

Nos limitaremos a probar que $q \cdot \varphi$ es, efectivamente, un D-morfismo de A en Q. El resto de los detalles quedan a cargo del lector.

$$(q \cdot \varphi)(k \cdot a) = q \cdot (\varphi(k \cdot a)) = q \cdot (k \cdot \varphi(a)) = (q \cdot k) \cdot \varphi(a) =$$
$$= (k \cdot q) \cdot \varphi(a) = k \cdot (q \cdot \varphi(a)) = k \cdot ((q \cdot \varphi)(a)).$$

Vamos a calcular

$$\dim_Q \mathrm{Hom}_D(A, Q)$$

Para ello sea para cada i, $i = 1, \ldots, n$,

$$\varphi_i : A \to Q \tag{1}$$

definida por

$$\varphi_i(e_j) = 0, \text{ si } i \neq j$$
$$\varphi_i(e_i) = 1$$

donde $e_1, \ldots, e_n$ es una base de A fijada de antemano. Probaremos que $\{\varphi_i\}_{i=1}^{n}$ es una base de V. Sea $\varphi \in V$, entonces

$$\varphi = \sum_{i=1}^{n} \varphi(e_i)\varphi_i \tag{2}$$

dado que para todo j, $j = 1, \ldots, n$,

$$\Big[\sum_{i=1}^{n} \varphi(e_i)\varphi_i\Big](e_j) = \sum_{i=1}^{n} \varphi(e_i) \cdot \varphi_i(e_j) = \varphi(e_j)$$

lo cual dice que ambos miembros de (2) toman los mismos valores, como funciones, sobre una base de A. Son, por lo tanto, iguales. Veamos la idependencia lineal. Sea pues

$$\sum_{i=1}^{n} q_i \cdot \varphi_i = 0$$

Aplicando el primer miembro a e_j resulta

$$0 = \sum_{i=1}^{n} q_i \cdot \varphi_i(e_j) = q_j$$

y de allí la independencia lineal. Esto concluye la demostración de que (1) es base de V. Por lo tanto, V posee una dimensión igual a n. Como este n era el número de elementos de una base de A y como la dimensión de un espacio vectorial es una invariante, se concluye que dos bases de A poseen el mismo número de elementos. El teorema queda probado.

Definición 7.2.2. Sea A un módulo libre de tipo finito sobre un dominio principal. Se llama *rango* de A y se denota por $r(A)$ al invariante determinado por 7.2.1. Además, se fija $r(0) = 0$.

El siguiente teorema clasifica los D-módulos libres de tipo finito.

Teorema 7.2.3. Sean A y B módulos libres de tipo finito sobre un dominio principal D. Entonces

$$A \simeq B \text{ si, y sólo si, } r(A) = r(B).$$

Demostración. Es consecuencia inmediata de 7.2.1.

El D-módulo $D^n = D \oplus \ldots \oplus D$ (n copias) es un D-módulo libre de rango n. Por lo tanto, todo D-módulo libre de tipo finito es isomorfo a uno, y sólo uno, D^n.

Notemos finalmente que si A es un D-módulo de tipo finito y L, L' son submódulos de A, tales que

$$A = tA \oplus L = tA \oplus L'$$

entonces

a) $L \simeq L'$

b) L y L' son libres.

En efecto,

$$L \simeq A/tA \simeq L'$$

por lo tanto, L es sin torsión y de tipo finito, luego es libre.

Definición 7.2.4. Sea A un D-módulo de tipo finito. Se llama *rango* de A, al rango $r(L)$ de la parte libre en la descomposición

$$A = tA \oplus L.$$

Escribimos $r(A)$ como en el caso libre. Notemos que se tiene

$$r(A) = r(L), \text{ si } A = tA \oplus L.$$

Ejemplo. $r(\mathbf{Z}_n) = 0$, $r(\mathbf{Z} \oplus \mathbf{Z}_n) = 1$, $r(\mathbf{Z}^n) = n$.

Se deja a cargo del lector la demostración de las siguientes propiedades:

i) Si A es un D-módulo de tipo finito y $A = A' \oplus A''$, entonces $r(A) = r(A') + r(A'')$.

ii) Si $0 \to A' \to A \to A'' \to 0$ es una sucesión exacta corta de D-módulos de tipo finito, entonces $r(A) = r(A') + r(A'')$.

iii) Sea A un D-módulo de tipo finito. Entonces

$$r(A) = \dim_Q(\mathrm{Hom}_D(A, Q)).$$

Nota. Este resultado permite definir $r(A)$ para todo D-módulo, y aun para módulos sobre dominios de integridad (no necesariamente principales).

iv) Un D-módulo A de tipo finito es de torsión si, y sólo si, $r(A) = 0$. (En efecto, si $A = tA$, entonces cualquiera que sea $f \in \mathrm{Hom}_D(A, Q)$, se tiene $f(A) \subset tQ = 0$, luego $f = 0$. Recíprocamente, si $r(A) = 0$, entonces $\mathrm{Hom}_D(A, Q) = 0$ y por 7.1.3 es $A = tA$.

3. MÓDULOS DE TORSIÓN

Comencemos por repasar algunas definiciones y señalar algunos hechos elementales. Sea D un dominio principal, P la totalidad de elementos extremales (o irreducibles) de D, y A un D-módulo de torsión. Si $\pi \in P$ definimos la componente π-primaria de A por

$$A_\pi = \{a/a \in A \text{ y existe } n \in N \text{ tal que } \pi^n \cdot a = 0\}.$$

Se dice que A es un π-módulo, si $A = A_\pi$. Si A es un D-módulo de torsión, vale la siguiente representación de A

$$A = \sum_{\pi \in P} \oplus A_\pi$$

hecho que se demuestra en forma enteramente análoga al caso de grupos abelianos de torsión.

Sea $a \in A$. Llamaremos *orden de* a al ideal de D, anulador de a, es decir

$$O_a = \mathrm{An}(a) = \{r/r \in D \text{ y } r \cdot a = 0\}.$$

Puesto que $O_a = \langle d \rangle$, por abuso de lenguaje diremos también que d es orden de a. (En general, no hay posibilidad de elegir un generador canónico (o sea natural) de O_a, pero en el caso de Z, d puede elegirse no negativo y en el caso de $K[X]$, K un cuerpo, se puede elegir d mónico o sea con coeficiente de mayor grado igual a 1). Recordemos que vale el siguiente isomorfismo

$$\langle a \rangle \simeq D/O_a$$

Este isomorfismo puede verse fácilmente, definiendo

$$f : D \to A \quad \text{por} \quad f : r \to r \cdot a .$$

Entonces $\langle a \rangle = f(D) \simeq D/Nu(f) = D/O_a$, como se quería probar. Si $\langle d \rangle$ es el ideal de D, generado por d, $d \in D$, convendremos en representar por D_d el módulo cociente $D/\langle d \rangle$.

En general, podemos definir, para cada subconjunto X de A su anulador, el ideal

$$An(X) = \{r / r \cdot x = 0 \text{ para todo } x \in X\}.$$

Es fácil ver la validez de la relación siguiente

$$An(D_d) = \langle d \rangle .$$

En efecto, si $\rho : D \to D/\langle d \rangle$ designa el morfismo canónico, $\underline{1} = \rho(1)$ es generador de $D/\langle d \rangle$, llamado generador canónico de $D/\langle d \rangle$. Entonces

$$r \in An(D_d) \Leftrightarrow 0 = r \cdot \underline{1} = r \cdot \rho(1) = \rho(r) \Leftrightarrow r \in \langle d \rangle .$$

Vale también la siguiente relación

$$An(A \oplus C) = An(A) \cap An(C).$$

Así, por ejemplo

$$An(\mathbf{Z}_n \oplus \mathbf{Z}_m) = \langle [n,m] \rangle .$$

Si D = $\mathbf{Z}$ la noción de orden de un elemento $a \in A$ coincide con la noción de orden de la teoría de grupos, es decir con el cardinal del subgrupo generado por a, o lo que es lo mismo, con el menor $d \in N$, tal que $da = 0$.

Otra propiedad válida si D = $\mathbf{Z}$, es la siguiente: Todo $\mathbf{Z}$-módulo de torsión de tipo finito *es finito* (o sea todo grupo abeliano de torsión y de tipo finito es finito). En efecto, sea $v_1, \ldots, v_n$ un sistema de generadores de un grupo abeliano A de torsión y de tipo finito. Sea m = máximo (orden(v_1), ..., orden(v_n)). Entonces escribiendo para todo $x \in A$

$$x = m_1 \cdot v_1 + \ldots + m_n \cdot v_n$$

los coeficientes m_i pueden tomarse en el intervalo natural $[\![1, m]\!]$. Por lo tanto, A puede tener a lo sumo

$$m \times \ldots \times m = m^n$$

elementos distintos.

Sea π un elemento extremal de D. Vamos a construir el análogo a $\mathbf{Z}_{p\infty}$. Puesto que nuestra discusión de la construcción de $\mathbf{Z}_{p\infty}$ fue lo suficientemente detallada, se omite ahora algunas explicaciones. De todos modos, se invita al lector, en este punto, a repasar las propiedades de $\mathbf{Z}_{p\infty}$.

Sea H_π el submódulo de Q (el cuerpo de cocientes de D) formado por todas las fracciones que admiten una representación

$$a/\pi^i, \quad i \in N, \quad a \in D$$

H_π puede expresarse como unión de la cadena infinita de submódulos cíclicos

$$(1) \qquad D \subset \pi^{-1} \cdot D \subset \pi^{-2} \cdot D \subset \pi^{-3} \cdot D \subset \ldots \to H_\pi .$$

Además, cada término $\pi^{-1} \cdot D$ es maximal en el siguiente $\pi^{-(i+1)} \cdot D$. En efecto, la multiplicación por π^{i+1} induce un diagrama conmutativo

$$\begin{array}{ccc} \pi^{-(i+1)} \cdot D & \xrightarrow{\pi^{i+1}} & D \\ \uparrow & & \uparrow \\ \pi^{-1} \cdot D & \xrightarrow{\pi^{i+1}} & \pi \cdot D \end{array}$$

donde los morfismos verticales son las inclusiones y los morfismos horizontales son isomorfismos. Puesto que $\pi \cdot D$ es maximal en D, nuestra afirmación queda probada.

Sea $D_{\pi\infty}$ el módulo cociente

$$D_{\pi\infty} = H_\pi / D$$

(1) induce al pasar al cociente, la sucesión de módulos cíclicos

$$(2) \qquad 0 \subset D_\pi \subset D_{\pi^2} \subset D_{\pi^3} \subset \ldots \to D_{\pi\infty}, \quad D_{\pi^i} \simeq D/\langle \pi^i \rangle$$

donde cada D_{π^i} es maximal en el siguiente $D_{\pi^{i+1}}$.

Esta propiedad hace, como se vio en $\mathbf{Z}_{p\infty}$, que los únicos submódulos de $D_{\pi\infty}$ sean los que aparecen en (2).

Nota. La inclusión $\pi^{-1} \cdot D \subset \pi^{-(i+1)} \cdot D$ está dada por $\pi^{-1} \to \pi \cdot \pi^{-(i+1)} = \frac{\pi}{\pi^{i+1}}$ esto implica que la inclusión $D_{\pi^i} \to D_{\pi^{(i+1)}}$ está dada por

$$\underline{1} \to \pi \cdot \underline{1}$$

donde $\underline{1}$ indica el generador de D_{π^i} canónico, es decir la imagen de 1 en el morfismo canónico $D \to D_{\pi^i}$.

Sea A un D-módulo de torsión. Entonces podemos escribir

$$A = \sum_{\pi \in P} \oplus A_\pi$$

suma directa de las componentes π-primarias. Esta descomposición es única, puesto que los A_π están unívocamente determinados. Por lo tanto, podemos particularizar el estudio de A a sus componentes π-primarias. Es decir, podemos, sin pérdida de generalidad, suponer que A es un π-módulo, es decir $A = A_\pi$.

Teorema 7.3.1. Sea A un π-módulo de tipo finito. Entonces A es suma directa de módulos cíclicos:

$$A \simeq D_{\pi^{i_1}} \oplus \ldots \oplus D_{\pi^{i_s}}$$

Demostración. Sea $\langle \pi^m \rangle$ el anulador de A. Si $a_1, \ldots, a_h$ es un sistema de generadores de A entonces

$$\langle \pi^m \rangle = 0_{a_1} \cap \ldots \cap 0_{a_h} = \langle \pi^{s_1} \rangle \cap \ldots \cap \langle \pi^{s_h} \rangle = \langle \pi^{\max(s_1, \ldots, s_h)} \rangle$$

Por lo tanto, algún $s_i = m$. Además, si $x \in A$ posee un orden $\langle \pi^f \rangle$ es $f \leq m$, pues escribiendo $x = \sum_{i=1}^{h} r_i \cdot a_i$, π^m anula al segundo miembro y, por tanto, al primero, con lo que $\pi^m \in \langle \pi^f \rangle$, y así $f \leq m$. Hemos pues determinado un elemento a de A tal que su orden $\langle \pi^m \rangle$ es maximal en m. $\langle a \rangle$ es isomorfo a D_{π^m} e induce un morfismo

$$\varphi' : \langle a \rangle \rightarrow D_{\pi^m} \subset D_{\pi^\infty}$$

En virtud de 7.1.1 (o su equivalente, reemplazando Q por cualquier módulo divisible) φ' admite una extensión a un morfismo

$$\varphi : A \rightarrow D_{\pi^\infty}$$

y puesto que los únicos submódulos de D_{π^∞} son del tipo

$$0, \; D_{\pi^t}, \; D_{\pi^\infty}$$

se tiene que

$$\varphi(A) = D_{\pi^t}, \; m \leq t \quad \text{pues} \quad \varphi(\langle a \rangle) = D_{\pi^m} \subset \varphi(A).$$

100

Puesto que $\pi^m \cdot A = 0$, se tiene que $\pi^m \cdot D_{\pi^t} = 0$, con lo cual se tiene que $t \leq m$. En definitiva $t = m$, lo cual implica

$$\varphi(\langle a \rangle) = \varphi(A) = D_{\pi^m}.$$

Vamos a probar que $\langle a \rangle$ es sumando directo de A. Sea $\underline{b} \in D_{\pi^m}$, tal que

$$\varphi(a) = \underline{b}$$

entonces $\underline{b}$ es generador de D_{π^m} y podemos definir un morfismo inverso $\Psi : D \rightarrow A$ por $\Psi(\underline{b}) = a$. En esta forma el morfismo φ es partible, con lo que

$$A = \mathrm{Nu}(\varphi) \oplus \mathrm{Im}(\Psi) = A' \oplus \langle a \rangle$$

$$A' = \mathrm{Nu}(\varphi).$$

El mismo razonamiento se puede repetir con A' y obtener así

$$A = A'' \oplus \langle a' \rangle + \langle a \rangle.$$

De esta forma queda determinada una cadena creciente

$$\langle a \rangle \subset \langle a \rangle \oplus \langle a' \rangle \subset \ldots$$

de submódulos de A. Siendo A noetheriano, dicha cadena debe estacionarse en un submódulo de A que no puede ser sino A. En definitiva hemos representado a A en la forma

$$A = \langle a_1 \rangle \oplus \ldots \oplus \langle a_n \rangle$$

es decir, como la suma directa de módulos cíclicos. El teorema queda probado.

De la demostración de 7.3.1 se sigue el siguiente resultado

Proposición 7.3.2. Sea A un π-módulo de tipo finito. Sea $a \in A$ un elemento de orden π^m, con m maximal (entre los exponentes de órdenes π^j de elementos de A). Entonces $\langle a \rangle$ es sumando directo de A.

El teorema 7.3.1. expresa entonces que los π-módulos de tipos finitos pueden describirse por sucesiones finitas de enteros positivos $(i_1, i_2, \ldots, i_h) i_1 \leq i_2 \leq \ldots \leq i_h$, correspondientes a la representación

$$D_{\pi^{i_1}} \oplus D_{\pi^{i_2}} \oplus \ldots \oplus D_{\pi^{i_h}}.$$

Así, por ejemplo, los únicos p-grupos (p primo) de órdenes

$$p^2 \text{ son } \mathbf{Z}_p \oplus \mathbf{Z}_p \text{ y } \mathbf{Z}_{p^2}$$
$$p^3 \text{ son } \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p,\ \mathbf{Z}_p \oplus \mathbf{Z}_{p^2} \text{ y } \mathbf{Z}_{p^3}$$

a los cuales corresponderían, respectivamente, los símbolos

$$(1,1) \text{ y } (2)$$
$$(1,1,1),\ (1,2) \text{ y } (3).$$

Se trata de ver si a un π-módulo pueden corresponderle diferentes símbolos del tipo $(i_1, i_2, \ldots, i_h)$, $i_1 \leq i_2 \leq \ldots \leq i_h$.

El teorema siguiente demostrará la invariancia de dichos símbolos, y los hechos elementales que se señalan a continuación se utilizarán en la demostración del mismo.

Sean R un anillo conmutativo, A un R-módulo y $r \in R$. Entonces

a) Los subconjuntos

$$r \cdot A = \{r \cdot a / a \in A\} \text{ y}$$
$${}_rA = \{a / r \cdot a = 0\}$$

son submódulos de A

b) La aplicación $h_r : A \to A$ definida por $h_r(x) = r \cdot x$, es un endomorfismo (denominado la *homotecia* de razón r) e induce la sucesión exacta

$$0 \to {}_rA \xrightarrow{i} A \xrightarrow{h_r} r \cdot A \to 0$$

donde i es la inclusión.

c) Sea $g : A \to C$ un morfismo de R-módulos. Entonces el siguiente diagrama, donde g' es la restricción de g a $r \cdot A$,

$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ {\scriptstyle h_r}\downarrow & & \downarrow{\scriptstyle h_r} \\ r \cdot A & \xrightarrow{g'} & r \cdot C \end{array}$$

es conmutativo.

d) Si en c) φ es un isomorfismo entonces φ' es un isomorfismo. Por abuso de notación escribiremos $\varphi' = \varphi$. Además, para todo dominio principal D y elemento extremal π identificamos D_{π^t} al submódulo de $D_{\pi^{t+1}}$, por el morfismo inducido por $\underline{1} \to \pi \cdot \underline{1}$, donde $\underline{1}$ denota en ambos casos el generador canónico de D_{π^t} y de $D_{\pi^{t+1}}$. Notemos que la multiplicación por π induce entonces una sucesión exacta

$$0 \to D_\pi \to D_{\pi^{t+1}} \xrightarrow{\pi} D_{\pi^t} \to 0$$

Antes de probar el teorema y con el propósito de fijar las ideas demos un ejemplo sencillo.

Ejemplo. No existe isomorfismo alguno $\varphi: \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_{p^2} \to \mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}$ donde p sea un primo. Razonando por el absurdo, supongamos la existencia de un tal isomorfismo. Consideremos el diagrama conmutativo siguiente

$$\begin{array}{ccc} \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_{p^2} & \xrightarrow{\varphi} & \mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2} \\ \downarrow h_p & & \downarrow h_p \\ \mathbf{Z}_p & \xrightarrow{\varphi} & \mathbf{Z}_p \oplus \mathbf{Z}_p \end{array}$$

φ induce entonces un isomorfismo $\mathbf{Z}_p \simeq \mathbf{Z}_p \oplus \mathbf{Z}_p$, el cual es también un isomorfismo de $\mathbf{Z}_p$-módulos, y siendo $\mathbf{Z}_p$ un cuerpo, se tienen dos espacios vectoriales de distinta dimensión (1 el miembro izquierdo y 2 el miembro derecho) isomorfos. Esto contradice la invariancia de la dimensión en espacios vectoriales. (En realidad, un isomorfismo $\mathbf{Z}_p \simeq \mathbf{Z}_p \oplus \mathbf{Z}_p$ es imposible por el simple hecho de tratarse de grupos de distinto orden, p el de la izquierda y p^2 el de la derecha, pero este argumento no se puede generalizar a módulos sobre un D cualquiera.)

Teorema 7.3.3. Sea

$$D_{\pi^{i_1}} \oplus \ldots \oplus D_{\pi^{i_h}} \simeq D_{\pi^{j_1}} \oplus \ldots \oplus D_{\pi^{j_k}} \tag{1}$$

con $i_1 \leq \ldots \leq i_h$, $j_1 \leq \ldots \leq j_k$ enteros positivos. Entonces $h = k$, y para todo índice t, $1 \leq t \leq h = k$ es $i_t = j_t$.

Demostración. Razonaremos inductivamente en el máximo (max) de los exponentes

$$i_1, \ldots, i_h; j_1, \ldots, j_k$$

Si max = 1, entonces (1) se escribe en la forma

$$\underbrace{D_\pi \oplus \ldots \oplus D_\pi}_{h \text{ copias}} \simeq \underbrace{D_\pi \oplus \ldots \oplus D_\pi}_{k \text{ copias}} \tag{2}$$

Puesto que π anula a ambos miembros de (2), dichos módulos son $D/\langle\pi\rangle$-módulos (Véase 7.1.4, ejemplo 4) y entonces (2) es un isomorfismo de D_π-módulos. Pero D_π es un cuerpo, pues $\langle\pi\rangle$ es un ideal maximal. (2) es pues un ismorfismo de espacios vectoriales sobre el cuerpo D_π. El miembro izquierdo tiene dimensión h y el de la derecha k, con respecto a D . Por la invariancia de la dimensión debe ser $k = h$, lo cual prueba el teorema en la situación particular en que max = 1. Sea pues 1 < max y razonemos inductivamente.

Denotemos por φ el isomorfismo (1). En virtud de ser φ un morfismo, la propiedad $\varphi(k \cdot x) = k \cdot \varphi(x)$, $k \in D$ implica

$$\forall \gamma \in D,\ \gamma \cdot x = 0 \text{ si, y sólo si, } \gamma \cdot \varphi(x) = 0$$

con lo que aplica biyectivamente los elementos de orden π en los elementos de orden π. Además, aplica múltiplos de π en múltiplos de π.

En la sucesión

$$(i_1, \ldots, i_h) \quad \text{con} \quad i_1 \leq \ldots \leq i_h$$

denotemos por s, $1 \leq s \leq h$ el primer índice tal que $1 < i_s$. Análogamente, sea t, $1 \leq t \leq k$, el primer índice en $(j_1, \ldots, j_k)$, tal que $1 < j_t$.

Teniendo en cuenta los hechos mencionados construimos el siguiente diagrama

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
D_\pi \oplus \ldots \oplus D_\pi & \xrightarrow{\varphi} & D_\pi \oplus \ldots \oplus D_\pi \\
h \text{ copias} & & k \text{ copias} \\
\downarrow & & \downarrow \\
D_{\pi^{i_1}} \oplus \ldots \oplus D_{\pi^{i_h}} & \xrightarrow{\varphi} & D_{\pi^{j_1}} \oplus \ldots \oplus D_{\pi^{j_k}} \\
\downarrow \pi & & \downarrow \pi \\
D_{\pi^{i_s - 1}} \oplus \ldots \oplus D_{\pi^{i_h - 1}} & \xrightarrow{\varphi} & D_{\pi^{j_t - 1}} \oplus \ldots \oplus D_{\pi^{j_k - 1}} \\
\downarrow & & \downarrow \\
0 & & 0
\end{array}$$

Dicho diagrama es conmutativo. En efecto, verifiquémoslo por rastreo

$$\begin{array}{ccc}
x & \longrightarrow & \varphi(x) \\
\downarrow & & \downarrow \\
\pi \cdot x \to \varphi(\pi \cdot x) & = & \pi \cdot \varphi(x),
\end{array}$$

además las columnas son exactas y las filas son isomorfismos. La fila superior implica, según la primera parte de la demostración, que $h = k$. La fila inferior implica, en virtud de la hipótesis inductiva, que

$$\begin{aligned}
h - (s - 1) &= \text{número de sumandos en } D_{\pi^{i_s - 1}} \oplus \ldots \oplus D_{\pi^{i_h - 1}} = \\
&= \text{número de sumandos en } D_{\pi^{j_t - 1}} \oplus \ldots \oplus D_{\pi^{j_k - 1}} = \\
&= k - (t - 1)
\end{aligned}$$

y como $k = h$, se tiene que $s = t$. Además, la hipótesis inductiva implica que $i_s - 1 = j_t - 1 = j_s - 1$, con lo que $i_s = j_s$ y así

$$i_r = j_r \text{ para todo } r,\ s \leq r \leq h$$

Los índices r, tales que $1 \leq r < s$, corresponden a $i_r = 1$, y análogamente, $j_r = 1$.

En definitiva, hemos probado que el isomorfismo (1) implica inductivamente

$$k = h$$
$$i_1 = j_1, \ldots, i_h = j_h .$$

La validez del teorema en general es consecuencia del Principio de Inducción.

Definición 7.3.4. Sea A un D-módulo de torsión. Sea $\pi \in P$ un elemento extremal de D. Se dice que π es un *elemento extremal característico de* A, si $A_\pi \neq 0$. Sea A un D-módulo de torsión de tipo finito y sea C la totalidad de elementos extremales característicos de A. Para cada π, denotamos por

$$(i_1, \ldots, i_h)_\pi \; i_1 \leq \ldots \leq i_h$$

el invariante definido por

$$A_\pi = D_\pi{}^{i_1} \oplus \ldots \oplus D_\pi{}^{i_h} .$$

La totalidad de símbolos

$$\{(a_1, \ldots, a_h)_\pi / a_1 \leq \ldots \leq a_h\}_{\pi \in C}$$

se denominan los *divisores elementales* de A.

Ejemplo. Sea $A = \mathbf{Z}_6 \oplus \mathbf{Z}_{10}$. Entonces los primos característicos son 2, 3 y 5. Puesto que $A = (\mathbf{Z}_2 \oplus \mathbf{Z}_2) \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5$ los divisores elementales son $(1, 1)_2$, $(1)_3$, $(1)_5$.

Nota. Si A es un módulo de torsión de tipo finito entonces A posee sólo un número finito de elementos extremales característicos. En efecto, $A = \sum_{\pi \in P}^{\oplus} A_\pi$, y por lo tanto, si esta suma directa posee infinitos sumandos $\neq 0$, A no puede ser de tipo finito.

Ejemplo. Sea A un grupo abeliano finito de orden n. Por el teorema de Lagrange (véase Estructuras Algebraicas, parte I, pág. 77), todo elemento a de A tiene un orden que es divisor de n. Se sigue que los primos característicos de A son exactamente los divisores primos de n. Sea p primo con $n = p^d \cdot m$, $(m, p) = 1$, $1 < d$. Entonces la componente p-primaria A_p de A posee orden p^d y es expresable en la forma

$$A_p = Z_p{}^{i_1} \oplus \ldots \oplus Z_p{}^{i_h}$$

con

$$i_1 + \ldots + i_h = d .$$

Por lo tanto, las estructuras posibles de A_p corresponden biyectivamente con las posibles particiones

$$d = i_1 + \ldots + i_h, \quad i_1 \leq \ldots \leq i_h .$$

Si con $p(m)$ indicamos el número de particiones

$$m = m_1 + \ldots + m_k, \quad m_1 \leq \ldots \leq m_k$$

y si $n = p_1^{n_1} \ldots p_k^{n_k}$, p_i primos distintos, el número total de grupos abelianos de orden n (o más precisamente, el número de clases de isomorfismos de grupos abelianos de orden n) es el producto $p(n_1) \ldots p(n_k)$.

Ejemplo 1. Clasifiquemos los grupos abelianos de orden 60. Puesto que $60 = 2^2 \cdot 3 \cdot 5$, hay $p(2) \cdot p(1) \cdot p(1) = 2$ grupos abelianos de orden 60, los cuales son $\mathbf{Z}_{60}$ (cíclico) y $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{15}$ (no cíclico). Nótese que $\mathbf{Z}_{60} = \mathbf{Z}_4 \oplus \mathbf{Z}_{15}$.)

Ejemplo 2. Clasifiquemos los grupos abelianos de orden $8 = 2^3$. En este caso hay $p(3) = 3$ grupos abelianos de orden 8. Ellos son

$$\mathbf{Z}_8 \text{ (cíclico)}, \quad \mathbf{Z}_2 \oplus \mathbf{Z}_4 \quad \text{y} \quad \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2.$$

Los divisores elementales son $(3)_2$, $(1, 2)_2$ y $(1, 1, 1)_2$ respectivamente.

Ejemplo 3. Veamos en la figura 3 como se generan los grupos de orden $2^2 \cdot 3 \cdot 7^3$.

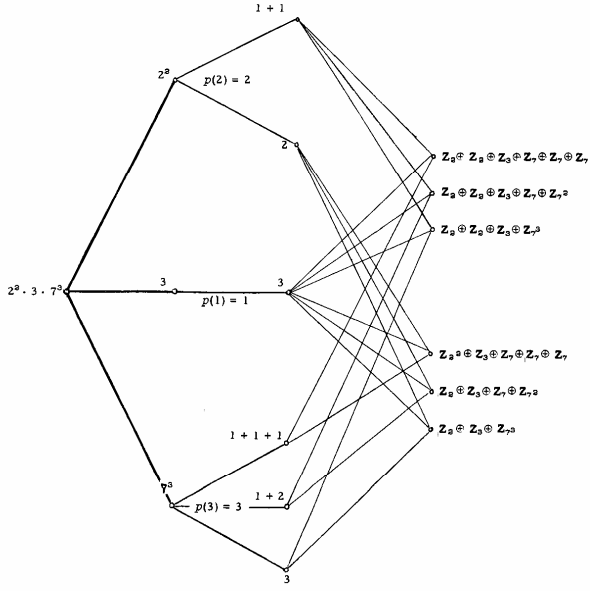


Fig. 3

4. FACTORES INVARIANTES

En esta sección se dará una variación del teorema de estructura de módulos de tipo finito sobre un dominio principal mediante la intro-

ducción de los *factores invariantes* del módulo, que se definen a continuación.

Sea A un módulo de torsión de tipo finito sobre un dominio principal D. Sean

$$
\begin{array}{ll}
(a_{11},\ldots,a_{1j},\ldots,a_{1m})\pi_1 & a_{11} \geq \ldots \geq a_{1j} \ldots \geq a_{1m} \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
(a_{i1},\ldots,a_{ij},\ldots,a_{im})\pi_i & a_{i1} \geq \ldots \geq a_{ij} \ldots \geq a_{im} \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
(a_{n1},\ldots,a_{nj},\ldots,a_{nm})\pi_n & a_{n1} \geq \ldots \geq a_{nj} \ldots \geq a_{nm}
\end{array} \tag{1}
$$

los divisores elementales escritos en orden *decreciente*, y además para simplificar la notación, se ha uniformado el número de los términos de cada sucesión agregando ceros hasta completar m de ellos. Por ejemplo si $A = \mathbf{Z}_2 \oplus \mathbf{Z}_{22} \oplus \mathbf{Z}_{32} \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_{52}$ se escribe

$$(2, 1, 0)_2$$
$$(2, 0, 0)_3$$
$$(2, 1, 1)_5$$

Definición 7.4.1. Se llama j-simo *factor invariante* de A al elemento α_j de A

$$\alpha_j = \prod_{i=1}^{n} \pi_i^{a_{ij}}$$

o sea al producto de los divisores elementales correspondientes a la columna j de (1).

Propiedad 7.4.2. $i \leq j \Rightarrow \alpha_j/\alpha_i$.

En el ejemplo que precede a la definición 7.4.1 los factores invariantes son

$$\alpha_1 = 2^2 \cdot 3^2 \cdot 5^2, \quad \alpha_2 = 2 \cdot 5, \quad \alpha_3 = 5.$$

Adviértase que es posible escribir también

$$A = \mathbf{Z}_{a_1} \oplus \mathbf{Z}_{a_2} \oplus \mathbf{Z}_{a_3}.$$

Obsérvese que cada módulo del tipo que estamos considerando determina un solo esquema (1). Recíprocamente, cada esquema (1) determina un único módulo, cuyos divisores elementales son $\pi_i^{a_{ij}}$.

Por lo tanto, fijados n elementos extremales distintos

$$\pi_1, \ldots, \pi_n$$

el número total de (clases de isomorfismos de) módulos de torsión de tipo finito con elementos extremales característicos en $\{\pi_1, \ldots, \pi_n\}$ está en correspondencia biyectiva con la totalidad $E_{n,\infty}$ de matrices

$$\begin{Vmatrix} a_{11} & \dots & a_{1m} \\ \cdot & \dots & \cdot \\ a_{n1} & \dots & a_{nm} \end{Vmatrix}$$

con coeficientes enteros no negativos, tales que

$$a_{1m} \leq \dots \leq a_{11}$$

$$\cdot \quad \dots \quad \cdot$$

$$a_{nm} \leq \dots \leq a_{n1}$$

y algún $a_{1m} \neq 0$.

Teorema 7.4.3. Sea A un módulo de torsión de tipo finito sobre un dominio principal D. Existen entonces elementos $\alpha_j \in D$ tales que

1) $$i \leq j \Rightarrow \alpha_j / \alpha_i$$

2) $$A = D_{\alpha_1} \oplus \dots \oplus D_{\alpha_m}$$

A está unívocamente determinado, salvo isomorfismos, por la sucesión $\alpha_1, \dots, \alpha_m$ con las propiedades 1) y 2).

Demostración. Tomaremos como α_j los factores invariantes que definimos en 7.4.1. La verificación de la propiedad 1) es automática a partir de 7.4.2. Ahora bien, cada D_{α_j} no es otra cosa que

$$D_{\pi_1^{a_{1j}}} \oplus \dots \oplus D_{\pi_n^{a_{nj}}}$$

o sea que 2) resulta de la representación de A en suma directa $\sum_{\oplus} D_{\pi_i^{a_{ij}}}$ correspondiente a sus divisores elementales, reordenando los sumandos según se hizo al definir los factores invariantes. La unicidad de los divisores elementales de A determina la unicidad de los factores invariantes. En efecto, factorizando cada α_j en producto $\alpha_j = \prod_{i=1}^{n} \pi_i^{a_{ij}}$ se obtiene un esquema del tipo (1) el cual está unívocamente determinado por los divisores elementales.

Nota. El teorema 7.4.3 asegura que los α_j son, en efecto, un conjunto de invariantes para cada módulo.

Ejemplo 1. Factores invariantes de $\mathbf{Z}_2 \oplus \mathbf{Z}_2 : \alpha_1 = 2$, $\alpha_2 = 2$.

Ejemplo 2. Factores invariantes de $\mathbf{Z}_2 \oplus \mathbf{Z}_3 : \alpha_1 = 6$

Ejemplo 3. Factores invariantes de $\mathbf{Z}_{15} \oplus \mathbf{Z}_{20} : \alpha_1 = 60$, $\alpha_2 = 5$, y podemos escribir

$$\mathbf{Z}_{15} \oplus \mathbf{Z}_{20} = \mathbf{Z}_{60} \oplus \mathbf{Z}_5$$

Ejemplo 4. Factores invariantes de $\mathbf{Z}_{112} \oplus \mathbf{Z}_{336} \oplus \mathbf{Z}_{1680} : \alpha_1 = 1680$, $\alpha_2 = 336$, $\alpha_3 = 112$, pues 112/336 y 336/1680.

5. MÓDULOS DADOS POR GENERADORES Y RELACIONES

Sea A un módulo de tipo finito sobre un dominio principal D. Si $\{a_1, \ldots, a_n\}$ es un conjunto de generadores de A, existe un módulo libre F con una base $\{e_1, \ldots, e_n\}$ y un epimorfismo $\rho : F \to A$, tal que $\rho(e_i) = a_i$, $i = 1, \ldots, n$. Sea H el núcleo del morfismo ρ. Se tiene entonces un isomorfismo $F/H \simeq A$. Ahora, siendo F de tipo finito, es noetheriano, por lo tanto H es de tipo finito. Sean $h_1, \ldots, h_d$ generadores de H. Podemos escribir

$$\begin{aligned} h_1 &= r_{11} \cdot e_1 + \ldots + r_{1n} \cdot e_n \\ &\cdot \quad\quad \cdot \quad\quad \ldots \quad\quad \cdot \\ h_d &= r_{d1} \cdot e_1 + \ldots + r_{dn} \cdot e_n \end{aligned} \tag{1}$$

con los $r_{ij} \in D$.

Al pasar de F a A por el morfismo ρ, las relaciones (1) se convierten en

$$\begin{aligned} 0 &= r_{11} \cdot a_1 + \ldots + r_{1n} \cdot a_n \\ &\cdot \quad\quad \cdot \quad\quad \ldots \quad\quad \cdot \\ 0 &= r_{d1} \cdot a_1 + \ldots + r_{dn} \cdot a_n . \end{aligned} \tag{2}$$

Por lo tanto, podemos describir A como el módulo generado por

$$a_1, \ldots, a_n$$

sometido a las relaciones (2).

Recíprocamente, dado un conjunto $\{a_1, \ldots, a_n\}$ de elementos y las relaciones formales (2), existe un módulo A, tal que los $a_1, \ldots, a_n$ constituyen un sistema de generadores y los mismos satisfacen las relaciones (2). En efecto, basta formar el cociente de un módulo libre F de base $e_1, \ldots, e_n$ por el subgrupo generado por los elementos (1).

Por ejemplo, el grupo abeliano Z_n puede considerarse como un grupo abeliano con un generador $\underline{a}$ sometido a la relación $n \cdot \underline{a} = 0$. Puesto que todo módulo es imagen de un módulo libre, es claro que todo módulo se puede describir por generadores y relaciones. En general y por abuso de lenguaje, si $A \simeq F/H$, con F libre, decimos que H es el submódulo de relaciones de A. Un problema equivalente al de determinar la estructura de los módulos sobre un anillo es, pues, el determinar los submódulos de un módulo libre, o, como suele decirse, el determinar la "posición" de un submódulo en un módulo libre. En general, éste es un problema difícil, pero en el caso de un dominio principal D y D-módulos de tipo finito, se conoce completamente su solución (véase el lema 7.5.2).

Demos otros ejemplos a fin de fijar las ideas

Ejemplo 1. $\mathbf{Z}_2 \oplus \mathbf{Z}_3$ es un grupo abeliano con dos generadores u, v, tales que $2 \cdot u = 3 \cdot v = 0$. En términos de grupos cocientes corresponde a la sucesión exacta

$$0 \to \mathbf{Z}(2,0) + \mathbf{Z} \cdot (0,3) \to \mathbf{Z} \oplus \mathbf{Z} \to \mathbf{Z}_2 \oplus \mathbf{Z}_3 \to 0.$$

Ejemplo 2. ¿Cuál será el grupo abeliano con dos generadores e_1 y e_2, tales que $2 \cdot e_1 + 3 \cdot e_2 = 0$? Se trata de hallar el grupo cociente del grupo libre L con dos generadores e_1, e_2 por el subgrupo generado por $2 \cdot e_1 + 3 \cdot e_2$. Es fácil ver que $2 \cdot e_1 + 3 \cdot e_2$ se extiende a una base $\{2 \cdot e_1 + 3 \cdot e_2, f\}$ de L, por lo tanto $L = \langle 2 \cdot e_1 + 3 \cdot e_2 \rangle \oplus \langle f \rangle$, y consecuentemente $L/\langle 2 \cdot e_1 + 3 \cdot e_2 \rangle \simeq \langle f \rangle \simeq \mathbf{Z}$. Por lo tanto, el grupo abeliano con dos generadores e_1, e_2 sometidos a la relación $2 \cdot e_1 + 3 \cdot e_2 = 0$ es isomorfo a $\mathbf{Z}$.

Ejemplo 3. ¿Cuál será el grupo abeliano con dos generadores e_1, e_2, tales que $2 \cdot e_1 + 2 \cdot e_2 = 0$ y $3 \cdot e_1 = e_2$? Sean

$$(1) \qquad \begin{aligned} f_1 &= 3 \cdot e_1 - e_2 \\ f_2 &= 2 \cdot e_1 + 2 \cdot e_2 \end{aligned}$$

f_1, f_2 generan en el grupo abeliano libre $\mathbf{Z} \cdot e_1 + \mathbf{Z} \cdot e_2$ el subgrupo de relaciones del grupo dado.

Podemos transformar el sistema (1) en otros equivalentes operando sobre las filas. Se obtienen

$$\begin{aligned} f_1' &= f_1 + f_2 = 5 \cdot e_1 + e_2 \\ f_2' &= f_2 = 2 \cdot e_1 + 2 \cdot e_2 \end{aligned}$$

$$(2) \qquad \begin{aligned} f_1'' &= f_1 + f_2 = 5 \cdot e_1 + e_2 = 1 \cdot (5 \cdot e_1 + e_2) + 0 \cdot (-e_1) \\ f_2'' &= -2 \cdot f_1 - f_2 = -8 \cdot e_1 = 0 \cdot (5 \cdot e_1 + e_2) + 8 \cdot (-e_1). \end{aligned}$$

Nota. La equivalencia significa que el carácter de "generadores" no se pierde; en efecto, f_1', f_2' y f_1'', f_2'' generan el mismo subgrupo que f_1 y f_2. Nótese, además, que $e_1' = 5 \cdot e_1 + e_2$, $e_2' = -e_1$ es base de $\mathbf{Z} \cdot e_1 \oplus \mathbf{Z} \cdot e_2$. Se sigue de (2) que

$$\frac{\mathbf{Z} \cdot e_1 \oplus \mathbf{Z} \cdot e_2}{\langle f_1, f_2 \rangle} = \frac{\mathbf{Z} \cdot e_1' \oplus \mathbf{Z} \cdot e_2'}{\langle f_1'', f_2'' \rangle} = \frac{\mathbf{Z} \cdot e_1' \oplus \mathbf{Z} \cdot e_2'}{\mathbf{Z} \cdot e_1' \oplus \mathbf{Z} \cdot (8 \cdot e_2')} \simeq$$

$$\simeq \mathbf{Z}_8$$

$\mathbf{Z}_8$ es, pues, el grupo que satisface las condiciones del problema.

Nota. Si el lector observa el ejemplo anterior notará que lo que se ha hecho es "diagonalizar" la matriz

$$\begin{Vmatrix} 3 & -1 \\ 2 & 2 \end{Vmatrix} \quad \text{asociada a (1)}$$

efectuando "ciertas operaciones" sobre (1) cuidando de no alterar el carácter de "ser conjunto de generadores". Esa idea desarrollada con toda generalidad permitirá determinar la estructura de módulos de tipo finito, dados por relaciones y a la vez calcular sus factores invariantes.

Antes de entrar a calcular los factores invariantes se introducirá una estructura especial, que puede definirse sin mayores restricciones sobre el anillo. Sea, pues, R un anillo con identidad y sea A un R-módulo a la izquierda. Sea $n \in \mathbf{N}$ y $\mathbf{M}_n(R)$ el anillo completo de matrices de n filas por n columnas con coeficientes en R. Definiremos sobre

$$A^n = A \oplus \ldots \oplus A \qquad (n \text{ copias})$$

una estructura de $\mathbf{M}_n(R)$-módulo a la izquierda como sigue. Primeramente convendremos en escribir los elementos

$$\underline{a} = (a_1, \ldots, a_n) \in A^n$$

en columna (vector columna)

$$\underline{a} = \begin{vmatrix} a_1 \\ \cdot \\ \cdot \\ a_n \end{vmatrix}$$

Si $\alpha = ((\alpha_{ij})) \in \mathbf{M}_n(R)$ y $\underline{a} \in A^n$ definimos

$$\alpha \cdot \underline{a} = \begin{vmatrix} \sum_{j=1}^{n} \alpha_{1j} \cdot a_j \\ \sum_{j=1}^{n} \alpha_{nj} \cdot a_j \end{vmatrix}$$

110

Por ejemplo, si $n = 2$

$$\begin{Vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{Vmatrix} \cdot \begin{vmatrix} a_1 \\ a_2 \end{vmatrix} = \begin{vmatrix} \alpha_{11} \cdot a_1 + \alpha_{12} \cdot a_2 \\ \alpha_{21} \cdot a_1 + \alpha_{22} \cdot a_2 \end{vmatrix}.$$

No ofrece ninguna dificultad conceptual probar que en esas condiciones queda definida sobre A^n una estructura de $\mathbf{M}_n(R)$-módulo a la izquierda. Dejamos a cargo del lector esta verificación computacional. Para el lector familiarizado con el álgebra lineal no será otra cosa que una revisión de las propiedades elementales de operaciones con matrices. Digamos también que si quisiéramos definir una estructura de $\mathbf{M}_n(R)$-módulo a la derecha tendríamos que partir de un R-módulo a la derecha A y definir un producto a la derecha de matrices, escribiendo los elementos de A^n como vectores fila.

Sea L un módulo (a la izquierda sobre R) libre de tipo finito, y sea $\{e_1, \ldots, e_n\}$ una base de L. Sea $\alpha \in \mathbf{M}_n(R)$. Entonces

Proposición 7.5.1. $\quad \{f_i = \sum_{j=1}^{n} \alpha_{ij} \cdot e_j\}, \ i = 1, \ldots, n$

es base de L si, y sólo si, α es inversible en $\mathbf{M}_n(R)$.

Demostración. Sea $\{f_i\}$, $i = 1, \ldots, n$ base de A. Existe entonces una matriz $((\beta_{ij})) \in \mathbf{M}_n(R)$ tal que

$$(1) \qquad ((\beta_{ij})) \cdot \begin{vmatrix} f_1 \\ . \\ . \\ f_n \end{vmatrix} = \begin{vmatrix} e_1 \\ . \\ . \\ e_n \end{vmatrix}$$

Multiplicando a la izquierda por $((\alpha_{ij}))$, se obtiene (justifique!)

$$((\alpha_{ij})) \cdot ((\beta_{ij})) = I_n$$

(donde I_n denota la matriz identidad de $\mathbf{M}_n(R)$).

Invirtiendo los papeles de $\{f_i\}$ y $\{e_i\}$ se obtiene, análogamente,

$$((\beta_{ij})) \cdot ((\alpha_{ij})) = I_n$$

lo cual demuestra que $((\alpha_{ij}))$ es inversible.

Recíprocamente, si $((\alpha_{ij}))$ es inversible

$$\begin{vmatrix} e_1 \\ . \\ . \\ e_n \end{vmatrix} = ((\alpha_{ij}))^{-1} \cdot (((\alpha_{ij}))) \cdot \begin{vmatrix} e_1 \\ . \\ . \\ e_n \end{vmatrix}) = ((\alpha_{ij}))^{-1} \cdot \begin{vmatrix} f_1 \\ . \\ . \\ f_n \end{vmatrix}$$

lo cual expresa que los e_i son combinaciones lineales de los f_j. Con esto podemos afirmar que los f_i generan L. Veamos la independencia lineal de los f_i. Sean $k_1, \ldots, k_n \in R$ tales que $\sum_{i=1}^{n} k_i \cdot f_i = 0$. Dicha relación se puede escribir en forma matricial como sigue

$$0 = \begin{Vmatrix} k_1 & \ldots & k_n \\ . & \ldots & . \\ k_1 & \ldots & k_n \end{Vmatrix} \cdot \begin{vmatrix} f_1 \\ . \\ f_n \end{vmatrix} = \begin{Vmatrix} k_1 & \ldots & k_n \\ . & \ldots & . \\ k_1 & \ldots & k_n \end{Vmatrix} \cdot ((\alpha_{ij})) \cdot \begin{vmatrix} e_1 \\ . \\ e_n \end{vmatrix}$$

y siendo $\{e_i\}$ base de L, resulta

$$\begin{Vmatrix} k_1 & \ldots & k_n \\ . & \ldots & . \\ k_1 & \ldots & k_n \end{Vmatrix} \quad ((\alpha_{ij})) = 0$$

y además $((\alpha_{ij}))$ inversible, resulta inmediatamente que

$$k_1 = \ldots = k_n = 0$$

lo cual prueba la independencia lineal de los f_i. La proposición queda probada.

Nota. Observe el lector que al probarse la independencia de los f_i se ha utilizado, en la primera parte de la demostración, que $((\alpha_{ij}))$ era inversible a la izquierda, y en la segunda, que era inversible a la derecha.

Estamos en condiciones ahora de probar el toerema fundamental de de estructura de módulos de tipo finito sobre un dominio principal. Utilizamos el resultado 6.3.7, que afirma que si $((\alpha_{ij})) \in \mathbf{M}_n(D)$, existen entonces matrices $\nu, \tau \in \mathbf{M}_n(D)$, tales que

$$\nu \cdot ((\alpha_{ij})) \cdot \tau = ((d_i))$$

donde $((d_i))$ es la matriz diagonal con coeficientes d_i, tales que

$$i \leq j, d_i \neq 0 \Rightarrow d_i / d_j .$$

Lema 7.5.2. Sea L un módulo libre de tipo finito sobre un dominio principal D. Sea H submódulo de L. Existen entonces una base $e_1, \ldots, e_n$ de L,

$$d_1, \ldots, d_n \in D, \text{ con } d_i / d_j \text{ si } i \leq j$$

tales que

$$d_1 \cdot e_1, \ldots, d_n \cdot e_n$$

forman un sistema de generadores de H.

Demostración. Siendo D noetheriano y L de tipo finito, H admite un sistema de generadores $f_1, \ldots, f_h$, por lo tanto existe una matriz $((\alpha'_{ij}))$ de h filas y n columnas con coeficientes en D, tal que

$$(1) \qquad \begin{aligned} f_1 &= \alpha'_{11} \cdot e_1 + \ldots + \alpha'_{1n} \cdot e_n \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_h &= \alpha'_{h1} \cdot e_1 + \ldots + \alpha'_{hn} \cdot e_n . \end{aligned}$$

En L^n, dotado de la estructura ya definida de $\mathbf{M}_n(D)$-módulo, la situación (1) puede describirse de la manera siguiente

$$(2) \qquad \begin{vmatrix} f_1 \\ \cdot \\ \cdot \\ f_h \\ 0 \\ \cdot \\ \cdot \\ 0 \end{vmatrix} = \begin{Vmatrix} \alpha'_{11} & \cdots & \alpha'_{1n} \\ & & \\ & & \\ \alpha'_{h1} & \cdots & \alpha'_{hn} \\ 0 & \ldots & 0 \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ 0 & \ldots & 0 \end{Vmatrix} \cdot \begin{vmatrix} e_1 \\ \cdot \\ \cdot \\ e_h \\ e_{h+1} \\ \cdot \\ \cdot \\ e_n \end{vmatrix} .$$

Sea $((\alpha_{ij}))$ la matriz primitiva $((\alpha'_{ij}))$ completada con $n-h$ filas de ceros. Existen entonces matrices $\nu, \tau \in \mathbf{M}_n(D)$ inversibles, tales que

$$\nu \cdot ((\alpha_{ij})) \cdot \tau = ((d_i))$$

donde $((d_i))$ es una matriz diagonal con las propiedades de divisibilidad

$$i \leq j, d_i \neq 0 \Rightarrow d_i / d_j$$

(2) puede escribirse en la forma

$$\nu \cdot \begin{vmatrix} f_1 \\ \cdot \\ \cdot \\ f_h \\ 0 \\ \cdot \\ \cdot \\ 0 \end{vmatrix} = \nu \cdot ((\alpha_{ij})) \cdot \tau \cdot (\tau^{-1} \cdot \begin{vmatrix} e_1 \\ \cdot \\ \cdot \\ e_h \\ e_{h+1} \\ \cdot \\ \cdot \\ e_n \end{vmatrix})$$

y luego de operar resulta

$$\begin{vmatrix} f'_1 \\ \cdot \\ \cdot \\ f'_h \\ f'_{h+1} \\ \cdot \\ \cdot \\ f'_n \end{vmatrix} = ((d_i)) \cdot \begin{vmatrix} e'_1 \\ \cdot \\ \cdot \\ e'_h \\ e'_{h+1} \\ \cdot \\ \cdot \\ e'_n \end{vmatrix}$$

y es claro que entonces $f'_i = d_i \cdot e'_i$, $i = 1, \ldots, n$.

El hecho de ser ν y τ matrices inversibles en $\mathbf{M}_n(D)$ implica que $f'_1, \ldots, f'_h$ es un sistema de generadores de H, y $e'_1, \ldots, e'_n$ es una base de L. El lema queda probado. 113

Teorema 7.5.3. Sea A un módulo de tipo finito sobre un dominio principal D. Existen entonces elementos

$$d_1, \ldots, d_h \text{ en } D$$

tales que

$$d_i \neq 0, i \leq j \Rightarrow d_i / d_j$$

y

$$A \simeq D_{d_1} \oplus \ldots \oplus D_{d_h}$$

(donde, eventualmente, $d_i = 0$, con lo que $D_d = D$.)

Demostración. Sea L un módulo libre de tipo finito, y $\rho : L \to A$ un epimorfismo. Sea $H = Nu(\rho) \neq 0$. Sea $e_1, \ldots, e_n$ una base de L, y sean $d_i \in D$ elementos con las propiedades descritas en 7.5.2. Entonces $d_1 \cdot e_1, \ldots, d_n \cdot e_n$ forman un sistema de generadores de H. Por lo tanto (!) existe $h \in \mathbf{N}$ tal que

$$d_1 \cdot e_1, \ldots, d_h \cdot e_h$$

es una base de H. Se tiene

$$A \simeq \frac{L}{H} = \frac{\langle e_1 \rangle \oplus \ldots \oplus \langle e_h \rangle \oplus \langle e_{h+1} \rangle \oplus \ldots \oplus \langle e_n \rangle}{\langle d_1 e_1 \rangle \oplus \ldots \oplus \langle d_h e_h \rangle \oplus 0 \oplus \ldots \oplus 0} \simeq$$

$$\simeq D_{d_1} \oplus \ldots \oplus D_{d_h} \oplus D \oplus \ldots \oplus D$$

Escribiendo

$$d_1, \ldots, d_h, \ 0, \ldots, 0$$

se obtienen los elementos pedidos.

Nótese que el teorema 7.5.3 da, simultáneamente, la descomposición de A en suma directa $tA \oplus F$ del submódulo de torsión y un submódulo libre. tA corresponde a los factores $d_i \neq 0$ y F a los factores $d_i = 0$.

La unicidad de los factores invariantes se probó en 7.4.3 por lo que no es necesario repetirla aquí. Lo importante del tratamiento presentado en esta sección es que el cálculo de los factores invariantes, se puede realizar en forma efectiva llevando a la forma diagonal, por equivalencia (véase 6.3.7), a la matriz $((\alpha_{ij}))$ (ampliada convenientemente con ceros), tal que

$$\begin{aligned} f_1 &= \alpha_{11} \cdot e_1 + \ldots + \alpha_{1n} \cdot e_n \\ &\cdot \quad \cdot \quad \cdot \quad \ldots \quad \cdot \quad \cdot \\ f_h &= \alpha_{h1} \cdot e \ + \ldots + \alpha_{hn} \cdot e_n . \end{aligned}$$

$\{e_1, \ldots, e_n\}$ es una base de un módulo libre F, y $\{f_1, \ldots, f_h\}$ un sistema de generadores del submódulo de relaciones H, del módulo A, tal que $A \simeq F/H$.

Ejemplo. Sea A el grupo abeliano dado por generadores e_1, e_2, e_3
114 sometido a las relaciones $2e_1 - 6 \cdot e_3 = 12 \cdot e_1 + 6 \cdot e_2 - 36 \cdot e_3 = 0$. Se trata de hallar los factores invariantes de A. Procederemos en forma general estudiando el módulo libre generado por e_1, e_2, e_3 y el submódulo generado por $f_1 = 2 \cdot e_1 - 6 \cdot e_3$, $f_2 = 12 \cdot e_1 - 6 \cdot e_2 - 36 \cdot e_3$. Utilizando el esquema de matrices se tiene

$$(1) \qquad \begin{vmatrix} f_1 \\ f_2 \\ 0 \end{vmatrix} = \begin{Vmatrix} 2 & 0 & -6 \\ 12 & 6 & -36 \\ 0 & 0 & 0 \end{Vmatrix} \cdot \begin{vmatrix} e_1 \\ e_2 \\ e_3 \end{vmatrix}$$

El problema es diagonalizar la matriz

$$\begin{Vmatrix} 2 & 0 & -6 \\ 12 & 6 & -36 \\ 0 & 0 & 0 \end{Vmatrix}$$

Se irá operando no sólo con esta matriz, sino también con los generadores $\{f_i\}$ y la base $\{e_i\}$, de manera de obtener la base a que se hace referencia en el lema 7.5.2.

Multiplicando a la izquierda de (1) por la matriz elemental

$$\begin{Vmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{Vmatrix}$$

se obtiene

$$\begin{vmatrix} f_1 \\ -5f_1 + f_2 \\ 0 \end{vmatrix} = \begin{Vmatrix} 2 & 0 & -6 \\ 2 & 6 & -6 \\ 0 & 0 & 0 \end{Vmatrix} \cdot \begin{vmatrix} e_1 \\ e_2 \\ e_3 \end{vmatrix} =$$

$$= \begin{Vmatrix} 2 & 0 & -6 \\ 2 & 6 & -6 \\ 0 & 0 & 0 \end{Vmatrix} \cdot \underbrace{\begin{Vmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{Vmatrix}}_{T} \cdot \underbrace{\begin{Vmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{Vmatrix}}_{T^{-1}} \cdot \begin{vmatrix} e_1 \\ e_2 \\ e_3 \end{vmatrix}$$

$$= \begin{Vmatrix} 2 & 0 & 0 \\ 2 & 6 & 0 \\ 0 & 0 & 0 \end{Vmatrix} \cdot \begin{vmatrix} e_1 - 3e_3 \\ e_2 \\ e_3 \end{vmatrix}$$

Multiplicando a la izquierda por

$$\begin{Vmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{Vmatrix}$$

resulta

$$\begin{vmatrix} f_1 \\ -6f_1 + f_2 \\ 0 \end{vmatrix} = \begin{Vmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{Vmatrix} \cdot \begin{vmatrix} e_1 - 3 \cdot e_3 \\ e_2 \\ e_3 \end{vmatrix}$$

La base pedida en 7.5.2 es

$$e_1 - 3 \cdot e_3, e_2, e_3$$

(siendo e_1, e_2, e_3 una base original arbitraria)

$$d_1 = 2, d_2 = 6, d_3 = 0$$

$$2 \cdot (e_1 - 3 \cdot e_3), 6 \cdot e_2$$

es el sistema de generadores de H asociado, y finalmente

$$A \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_6 \oplus \mathbf{Z}$$

EPÍLOGO AL CAPÍTULO 7

Reuniendo los resultados de las distintas secciones correspondientes a este capítulo podemos enunciar el siguiente teorema.

Teorema de Estructura. Sea D un dominio principal y sea A un D-módulo de tipo finito. Entonces

i) Si $A = A_\pi$ (la componente primaria de A), donde π es un elemento extremal, entonces

$$A = D/_{\langle \pi^{i_1} \rangle} \oplus \ldots \oplus D/_{\langle \pi^{i_h} \rangle}$$

donde los $i_1, \ldots, i_h$ son enteros positivos, tales que $i_1 \leq \ldots \leq i_h$. Además A está unívocamente determinado, salvo isomorfismos, por la sucesión

$$(i_1, \ldots, i_h).$$

ii) Si A es de torsión, existe entonces un conjunto finito $\pi_1, \ldots, \pi_n$ de elementos extremales de D, tales que

$$A = A_{\pi_1} \oplus \ldots \oplus A_{\pi_n}.$$

Además, A está unívocamente determinado, salvo isomorfismos, por los símbolos definidos para cada π en i)

$$(a_{11}, \ldots, a_{1m_1})_{\pi_1}$$
$$\cdot \quad \ldots \quad \cdot$$
$$(a_{n1}, \ldots, a_{nm_n})_{\pi_n}$$

que denominamos los *divisores elementales* de A.

iii) Si A es sin torsión, entonces A es libre y está determinado, salvo isomorfismos, por el número de elementos de cualquier base, es decir por el *rango* de A.

iv) Si A es arbitrario, existe un único subgrupo de A de torsión (el subgrupo de torsión) tA, tal que

$$A = tA \oplus L$$

donde L es libre de tipo finito.

A está determinado, salvo isomorfismos, por los invariantes determinados por tA y L, según ii) y iii).

ii*) Si A es de torsión, existe un conjunto finito de elementos no nulos

a) $$d_1, \ldots, d_m \text{ en } D$$

con la propiedad de divisibilidad

b) $$i \leq j \Rightarrow d_i / d_j$$

tales que

$$A = D/\langle d_1 \rangle \oplus \ldots \oplus D/\langle d_m \rangle .$$

Además, A está unívocamente determinado, salvo isomorfismos por a) y b). Los elementos a) que cumplen b) se denominan los *factores invariantes* de A.

iv*) Si A es arbitrario, existe un conjunto finito de elementos

a') $$d_1, \ldots, d_k \text{ en } D$$

con la propiedad de divisibilidad

b') $$d_i \neq 0,\ i \leq j \Rightarrow d_i / d_j$$

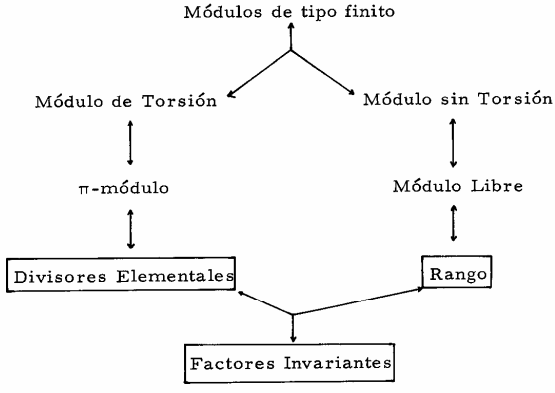
tales que

$$A = D/\langle d_1 \rangle \oplus \ldots \oplus D/\langle d_k \rangle .$$

Además, A está unívocamente determinado, salvo isomorfismos, por a') y b'). Los elementos a'), que cumplen b'), se denominan los *factores invariantes* de A.

Nota. Los factores invariantes, definidos en ii*) para módulos de torsión, se extienden en iv*) a módulos arbitrarios, agregando $d_i = 0$ en número igual al rango de A. Por ejemplo, los factores invariantes de $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z} \oplus \mathbf{Z}$ son 2, 4, 0, 0.

La teoría de módulos de tipo finito sobre un dominio principal se puede representar por el siguiente diagrama.



8

APLICACIONES A LA TEORÍA DE UNA TRANSFORMACIÓN LINEAL

1. INTRODUCCIÓN Y DEFINICIONES PREVIAS

Esta sección describe un ejemplo de naturaleza diferente a los considerados previamente. Constituye una verdadera aplicación de la teoría presentada en el capítulo anterior, al estudio de la "estructura" de una transformación lineal de un espacio vectorial en sí mismo (de dimensión finita). A fin de no extender demasiado esta monografía, nos vamos a limitar a mostrar hechos salientes y aconsejamos al lector complementar la exposición con el material que se cita en la bibliografía.

En lo que sigue K denota un cuerpo (conmutativo). Sea V un espacio vectorial sobre K y $\sigma : V \to V$ un endomorfismo de K-módulos. Por $\mathrm{End}_K(V)$ denotamos el K-módulo $\mathrm{Hom}_K(V, V)$ dotado de la estructura de anillo (el anillo de K-endomorfismos de V). Sea K[X] el anillo de polinomios en una indeterminada X con coeficientes en K. Sabemos que K[X] es un dominio euclidiano, y, por tanto, principal.

Proposición 8.1.1. Existe un único morfismo de anillos

$$\rho : K[X] \to \mathrm{End}_K(V)$$

tal que

$$\rho(1) = \mathrm{Id}$$

$$\rho(X) = \sigma .$$

Demostración. Todo elemento de K[X] se escribe *unívocamente* como una combinación lineal $a_0 + a_1 \cdot X + \ldots + a_n \cdot X^n$ de $1, X, \ldots, X^i, \ldots$, con coeficientes en K. O sea, todo elemento de K[X] está determinado unívocamente por los coeficientes a_i de X^i. Por lo tanto, el asignar a cada $a_0 + a_1 \cdot X + \ldots + a_n \cdot X^n$, el elemento de $\mathrm{End}_K(V)$ definido por

$$a_0 \cdot \mathrm{id} + a_1 \cdot \sigma + \ldots + a_n \cdot \sigma^n,$$

define una aplicación, que se denomina la especialización de X por σ y se denota por

$$P(X) \to P(\sigma)$$

donde P(X) denota un elemento típico de K[X].

Nótese que por la especialización, en particular,

$$1 \mapsto \mathrm{id}$$

$$X \mapsto \sigma .$$

Una verificación sencilla muestra que la especialización es un morfismo de anillos, o sea

$$P(X) + T(X) \mapsto P(\sigma) + T(\sigma)$$

$$P(X) \cdot T(X) \mapsto P(\sigma) \cdot T(\sigma).$$

Además, siendo 1 y X un sistema de generadores de $K[X]$, *como anillo*, todo morfismo de anillos de $K[X]$ en $\mathrm{End}_K(V)$ está unívocamente determinado por la imagen de X. La proposición 8. 1. 1 queda pues probada.

Por abuso de notación, se denota por $K[\sigma]$ el subanillo de $\mathrm{End}_K(V)$, imagen de $K[X]$ por ρ, y se denomina el anillo de expresiones polinomiales en σ. En virtud de 8. 1. 1 se tiene una representación de $K[X]$ en el anillo de endomorfismos de V (como espacio vectorial), pero

$$\mathrm{End}_K(V) \subset \mathrm{End}_Z(V)$$

en forma natural. Por lo tanto, se sigue de 8. 1. 1 que existe sobre V una estructura de $K[X]$-módulo, tal que (si $v \in V$)

$$1 \cdot v = v$$

$$X \cdot v = \sigma(v)$$

$$X \cdot (k \cdot v) = k \cdot (X \cdot v), \quad k \in K$$

$$X^2 v = \sigma(\sigma(v)) = \sigma^2(v) \text{ etc.}$$

Escribiremos

120

$$V_\sigma$$

para denotar esta estructura de $K[X]$-módulo.

Proposición 8.1.2. Sean $\sigma, \tau \in \mathrm{End}_K(V)$. Entonces $V_\sigma \simeq V_\tau$ (como $K[X]$-módulos) si, y sólo si, existe un isomorfismo $\theta : V \to V$ de K-espacio vectorial, tal que

$$\tau = \theta \cdot \sigma \cdot \theta^{-1}.$$

Demostración. Sea $\theta : V_\sigma \to V_\tau$ un isomorfismo (como $K[X]$-módulos). Entonces, para todo $v \in V$, es $\theta(X \cdot v) = X \cdot \theta(v)$, por ser θ un morfismo de $K[X]$-módulos. En otros términos

$$(\theta\sigma)(v) = \theta(\sigma(v)) = \theta(X \cdot v) = X \cdot \theta(v) = \tau(\theta(v)) = (\tau \cdot \theta)(v)$$

o sea, $\theta\sigma = \tau\theta$, y de ahí $\tau = \theta \cdot \sigma \cdot \theta^{-1}$.

Recíprocamente, dada la θ con la propiedad de la proposición, dicha propiedad no expresa otra cosa que θ *conmuta con* X, o sea $\theta(X \cdot v) = X \cdot \theta(v)$, cualquiera que sea $v \in V$.

Nota. Dos endomorfismos σ, τ, tales que existe un automorfismo θ de V, tal que $\tau = \theta \cdot \sigma \cdot \theta^{-1}$, se dicen *semejantes*. La semejanza es una relación de equivalencia en $\mathrm{End}_K(V)$. Por lo tanto, 8. 1. 2 dice que las clases de isomorfismos de $K[X]$-módulos sobre V corresponden biyectivamente a las clases de equivalencia por semejanza en $\mathrm{End}_K(V)$.

Estudiemos los submódulos de V_σ. Sea W un subespacio de V, entonces es claro que W es submódulo de V_σ si, y sólo si,

$$\forall\, w \in W,\quad X \cdot w \in W$$

o, equivalentemente, si, y sólo si, W es *estable* por σ: $\sigma(W) \subset W$.

Ejemplo 1. Sea $\sigma \in \mathrm{End}_K(V)$. Sea $v \in V$. Entonces el submódulo $\langle v \rangle$ de V_σ coincide con el subespacio de V generado por los vectores v, $\sigma(v)$, ..., $\sigma^i(v)$, ...

Ejemplo 2. Sea $\sigma \in \mathrm{End}_K(V)$. Se dice que $k \in K$ es *valor propio de* σ, si existe $0 \neq v$, tal que $\sigma(v) = k \cdot v$. v se dice *vector propio* de σ asociado a k.

Sea, para todo $k \in K$, $V_k = \{v / v \in V$, tal que existe $i \in N$ con $(\sigma - k \cdot \mathrm{id})^i (v) = (X - k \cdot 1)^i \cdot v = 0\}$. Valen entonces las siguientes afirmaciones, cuyas demostraciones se dejan como ejercicio para el lector: a) V_k es submódulo de V_σ. b) $V_k \neq 0$ si, y sólo si, k es valor propio de σ.

2') Sea $\sigma: Q^2 \to Q^2$, tal que $\sigma(1, 0) = (1, -1)$, $\sigma(0, 1) = (1, 1)$. Afirmamos que los únicos submódulos de $(Q^2)_\sigma$ son 0 y Q^2. En efecto, si existe un submódulo $W \neq 0$, Q^2, W es un subespacio de dimensión 1, $W = \langle w \rangle$, $0 \neq w$. Pero, entonces, w es vector propio de σ, $\sigma(w) = k \cdot w$, $k \in Q$. Sea $w = (a, b)$. Resulta

$$\sigma(a, b) = (k \cdot a,\ k \cdot b)$$

$$\sigma(a, b) = a \cdot (1, -1) + b \cdot (1, 1) = (a + b, b - a)$$

o sea

$$\begin{cases} k \cdot a = a + b, & 0 = (k - 1) \cdot a - b \\ k \cdot b = b - a, & 0 = a + (k - 1) \cdot b. \end{cases}$$

Siendo (a, b) una solución no trivial del sistema debe verificarse

$$0 = (k - 1)^2 + 1 = k^2 - 2k + 2$$

pero esto es un absurdo, pues la ecuación $X^2 - 2x + 2 = 0$ no admite ninguna solución racional.

2. POLINOMIO MINIMAL

Sea ahora V un espacio vectorial de *dimensión finita*. Sea $\sigma \in \mathrm{End}_K(V)$. La representación

$$\rho: K[X] \to \mathrm{End}_K(V)$$

con

$$\rho(1) = \mathrm{id}, \qquad \rho(X) = \sigma$$

no puede ser un monomorfismo por la razón siguiente. $\mathrm{End}_K(V)$ es un espacio vectorial de dimensión finita igual a $(\dim_K(V))^2$ (en efecto, si e_1, ..., e_n es una base de V, los endomorfismos f_{ij} de V, $i, j \in [\![1, n]\!]$,

tales que $f_{ij}(e_h) = 0$ si $i \neq h$, $f_{ij}(e_i) = e_j$, forman una base de $\mathrm{End}_K(V)$). Por otra parte, *cualquiera que sea* $m \in N$ el conjunto

$$1,\ X,\ X^2,\ \ldots,\ X^m$$

es linealmente independiente en $K[X]$. Como todo monomorfismo preserva independencia lineal, está claro que ρ no puede ser un monomorfismo. $\mathrm{Nu}(\rho)$ es un ideal no nulo de $K[X]$. Sea $m_\sigma(X)$ un generador de $\mathrm{Nu}(\rho)$, que sea además mónico.

Definición 8.2.1. El polinomio mónico $m_\sigma(X)$ se denomina el *polinomio minimal* de σ.

Proposición 8.2.2. Valen las siguientes propiedades

i) Para todo $v \in V$, $m(X) \cdot v = 0$

ii) V_σ es un $K[X]$-módulo de torsión

iii) Sea $p(X) \in K[X]$, tal que $p(X) \cdot v = 0$, cualquiera que sea $v \in V$, entonces $m_\sigma(X)$ divide a $p(X)$.

Demostración. 1) está claro, pues $m_\sigma(X) \cdot v = m_\sigma(\sigma)(v) = 0$, ya que $m_\sigma(\sigma) = 0$.

2) es consecuencia de 1).

3) $p(X) \in \mathrm{Nu}(\rho)$, por lo tanto $p(X)$ es múltiplo de $m_\sigma(X)$.

Ejemplo 1. Sea $k \in K$ y sea $h_k : V \to V$ la homotecia de razón k. Entonces $m_{h_k}(X) = X - k$.

Ejemplo 2. Sea $e_1, \ldots, e_n$ una base de V y sea $\sigma : V \to V$ definida por $\sigma(e_1) = e_{i+1}$, si $i < n$, y $\sigma(e_n) = 0$. Entonces $X^n = m_\sigma(X)$. En efecto, X^n anula σ, por lo tanto $m_\sigma(X)$ es divisor de X^n, por lo tanto de la forma X^j. Si $j < n$, $\sigma^j \neq 0$. Luego debe ser $m_\sigma(X) = X^n$.

Un endomorfismo con la propiedad $\sigma^n = 0$ para algún n se denomina *nilpotente*. Un automorfismo de la forma $I + \sigma$, con σ endomorfismo nilpotente, se denomina *unipotente*.

3. POLINOMIO CARACTERÍSTICO

Sea V un espacio vectorial de dimensión finita y sea $\sigma \in \mathrm{End}_K(V)$). Sea $e_1, \ldots, e_n$ una base de V. La matriz $((\alpha_{ij}))$ definida por

$$\sigma(e_i) = \sum_{j=1}^{n} \alpha_{ij} \cdot e_j$$

se denomina la matriz de σ respecto de la base (e_i). Se escribe

$$((\alpha_{ij})) = ((\sigma))_e.$$

Sea $f_1, \ldots, f_n$ otra base de V. Si $((\beta_{ij}))$ denota la matriz definida por

$$f_i = \sum_{j=1}^{n} \beta_{ij} \cdot e_j \qquad \textit{(matriz de pasaje)}$$

y si

$$((\sigma))_f = ((\gamma_{ij}))$$

se verifica

$$((\gamma_{ij})) = ((\beta_{ij}))\cdot((\alpha_{ij}))\cdot((\beta_{ij}))^{-1}.$$

Sea $M_n(K[X])$ el anillo completo de matrices de n filas por n columnas con coeficientes en $K[X]$.

Definición 8.3.1. Se denomina matriz característica de σ respecto de la base (e_i) a la matriz

$$X\cdot I_n - ((\alpha_{ij}))_e = \begin{Vmatrix} X-\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ -\alpha_{21} & X-\alpha_{22} & \cdots & -\alpha_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & X-\alpha_{nn} \end{Vmatrix}$$

Proposición 8.3.2. Sean e_i, f_i, $i = 1, \ldots, n$ bases de V. Entonces $\det(X\cdot I_n - ((\sigma))_e) = \det(X\cdot I_n - ((\sigma))_f)$ donde det denota el determinante.

Demostración. Sea $((\beta_{ij}))$ la matriz de pasaje de f a e. Se tiene

$$\begin{aligned} \det(X\cdot I_n - ((\sigma))_f) &= \det(X\cdot I_n - ((\beta_{ij}))\cdot((\sigma))_e\cdot((\beta_{ij}))^{-1}) \\ &= \det(\ ((\beta_{ij}))\cdot(X\cdot I_n)\cdot((\beta_{ij}))^{-1} - \\ &\quad - ((\beta_{ij}))\cdot((\sigma))_e\cdot(\beta_{ij}))^{-1}) \end{aligned}$$

puesto que $X\cdot I_n$ es una matriz escalar y conmuta con cualquier matriz de $M_n(K[X])$. Sacando factor común y utilizando la propiedad multiplicativa de det se tiene

(c) $\det(X\cdot I_n - ((\sigma))_f) = \det(X\cdot I_n - ((\sigma))_e)$

Definición 8.3.3. El polinomio

$$\chi_\sigma = \det(X\cdot I_n - ((\sigma))_e)$$

se denomina el *polinomio característico* de σ. Por la relación (c), χ_σ no depende de la base utilizada para representar matricialmente a σ.

Ejemplo. Sea V un espacio vectorial de dimensión n sobre el cuerpo K y sea $k \in K$. Entonces, el polinomio característico de la homotecia $h_k : V \to V$ de razón k es $(X-k)^n$.

4. MÓDULOS CÍCLICOS

Sea V un espacio vectorial de dimensión finita sobre K. Sea $\sigma \in \mathrm{End}_K(V)$. Sea $V_\sigma = \langle v \rangle$ un módulo cíclico. Se trata de ver en qué propiedad de σ se traduce el carácter de cíclico de V_σ.

Si v es generador de V_σ entonces el morfismo

$$\varphi : K[X] \to V_\sigma$$

tal que

$$\varphi : 1 \mapsto v$$

es un epimorfismo. Sea $\mathrm{Nu}(\varphi) = \langle p(X) \rangle$, con $p(X) = X^n + a_{n-1} X^{n-1} + \ldots + a_o$. Afirmamos que

$$(*) \qquad v,\ \sigma(v),\ \ldots,\ \sigma^{n-1}(v)$$

es una *base* de V (como K-espacio vectorial).

Puesto que $V_\sigma \simeq K[X]/\langle p(X) \rangle$ todo elemento de $K[X]/\langle p(X) \rangle$ se representa por un polinomio de grado $< n = \mathrm{gr}(p(X))$, de manera que

$$\underline{1},\ \underline{X},\ \ldots,\ \underline{X}^{n-1} \qquad \text{(clases módulo } p(X))$$

es una base de $K[X]/\langle p(X) \rangle$ como K-espacio vectorial. Por lo tanto

$$v,\ \sigma(v),\ \ldots,\ \sigma^{n-1}(v)$$

es una base de V como K-espacio vectorial.

Determinemos la matriz de σ respecto de la base (*). Ésta es

$$\begin{Vmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \ldots & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -a_o & -a_1 & -a_2 & \ldots & & -a_{n-1} \end{Vmatrix}$$

en efecto, $\sigma(v) = 0 \cdot v + 1 \cdot \sigma(v)$, $\sigma(\sigma(v)) = 0 \cdot v + 0 \cdot \sigma(v) + 1 \cdot (\sigma^2(v))$, $\ldots$, $\sigma(\sigma^{n-1}(v)) = \sigma^n(v) = (-a_o \cdot id - a_1 \cdot \sigma + \ldots + -a_{n-1} \sigma^{n-1})(v) = (-a_o) \cdot v - a_1 \cdot \sigma(v) + \ldots + (-a_{n-1}) \sigma^{n-1}(v)$.

Proposición 8.4.1. $\chi_\sigma = p(X) = m_\sigma$.

Demostración. Basta desarrollar el determinante por los elementos de la última fila. Para fijar las ideas conviene referirse a un ejemplo particular de 4×4.)

Definición 8.4.2. Sea $t(X) = X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_o \in K[X]$. Se denomina *matriz compañera* de $t(X)$ a la matriz en $M_n(K)$

$$\begin{Vmatrix} 0 & 1 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \cdot & \cdot & \ldots & \cdot \\ 0 & 0 & \ldots & 1 \\ -a_o & -a_1 & \ldots & -a_{n-1} \end{Vmatrix}$$

Entonces, si σ es un endomorfismo tal que, respecto de alguna base, su matriz es la matriz compañera de un polinomio $t(X)$, se verifica que su polinomio característico es precisamente $t(X)$. Recíprocamente, dado un polinomio $t(X)$, existe un endomorfismo cuya matriz respecto de alguna base es la matriz compañera de $t(X)$. Analicemos el caso de un módulo cíclico con

$$p(X) = \pi^m, \qquad \pi \text{ irreducible en } K[X]$$

$$\pi = X^s + a_{s-1}X^{s-1} + \ldots + a_1 X + a_o.$$

Sea v generador de V_σ. Se trata de hallar una base de V conveniente. Formemos el conjunto de generadores

$$v,\ \sigma(v),\ \sigma^2(v),\ \ldots,\ \sigma^{h-1}(v). \qquad h = gr(p(X))$$

que es, en realidad, una base por razones de dimensión. Pero ella no es conveniente, pues no considera el polinomio π. Seleccionemos los elementos $\sigma^i(v)$ con mayor cuidado.

(') $$v,\ \sigma(v),\ \ldots,\ \sigma^{s-1}(v)$$

son linealmente independientes. Como

$$\pi = X^s + a_{s-1}\cdot X^{s-1} + \ldots + a_1 \cdot X + a_o$$

(") $$\sigma^s(v) = \pi \cdot v - a_{s-1}\cdot \sigma^{s-1}(v) - \ldots - a_o \cdot v.$$

Por lo tanto, seguimos la sucesión (') con

$$\pi \cdot v,\ \sigma\pi \cdot v,\ \ldots,\ \sigma^{s-1}\pi v$$

y, utilizando ("), continuamos con

$$\pi^2 \cdot v,\ \sigma \cdot \pi^2 v,\ \ldots,\ \sigma^{s-1}\,\pi^2 \cdot v$$

$$\cdot \qquad \cdot \qquad \ldots$$

$$\pi^{m-1} \cdot v,\ \sigma\pi^{m-1} v,\ \ldots,\ \sigma^{s-1} \cdot \pi^{m-1} v.$$

Se tienen, en definitiva, $m \cdot s = gr(\pi^m)$ vectores y, por la forma de considerar dichos vectores, son un sistema de generadores, y también una base. La matriz de σ respecto de dicha base tiene la forma interesante:

(C)

$$\left\|\begin{array}{cccc|cccc|cccc|c|cccc}
0 & 1 & \ldots & 0 & & & & & & & & & & & & \\
0 & 0 & \ldots & 0 & & & & & & & & & & & & \\
\cdot & \cdot & \ldots & \cdot & & & & & & & & & & & & \\
-a_o & -a_1 & \ldots & -a_{s-1} & 1 & & & & & & & & & & & \\
\hline
 & & & & 0 & 1 & \ldots & 0 & & & & & & & & \\
 & & & & 0 & 0 & \ldots & 0 & & & & & & & & \\
 & & & & \cdot & \cdot & \ldots & \cdot & & & & & & & & \\
 & & & & -a_o & -a_1 & \ldots & -a_{s-1} & 1 & & & & & & & \\
\hline
 & & & & & & & & 0 & & & & & & & \\
 & & & & & & & & \vdots & \ddots & & \vdots & & & & \\
 & & & & & & & & \cdot & \ldots & -a_{s-1} & 1 & & & & \\
\hline
 & & & & & & & & & & & & 0 & 1 & \ldots & 0 \\
 & & & & & & & & & & & & 0 & 0 & \ldots & 0 \\
 & & & & & & & & & & & & \cdot & \cdot & \ldots & \cdot \\
 & & & & & & & & & & & & -a_o & -a_1 & \ldots & -a_{s-1}
\end{array}\right\|$$

con m bloques de la matriz compañera de π, ceros en los lugares restantes. Llamando C a la matriz compañera de σ, la matriz anterior se puede escribir en forma compacta como sigue

$$\begin{Vmatrix} CL & & & \\ & CL & & \\ & & \ddots & \\ & & & CL \\ & & & C \end{Vmatrix}$$

donde L denota la matriz de $s \times s$

$$L = \begin{Vmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 1 & 0 & \dots & 0 \end{Vmatrix}$$

(0 en todos los coeficientes, excepto en el lugar $s1$ donde figura 1).

Ejemplo 1. Sea $k \in K$. El polinomio $\pi = X - k$ es irreducible en $K[X]$. Vamos a analizar la situación anterior en el caso $p(X) = (X - k)^n$. La matriz compañera del polinomio $X - k$ es $\|k\|$. Por lo tanto, la matriz anterior es

$$\begin{Vmatrix} k & 1 & & & \\ & k & 1 & & \\ & & \ddots & & \\ & & & k & 1 \\ & & & & k \end{Vmatrix}$$

Ejemplo 2. Sea $K = Q$. El polinomio $X^2 - 2$ es irreducible en $Q[X]$. Veamos la matriz correspondiente al caso $p(X) = (X^2 - 2)^n$. La matriz compañera de $X^2 - 2$ es

$$\begin{Vmatrix} 0 & 1 \\ 2 & 0 \end{Vmatrix}$$

por lo tanto, la matriz buscada es

$$\begin{Vmatrix} 0 & 1 & & & & \\ 2 & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & 2 & 0 & 1 & \\ & & & & 0 & \ddots \\ & & & & & 1 \\ & & & & & 0 \quad 1 \\ & & & & & 2 \quad 0 \end{Vmatrix}$$

5. APLICACIÓN DEL TEOREMA DE ESTRUCTURA

Sea $0 \neq V$ un espacio vectorial de dimensión finita sobre un cuerpo K. Sea $\sigma \in \mathrm{End}_K(V)$ y sea $m_\sigma(X) \in K[X]$ su polinomio minimal. Vamos a determinar los polinomios irreducibles característicos de V_σ, es decir los polinomios irreducibles π, tales que la componente π-primaria de V_σ es $\neq 0$.

Afirmación. El polinomio irreducible $\pi \in K[X]$ es característico de V_σ si, y sólo si, π / m_σ. En efecto, si π / m_σ, sea $t(X) \cdot \pi = m_\sigma$. Puesto que grado de $t(X)$ < grado de m_σ, existe un $0 \neq v \in V$, tal que $0 \neq t(X) \cdot v$. Pero, entonces, $0 = m_\sigma(X) \cdot v = \pi(t(X) \cdot v)$, lo cual prueba que $(V_\sigma)_\pi \neq 0$.

Recíprocamente, sea π un polinomio irreducible, tal que existe $0 \neq v \in V$ con $\pi \cdot v = 0$. Entonces el anulador $\mathrm{An}(v)$ en $K[X]$ es un ideal I que contiene a π. Luego, por ser irreducible π, es $I = \langle \pi \rangle$. Como $m_\sigma \cdot v = 0$, se tiene que $m_\sigma \in I$, con lo que π / m_σ. Por lo tanto, si $m_\sigma = \pi_1^{i_1} \ldots \pi_h^{i_h}$. con π_j irreducibles distintos entre sí, resulta

$$V_\sigma = (V_\sigma)_{\pi_1} \oplus \ldots \oplus (V_\sigma)_{\pi_h}.$$

Escribamos, para simplificar la notación

$$(V_\sigma)_{\pi_j} = V_j, \qquad j = 1, \ldots, h.$$

Cada V_j es un π_j-módulo. Se puede aplicar 6.3.1 y representar a V_j como la suma directa de π_j-módulos cíclicos de órdenes correspondientes a los divisores elementales de V_j. 127

Ejemplo. Sea σ un endomorfismo de un espacio vectorial V sobre un cuerpo K de característica $\neq 2$. Supongamos que $\sigma^2 = \mathrm{id}$. Esto implica que el polinomio $X^2 - 1$ anula a σ. Por lo tanto, el polinomio minimal de σ es un divisor de $X^2 - 1$. Puesto que $X^2 - 1 = (X - 1) \cdot (X + 1)$, hay tres posibilidades (por ser $1 \neq -1$ en K!!) $m_\sigma = X - 1$, $m_\sigma = X + 1$ ó $m_\sigma = X^2 - 1$. En los dos primeros casos, σ es una homotecia de razón 1 y -1, respectivamente. Analicemos el caso $m_\sigma = X^2 - 1$. V es suma directa de dos submódulos

$$V = V_{X-1} \oplus V_{X+1}$$

correspondiente a los factores irreducibles $X - 1$ y $X + 1$ de $X^2 - 1$. V_{X-1} *es anulado por* $X - 1$: en efecto, si $v \in V_{X-1}$, $(X - 1)^j \cdot v = 0$ para algún $j \in N$. Sea $\langle p(X) \rangle$ el anulador de v en $K[X]$. Como $(X^2 - 1) \cdot v = 0$, $p(X)$ divide a $X^2 - 1 = (X - 1) \cdot (X + 1)$ y también $p(X)$ divide a $(X - 1)^j$. La única posibilidad es que $p(X) = X - 1$.

Se sigue que sobre V_{X-1} el endomorfismo es una homotecia de razón 1. Por el mismo razonamiento se tiene que sobre V_{X+1}, σ es una homotecia de razón -1. En un sentido fácil de precisar hemos representado a σ como la "suma" de dos homotecias.

La siguiente proposición suministra información importante acerca de σ.

Proposición 8.5.1. Sea σ_j la restricción de σ a V_j. Entonces:

i) σ_j es un endomorfismo de V_j

ii) $m_{\sigma_j} = \pi_j^{t_j}$ (m_{σ_j} denota el polinomio minimal de σ_j y $\pi_j^{t_j}$ corresponde a la representación de m_σ en producto de factores primos).

iii) Si $\pi_j^{s_1}, \ldots, \pi_j^{s_d}$ son los divisores elementales de V_j, con $s_1 \geq \ldots \geq s_d$, resulta

iii') $\pi_j^{s_1} = m_{\sigma_j}$

iii'') $\dim_{\mathbb{Q}} V_j = (s_1 + \ldots + s_d) \cdot \mathrm{gr}(\pi_j)$

iii''') $\chi_{\sigma_j} = \pi_j^{(s_1 + \cdots + s_d)}$ (producto de los divisores elementales).

Demostración. i) es trivial, V_j es submódulo de V_σ.

ii) Si $m_\sigma = \pi_j^{t_j} \cdot t$, con $(\pi_j, t) = 1$, y si $v \in V_j$ es tal que $t \cdot v = 0$, sea $\pi_j^b \cdot v = 0$, y escribiendo $1 = u \cdot \pi_j^b + q \cdot t$ en $K[X]$, resulta $v = u \cdot \pi_j^b(v) + q \cdot t(v) = 0$. Como $m_\sigma \cdot V_j = 0$, debe ser $\pi_j^{t_j} \cdot V_j = 0$. Esto implica que $\pi_j^{t_j}$ es múltiplo del polinomio m_{σ_j}. Puesto que $m_{\sigma_j} \cdot t$ anula a V_σ, por definición de m_σ debe ser $m_{\sigma_j} = \pi_j^{t_j}$.

iii) Por el teorema 6.3.1

128 (*) $$V_j \simeq \frac{K[X]}{\langle \pi_j^{s_1} \rangle} \oplus \ldots \oplus \frac{K[X]}{\langle \pi_j^{s_d} \rangle}, \quad s_d \leq \ldots \leq s_1$$

entonces iii') resulta de ser $\langle \pi^{s_1} \rangle$ el anulador del segundo miembro; iii'') resulta de ser la dimensión de cada sumando igual al grado del polinomio $\pi_j^{s_r} = s_r \cdot \mathrm{gr}(\pi_j)$; iii''') resulta de 8.4.1 y de la propiedad multiplicativa de determinante.

Ejemplo 1. Sea $K = \mathbb{Q}$. Sea $p(X) = (X^2 + 1)^2$. Determinemos espacios vectoriales $\mathbb{Q}^h$ y $\sigma \in \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}^h)$ que tengan a $p(X)$ como polinomio minimal. $(X^2 + 1)^2$ es en cualquier caso el primer divisor elemental, de manera que, por iii''), $4 \leq h$.

Si $h = 4$ y $\sigma \in \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}^4)$ con $m_\sigma = (X^2 + 1)^2$, entonces $(\mathbb{Q}^4)_\sigma$ es cíclico y ya conocemos una representación matricial de σ. $h = 5$ es imposible, pues, por iii''), $\dim_{\mathbb{Q}} V$ es divisible por el grado de π_j, que en este caso es 2. $h = 6$ los divisores elementales posibles son

$$(X^2 + 1)^2, \quad (X^2 + 1).$$

$h = 8$ los divisores elementales posibles son

$$(X^2 + 1)^2, \quad (X^2 + 1), \quad (X^2 + 1)$$
$$(X^2 + 1)^2, \quad (X^2 + 1)^2.$$

En general, h debe ser par y para cada tal h el número posible de situaciones corresponde a la descomposición de h en sumas

$$h = \underbrace{(2 + \ldots + 2)}_{\text{par}} + \underbrace{(1 + \ldots + 1)}_{\text{par}}$$

$$= 2(1 + \ldots + 1) + (1 + \ldots + 1)$$

(par indica número par de sumandos).

Ejemplo 2. Sea $V = \mathbb{Q}^5$, $\sigma \in \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}^5)$ tal que $m_\sigma = (X + 1)^2 \cdot (X^2 + 2)$. Llamando $\pi_1 = X + 1$, $\pi_2 = X^2 + 2$. Se tiene

$$V = V_1 \oplus V_2.$$

El polinomio minimal de σ restringido a V_1 es $(X + 1)^2$, por lo tanto $\dim_{\mathbb{Q}}(V_1) \geq 2$, y análogamente, $\dim_{\mathbb{Q}}(V_2) \geq 2$. Pero, si escribimos V_2 como suma directa de cíclicos

$$\mathbb{Q}[X]/\langle (X^2 + 2)^i \rangle,$$

la dimensión de éstos es *par*. Por lo tanto, dado que V tiene dimensión 5, debe ser $\dim_{\mathbb{Q}}(V_1) = 3$ y $\dim_{\mathbb{Q}}(V_2) = 2$.

Los divisores elementales de V_1 deben ser $(X + 1)^2$, $(X + 1)$. Por lo tanto, la matriz puede representarse en la forma

$$\left\|\begin{array}{ccccc} -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -2 & 0 \end{array}\right\|$$

Ejemplo 3. Sean $V = \mathbb{Q}^9$ y $\sigma \in \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}^9)$, tal que $m_\sigma = X^2(X^2 + X + 1)^2$ $\dim_{\mathbb{Q}}(V_1) \geq 2$, $\dim_{\mathbb{Q}}(V_2) \geq 4$, donde $\pi_1 = X$, $\pi_2 = X^2 + X + 1$. Los posibles divisores elementales son

Si	V_1	V_2
$\dim_{\mathbb{Q}}(V_1) = 2$	imposible	
$\dim_{\mathbb{Q}}(V_1) = 3$	X^2, X	$(X^2 + X + 1)^2,\ X^2 + X + 1$
$\dim_{\mathbb{Q}}(V_1) = 4$	imposible	
$\dim_{\mathbb{Q}}(V_1) = 5$	X^3, X^2, X	$(X^2 + X + 1)^2$
	X^3, X, X, X	$(X^2 + X + 1)^2$

Las matrices correspondientes a la última situación serían

$$\left\|\begin{array}{ccccccccc} 0 & 1 & & & & & & & \\ 0 & & & & & & & & \\ & & 0 & 1 & & & & & \\ & & 0 & & & & & & \\ & & & & 0 & 0 & & & \\ & & & & 0 & & & & \\ & & & & & & 0 & 0 & 1 \\ & & & & & & -1 & -1 & 1 \\ & & & & & & & & 0 \quad 1 \\ & & & & & & & & -1 \ -1 \end{array}\right\| \qquad \left\|\begin{array}{ccccccccc} 0 & 1 & & & & & & & \\ 0 & & & & & & & & \\ & & 0 & 0 & & & & & \\ & & 0 & & 0 & 0 & & & \\ & & & & 0 & & & & \\ & & & & & & 0 & 0 & 1 \\ & & & & & & -1 & -1 & 1 \\ & & & & & & & & 0 \quad 1 \\ & & & & & & & & -1 \ -1 \end{array}\right\|$$

Volvamos al tratamiento general. En virtud de (*) cabe elegir una base de V_j, tal que la matriz de σ respecto de dicha base tiene la forma, en bloques,

$$F_{\pi_j} = \left\| \begin{array}{ccccccc} C_1 & & & & & & \\ & C_2 & & & & & \\ & & \ddots & & & & \\ & & & C_t & & & \\ & & & & \ddots & & \\ & & & & & C_d & \end{array} \right\| \quad t = 1, \ldots, d$$

donde cada C_t es del tipo (C) de la sección 8.4.

Siendo V_σ la suma directa de las componentes π_j-primarias, podemos elegir en cada V_j una base como la que da lugar a F_{π_j} y obtener una base de V, tal que la matriz de σ respecto de la misma es la matriz de bloques

$$\text{(FCC)} \qquad \left\| \begin{array}{ccccc} F_{\pi_1} & & & & \\ & \ddots & & & \\ & & F_{\pi_j} & & \\ & & & \ddots & \\ & & & & F_{\pi_h} \end{array} \right\| \quad j = 1, \ldots, h$$

Definición 8.5.2. La matriz (FCC) se denomina la *forma canónica clásica* de σ.

Definición 8.5.3. Se llaman *divisores elementales* de σ a los divisores elementales del módulo V_σ. Análogamente, se denominan *factores invariantes* de σ a los factores invariantes de V_σ. Utilizaremos a continuación los factores invariantes para obtener otra forma canónica de σ.

Sean $p_1, \ldots, p_m$ los factores invariantes de V_σ. Entonces

$$V_\sigma \simeq \frac{K[X]}{\langle p_1 \rangle} \oplus \cdots \oplus \frac{K[X]}{\langle p_m \rangle}$$

con p_i / p_j si $i \leq j$. Sobre cada

$$\frac{K[X]}{\langle p_j \rangle}$$

existe una base tal que σ_j, respecto de la misma, posee por matriz la matriz compañera de p_j. Por lo tanto, reuniendo todas esas bases se obtiene una base respecto de la cual la matriz de σ es la matriz de bloques

$$(\mathrm{FCJ}) \qquad J_\sigma = \begin{Vmatrix} C(p_1) & & & \\ & \ddots & & \\ & & C(p_j) & \\ & & & \ddots \\ & & & C(p_m) \end{Vmatrix} \qquad j = 1, \ldots, m.$$

donde cada $C(p_j)$ es la matriz compañera de p_j.

Definición 8.5.4. La matriz (FCJ) se denomina la *forma canónica de Jordan* de σ. Nótese que el polinomio característico de J_σ es el producto

$$\begin{aligned} \chi_\sigma &= \det(X \cdot I - C(p_1)) \ \ldots \ \det(X \cdot I - C(p_m)) \\ &= p_1 \ldots p_m. \end{aligned}$$

Puesto que

$$p_m \cdot V = 0 \qquad (\text{pues, } p_m \cdot \left(\frac{K[X]}{\langle p_i \rangle}\right) = 0, \ \forall i, \ i = 1, \ldots, m)$$

se tiene el siguiente teorema.

Teorema 8.5.5. (Hamilton-Cayley) $\chi_\sigma(\sigma) = 0$ (o sea el polinomio característico de σ anual a σ.

Corolario 8.5.6. m_σ / χ_σ, es decir el polinomio minimal, divide al polinomio característico.

Sea $e_1, \ldots, e_n$ una base de V y $((\alpha_{ij}))$ la matriz de σ respecto de la base e_i. Entonces, los factores invariantes de σ se calculan llevando la matriz característica

$$X \cdot I_n - ((\alpha_{ij})) \in M_n(K[X])$$

a la forma diagonal canónica

$$\mathrm{diag}(d_1 \ldots d_n), \ d_i \in K[X], \ d_i / d_j \text{ si } i \leq j.$$

Calculados los factores invariantes, es fácil calcular los divisores elementales como se hizo en el capítulo 7.

Ejemplo. Sea $\sigma : Q^3 \to Q^3$, tal que respecto de alguna base de Q^3 la matriz es

$$\begin{Vmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ -2 & -2 & -1 \end{Vmatrix}$$

La matriz característica es

$$\begin{Vmatrix} X-1 & -2 & 0 \\ 0 & X-2 & 0 \\ 2 & 2 & X+1 \end{Vmatrix}$$

Esta matriz ya fue diagonalizada en el capítulo 6. Los factores invariantes son

$$1,\ 1,\ (X-2)\cdot(X^2-1) = X^3-2X^2-X+2.$$

La forma de Jordán de σ es

$$\begin{Vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -2 & 1 & 2 \end{Vmatrix}$$

Los divisores elementales son $X-2$, $X-1$, $X+1$. Por lo tanto, la forma canónica clásica es

$$\begin{Vmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{Vmatrix}$$

EJERCICIOS

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 1.

Ejercicio 1. Sea A un R-módulo unitario a la izquierda. Probar

i) $0 \cdot a = 0$, para todo $a \in A$.

ii) $r \cdot 0 = 0$, para todo $r \in R$.

iii) $(-r) \cdot a = r \cdot (-a) = -(r \cdot a)$, si $a \in A$ y $r \in R$.

Ejercicio 2. Describir todas las estructuras de $\mathbf{Z}_n$-módulo unitario definidas sobre $\mathbf{Z}_2$, $\mathbf{Z}_4$, $\mathbf{Z}_6$, $\mathbf{Z}_8$. ¿Es $\mathbf{Z}_6$ un $\mathbf{Z}_3$-módulo unitario?

Ejercicio 3. Sea $\mathbf{Q}$ considerado como $\mathbf{Z}$-módulo.

i) Determinar el menor (respecto de la inclusión) submódulo de $\mathbf{Q}$ que contiene a $\mathbf{Z}$ y $1/2$.

ii) Probar que todo submódulos de $\mathbf{Q}$, finitamente generado, es cíclico.

iii) Probar que si $\sigma : \mathbf{Q} \to \mathbf{Q}$ es un endomorfismo, entonces $\sigma = 0$ ó σ es un automorfismo. Deducir que $\mathbf{Q}$ no posee submódulo propio alguno isomorfo a $\mathbf{Q}$.

iv) Dar un ejemplo de submódulo de $\mathbf{Q}$, distinto de $\mathbf{Q}$, que no sea de tipo finito.

v) Mostrar cinco o más submódulos de $\mathbf{Q}$ no isomorfos entre sí. Mostrar una familia infinita de submódulos de $\mathbf{Q}$ no isomorfos entre sí.

Ejercicio 4. Sea $\mathbf{Z}_{12}$ considerado como $\mathbf{Z}$-módulo. Determinar todos los submódulos de $\mathbf{Z}_{12}$. Determinar los ideales de $\mathbf{Z}$ que sean aniladores de elementos (o aniladores de submódulos) de $\mathbf{Z}_{12}$.

Ejercicio 5. Sea A un R-módulo a la izquierda y sean A', A'' submódulos. Sea $(A'' : A') = \{r / r \cdot A' \subset A''\} \subset R$.

i) Probar que $(A'' : A')$ es un ideal bilátero de R.

ii) Determinar $(A'' : 0)$, $(A'' : A'')$, $(A : A'')$, $(0 : A')$.

iii) Sean n, m enteros positivos. Probar que $(\langle m \rangle : \langle n \rangle) = \langle \frac{m}{d} \rangle$, donde $d = (m, n)$.

Ejercicio 6. Dar un ejemplo de módulo A sobre un anillo R con la propiedad de que dos submódulos distintos cualesquiera no sean isomorfos.

Ejercicio 7. Sea $R = \mathbf{Z}$. Probar que si A es un $\mathbf{Z}$-módulo, tal que dos subgrupos de A no nulos son isomorfos, entonces $A \simeq \mathbf{Z}$.

Ejercicio 8. Probar que no existe ningún morfismo no nulo de $\mathbf{Z}$-módulos de $\mathbf{Z}_n$ en $\mathbf{Z}_m$, si $(n,m) = 1$.

Ejercicio 9. i) Probar que no existe ningún epimorfismo de $\mathbf{Z}$ sobre $\mathbf{Q}$.

ii) Sean p y q primos. Probar que $\mathbf{Z}_{p^\infty} \simeq \mathbf{Z}_{q^\infty}$ si, y sólo si, $p = q$.

Ejercicio 10. Probar que todo submódulo de $\mathbf{Q}/\mathbf{Z}$ de tipo finito es cíclico.

Ejercicio 11. Probar que no existe ningún monomorfismo de $\mathbf{Z}$ en $\mathbf{Q}/\mathbf{Z}$.

Ejercicio 12. Sea H un subgrupo de $\mathbf{Q}$. Probar que si $H \neq \mathbf{Q}$, entonces existe un subgrupo H' de $\mathbf{Q}$, tal que $H \subset H' \subset \mathbf{Q}$, donde ambas inclusiones son estrictas. (O sea, $\mathbf{Q}$ no posee subgrupos maximales). Deducir que no existe ningún morfismo no nulo de $\mathbf{Q}$ en $\mathbf{Z}$. Análogamente no existe ningún morfismo no nulo de

i) $\mathbf{Q}$ en $\mathbf{Z}_n$.

ii) $\mathbf{Q}/\mathbf{Z}$ en $\mathbf{Z}$.

Ejercicio 13. Probar que no existe ningún morfismo no nulo de $\mathbf{Q}/\mathbf{Z}$ en $\mathbf{Q}$.

Ejercicio 14. Probar que no existe ningún epimorfismo (de $\mathbf{Z}$-módulos) de $\mathbf{Q}$ sobre $\mathbf{R}$.

Ejercicio 15. Sea A un grupo abeliano finito, tal que dos subgrupos cualesquiera H y L satisfagan alguna de las relaciones $H \subset L$ ó $L \subset H$. Probar que $A \simeq \mathbf{Z}_{p^t}$, p primo.

Ejercicio 16. Dar ejemplos de grupos abelianos, tales que todo endomorfismo sea una homotecia. Un problema de investigación sería caracterizar dichos grupos abelianos.

Ejercicio 17. Dar ejemplos de módulos A, con submódulos $A' \simeq A''$, tales que los módulos cocientes A/A' y A/A'' no sean isomorfos.

Ejercicio 18. Calcular

i) $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_5, \mathbf{Z}_{10})$

ii) $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_4, \mathbf{Z})$

iii) $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_5, \mathbf{Z}_5)$

iv) $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_5, \mathbf{Q})$

v) $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_2, \mathbf{Z}_4)$.

Describir explícitamente los morfismos en cada caso.

Ejercicio 19. a) Calcular

i) $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_{p^\infty})$, p primo racional

ii) $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_{p^\infty}, \mathbf{Z}_{q^\infty})$, p y q primos racionales

iii) $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_{p^1}, \mathbf{Z}_{p^\infty})$, p primo racional

b) ¿Es $\mathbf{Z}_{p^\infty}$, $\mathbf{Z}_n$-módulo unitario para algún $n \in \mathbf{N}$?

Ejercicio 20. Sea K uno de los cuerpos $\mathbf{Q}$ ó $\mathbf{R}$. K^2 el espacio vectorial, sobre K, de pares ordenados (a, b), con las operaciones

$$(a, b) + (a', b') = (a + a', b + b')$$

$$k \cdot (a, b) = (k \cdot a, k \cdot b).$$

i) Probar que si S es submódulo de K^2, entonces S tiene una (y sólo una) de las formas siguientes: 0, K^2 o existen $r, s \in K$, tales que $S = \{(x, y)/r \cdot x + s \cdot y = 0\}$. Utilizando la representación de K^2 en el plano, dibujar los posibles subespacios.

ii) Sea $f : K^2 \to K$ un morfismo de K-módulos.

a) Probar que existen $a, b \in K$ tales que $f(x, y) = a \cdot x + b \cdot y$, cualquiera que sea $(x, y) \in K^2$.

b) Probar que si f no es el morfismo nulo, entonces f es un epimorfismo.

c) Sea $k \in K$. Caracterizar los subconjuntos de K^2 de la forma

$$f^{-1}(k) = \{(x, y)/f(x, y) = k\}$$

Ilustrar en forma gráfica, tomando diferentes k.

d) Demostrar que no existe ningún morfismo f de K^2 en K, tal que si $T = \{(x, y)/x^2 + y^2 = 1\}$, entonces $f(t) = 1$ cualquiera que sea $t \in T$. (Utilizar c)). ¿Es la misma afirmación válida para cualquier cuerpo K?

e) Demostrar que todo submódulo de K^2 es de tipo finito.

f) Calcular $\mathrm{Hom}_K(K, K^2)$ y $\mathrm{Hom}_K(K^2, K)$.

Ejercicio 21. Sea V un espacio vectorial *racional*. Probar que si $f : V \to V$ es una aplicación aditiva, es decir $f(x + y) = f(x) + f(y)$, entonces f es un morfismo de $\mathbf{Q}$-módulos. ¿Es cierto lo mismo sobre el cuerpo real?

Ejercicio 22. Determinar todas las clases de isomorfismo de módulos sobre $\mathbf{Z}_n$. Ilustrar con $\mathbf{Z}_2$, $\mathbf{Z}_4$, $\mathbf{Z}_5$. ¿En qué casos hay dos únicas clases?

Ejercicio 23. Sea $R = \mathbf{Z}[\sqrt{2}]$ el subanillo de R de todos los elementos de la forma $a + b\sqrt{2}$, a y b enteros. ¿Existe sobre $\mathbf{Z}$ una estructura de $\mathbf{Z}[\sqrt{2}]$-módulo unitario? (Respuesta: No.)

Ejercicio 24. Determinar todas las clases de isomorfismos de módulos cíclicos sobre $\mathbf{R}[X]$. Lo mismo $\mathbf{C}[X]$.

Ejercicio 25. Dar ejemplos de $K[X]$-módulos que no sean submódulos o módulos cocientes de $K[X]$.

Ejercicio 26. Un módulo M sobre un anillo R se dice *simple* si $0 \neq M$ y, además, 0 y M son los únicos submódulos de M.

i) Probar que si $f : M \to A$ es un morfismo de módulos y M es simple, entonces f es el morfismo nulo o es un *mono*morfismo. Probar que si M y A son ambos simples, entonces f es el morfismo nulo o es un isomorfismo.

ii) Determinar todos los módulos simples sobre $\mathbf{Z}$.

iii) Probar que los ideales columnas de $\mathbf{M}_n(K)$ del tipo J_i, $i \in [\![1, n]\!]$ son módulos simples.

iv) Probar que dos módulos simples sobre $\mathbf{M}_n(K)$ son isomorfos.

v) Caracterizar los módulos simples sobre $K[X]$, K un cuerpo.

vi) Caracterizar los módulos simples sobre $\mathbf{Z}_n$.

136

vii) Caracterizar los módulos simples sobre $\mathbf{Z}_{(p)}$ (la localización de $\mathbf{Z}$ en el primo p).

viii) Dar ejemplos de anillos que poseen un módulo simple fiel.

Ejercicio 27. *Lema de los cinco.* Dado el diagrama conmutativo con filas exactas

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow h_1 & & \downarrow h_2 & & \downarrow h_3 & & \downarrow h_4 & & \downarrow h_5 \\ N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \xrightarrow{g_3} & N_4 & \xrightarrow{g_4} & N_5 \end{array}$$

se verifica:

i) Si h_1 es un epimorfismo y h_2 y h_4 son monomorfismos, entonces h_3 es un monomorfismo.

ii) Si h_5 es un monomorfismo y h_2 y h_4 son epimorfismos, entonces h_3 es un epimorfismo

iii) Si h_1 es un epimorfismo, h_5 es un monomorfismo y h_2 y h_4 son isomorfismos, entonces h_3 es un isomorfismo.

Ejercicio 28. Si S y T son submódulos de un R-módulo M, deducir de los homomorfismos de inclusión el diagrama conmutativo con filas y columnas exactas

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & S \cap T & \longrightarrow & S & \longrightarrow & S/S \cap T & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T & \longrightarrow & M & \longrightarrow & M/T & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T/S \cap T & \longrightarrow & M/S & \longrightarrow & M/S + T & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Aplicar a la situación $M = \mathbf{Z}$, $S = \langle m \rangle$, $T = \langle n \rangle$.

Ejercicio 29. Sean M_1 y M_2 submódulos de un módulo M. Probar que si $M_1 \cap M_2$ y $M_1 + M_2$ son de tipo finito, entonces así lo son M_1 y M_2.

Ejercicio 30. Sea $n \in \mathbf{N}$, $1 < n$. Para cada divisor r de n definir una sucesión exacta corta

$$0 \to r' \cdot \mathbf{Z}_n \to \mathbf{Z}_n \to r \cdot \mathbf{Z}_n \to 0$$

donde $r' = \frac{n}{r}$. Probar que el morfismo $\mathbf{Z}_n \to r \cdot \mathbf{Z}_n$ se parte (es decir, existe un morfismo $r \cdot \mathbf{Z}_n \to \mathbf{Z}_n$, tal que $\mathbf{Z}_n \to r \cdot \mathbf{Z}_n \to \mathbf{Z}_n$ es el morfismo identidad) si, y sólo si, $(r, r') = 1$.

Ejercicio 31. Dado el diagrama conmutativo de R-módulos

$$\begin{array}{ccc}
M & \xrightarrow{f} & N \\
h \downarrow & & \downarrow h' \\
M' & \xrightarrow{f} & N'
\end{array}$$

probar que existe un único morfismo $u: \mathrm{Nu}(h) \to \mathrm{Nu}(h')$ y un único morfismo $v: M'/h(M) \to N'/h(N')$ que hace conmutativo el diagrama

$$\begin{array}{ccc}
\mathrm{Nu}(h) & \xrightarrow{u} & \mathrm{Nu}(h') \\
\downarrow & & \downarrow \\
M & \xrightarrow{f} & N \\
\downarrow & & \downarrow \\
M' & \xrightarrow{f'} & N' \\
\downarrow & & \downarrow \\
M'/h(M) & \xrightarrow{v} & N'/h(N)
\end{array}$$

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 2

Ejercicio 1. Probar que el anillo $\mathbf{Z}[X]$ de polinomios con coeficientes enteros racionales es un anillo noetheriano.

Ejercicio 2. Probar que si R y S son anillos, $f: R \to S$ un epimorfismo de anillos, entonces R noetheriano implica S noetheriano.

Ejercicio 3. Sea $d \in \mathbf{Z}$ y sea $\sqrt{d}$ *una* raíz cuadrada de d en el cuerpo complejo. Sea $\mathbf{Z}[\sqrt{d}]$ el subanillo de $\mathbf{C}$ formado por la totalidad de elementos de la forma $a + b \cdot \sqrt{d}$, a y b enteros. Probar que $\mathbf{Z}[\sqrt{d}]$ es un anillo noetheriano.

Ejercicio 4. Probar que el anillo de funciones reales continuas definidas en el intervalo cerrado $[0, 1]$ no es noetheriano.

Ejercicio 5. Sea M un R-módulo noetheriano.

i) Probar que todo submódulo propio de M está contenido en un submódulo propio maximal de M.

ii) Probar que si $\sigma : M \to M$ es un epimorfismo, entonces σ es un isomorfismo, es decir $Nu(\sigma) = 0$.

Ejercicio 6. Sea D un dominio de integridad y sea Q su cuerpo de cocientes. Se denomina *ideal fraccionario de* D a todo submódulo F de Q, tal que existe $0 \neq a \in R$ con $a \cdot F \subset R$. Probar:

a) Que todo submódulo F de Q de tipo finito es un ideal fraccionario de D. ¿Es cierta la recíproca?

b) Que si F es un ideal fraccionario de D, F es isomorfo a un ideal de D.

c) Que si D es un dominio principal y F es un ideal fraccionario de D, entonces F es un módulo cíclico.

Ejercicio 7. Un R-módulo (a la izquierda) M se dice *artiniano* (a la izquierda), si toda cadena descendiente de submódulos de M, $N_1 \supset N_2 \supset \ldots$ es estacionaria, es decir, existe un índice $k \in N$, tal que $N_k = N_{k+1}$ para todo $i \in N$. Un anillo R se dice *artiniano* si R es un R-módulo artiniano. Probar:

a) Que M es artiniano si, y sólo si, toda familia no vacía de submódulos de M posee un elemento minimal.

b) Que si M es artiniano y si $\sigma : M \to M$ es un *mono*morfismo entonces σ es un isomorfismo, es decir $Im(\sigma) = M$.

Ejercicio 8. Probar que un dominio de integridad es artiniano si, y sólo si, es un cuerpo. (Sugerencia: Sea D dominio artiniano y $0 \neq \alpha$ un ideal minimal de D. Sea $0 \neq a \in \alpha$. Entonces $\alpha \cdot a = \alpha$, por lo tanto *existe* $x \in \alpha$, tal que $x \cdot a = a$, y así $x^2 \cdot a = a$ y, en consecuencia $1 = x^2 \in \alpha$. De aquí se infiere $\alpha = D$ (D es un cuerpo)).

Ejercicio 9. Dar ejemplos de módulos artinianos que no sean noetherianos (sugerencia: considere $\mathbf{Z}_{p^\infty}$).

Nota. Un resultado no muy fácil de probar afirma que todo *anillo* artiniano es noetheriano (véase, por ejemplo, Bourbaki: Algèbre, capítulo 8, Módulos y Anillos Semisimples, página 72). Otros resultados válidos son los siguientes:

i) Existen anillos artinianos a la izquierda que no son artinianos a la derecha, (véase Bourbaki, *loc, cit.*, página 27).

ii) Existen anillos noetherianos a la izquierda (aun principales a la izquierda) que no son noetherianos a la derecha.

Ejercicio 10. *Anillo de grupo.* Sea G un grupo finito (escrito multiplicativamente) y sea K un anillo conmutativo. Sea K[G] la totalidad de aplicaciones de G en K. Sean $f, g \in K[G]$. Se define

$$(f + g)(x) = f(x) + g(x)$$

$$(f * g)(x) = \sum_{y \in G} f(y) \cdot g(y^{-1} \cdot x) \quad \text{(producto de convolución)}$$

i) Probar que K[G], dotado de las dos leyes de composición precedentes, es un anillo, llamado *anillo (o álgebra) de grupo de G sobre K.*

ii) Probar que si G es un grupo cíclico de orden n, entonces K[G] es isomorfo al anillo cociente $K[X]/\langle X^n - 1 \rangle$.

iii) Sea, para cada $x \in G$, e_x la función característica del subconjunto puntual $\{x\}$ de G (o sea $e_x(x) = 1$ y $e_x(z) = 0$ si $x \neq z$). Probar que todo elemento f de K[G] se escribe unívocamente en la forma

$$f = \sum_{x \in G} a_x \cdot e_x, \qquad a_x \in K$$

(Se suele escribir, por abuso de notación, $f = \sum_{x \in G} a_x \cdot x$.)

iv) Probar que K[G] es un anillo conmutativo si, y sólo si, G es un grupo conmutativo.

v) Probar que K[G] es artiniano (respectivamente noetheriano) si, y sólo si, K es artiniano (respectivamente noetheriano).

vi) Probar que la aplicación $K[G] \to K$ definida por

$$\sum_{x \in G} a_x \cdot e_x \longmapsto \sum_{x \in G} a_x$$

es un morfismo de anillos cuyo núcleo es un ideal bilátero $\mathcal{J}$, denominado el ideal de aumentación de K[G]. Probar que $\mathcal{J}$ coincide con el K-submódulo de K[G] generado por los elementos de la forma $1 - g$, donde g recorre G.

vii) Se denomina K-representación de G a todo morfismo $\rho : G \to \mathrm{Aut}(M)$ del grupo G en el grupo de K-automorfismos de un K-módulo M. Probar que toda representación del grupo G determina un K[G]-módulo, y recíprocamente, todo todo K[G]-módulo da lugar a una representación de G. (Se dice también que el K[G]-módulo es un G-módulo.) (La teoría de representación de grupos es una rama importante de la matemática que ha permitido estudiar con éxito cuestiones de estructura de grupos. En la actualidad constituye un campo importante de investigación, principalmente por la utilización de resultados de la teoría algebraica de números. Se recomienda al lector la lectura del tratado de Curtiss-Reiner (6), así como también (21a).

viii) ¿Cómo definir K[G] en el caso de un grupo G *infinito*?

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 3

Ejercicio 1. Determinar cuáles de las siguientes sumas en $\mathbf{Z} \oplus \mathbf{Z}$ son directas.

i) $(1,1)\cdot \mathbf{Z} + (-1,1)\cdot \mathbf{Z}$

ii) $(2,3)\cdot \mathbf{Z} + (-2,-3)\cdot \mathbf{Z}$

iii) $(1,2)\cdot \mathbf{Z} + (3,6)\cdot \mathbf{Z}$

iv) $0 + (1,2)\cdot \mathbf{Z}$.

Ejercicio 2. ¿Es $(1,2,3)\cdot \mathbf{Z}$ un sumando directo en $\mathbf{Z}^3 = \mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z}$? Determinar una condición necesaria y suficiente sobre $a, b, c \in \mathbf{Z}$ para que $(a,b,c)\cdot \mathbf{Z}$ sea sumando directo de $\mathbf{Z}^3$.

Ejercicio 3. Probar que todo subgrupo de $\mathbf{Z}^2$ es isomorfo a uno de los siguientes grupos: 0, $\mathbf{Z}$ ó $\mathbf{Z} \oplus \mathbf{Z}$.

Ejercicio 4. Estudiar el anillo de endomorfismos $\mathrm{End}_{\mathbf{Z}}(\mathbf{Z} \oplus \mathbf{Z})$ de $\mathbf{Z} \oplus \mathbf{Z}$ y el grupo $\mathrm{Aut}(\mathbf{Z} \oplus \mathbf{Z})$ de automorfismos.

Ejercicio 5. Calcular, en cada caso, el anulador en $\mathbf{Z}$ de

i) $\mathbf{Z}_2 \oplus \mathbf{Z}_3$

ii) $\mathbf{Z} \oplus \mathbf{Z}_2$,

iii) $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_8$

iv) $\mathbf{Z}_{p^\infty}$

v) $\mathbf{Z}_{p^\infty} \oplus \mathbf{Z}_{q^\infty}$, $p \neq q$.

Ejercicio 6. Sea A un grupo abeliano, tal que existe una sucesión exacta

$$0 \to \mathbf{Z}_n \to A \to \mathbf{Q} \to 0.$$

Probar que A es isomorfo a la suma directa $\mathbf{Z}_n \oplus \mathbf{Q}$. Generalizar el resultado reemplazando $\mathbf{Q}$ por cualquier grupo abeliano sin torsión.

Ejercicio 7. Dar un ejemplo de grupo abeliano A, tal que tA no sea sumando directo de A.

Ejercicio 8. Probar la siguiente afirmación: Sean $n, m \in \mathbf{N}$. Entonces existe un epimorfismo $\mathbf{Z} \to \mathbf{Z}_n \oplus \mathbf{Z}_m$ si, y sólo si, $(n,m) = 1$.

Ejercicio 9. Probar la no existencia de epimorfismos en cualquiera de las situaciones siguientes:

i) $\mathbf{Z} \to \mathbf{Z} \oplus \mathbf{Q}$

ii) $\mathbf{Q} \to \mathbf{Q} \oplus \mathbf{Q}$

iii) $\mathbf{Z}_{p^\infty} \to \mathbf{Z}_{q^\infty}$, $p \neq q$

iv) $\mathbf{Q} \to \mathbf{R}$

v) $\mathbf{Z}^n \to \mathbf{Z}^m$, si $n < m$

vi) $\mathbf{Z} \oplus \mathbf{Z}_n \oplus \mathbf{Z}_n \to \mathbf{Z} \oplus \mathbf{Z}_{n^2}$.

Ejercicio 10. Con qué hipótesis adicionales es posible establecer epimorfismos en las situaciones siguientes:

i) $\mathbf{Z}_n \to \mathbf{Z}_m$

ii) $\mathbf{Z}_n \to \mathbf{Z}_h \oplus \mathbf{Z}_k$

iii) $\mathbf{Q} \to \mathbf{Z}_{p^\infty} \oplus \mathbf{Z}_{q^\infty}$.

Ejercicio 11. Sean $n, m \in \mathbf{N}$. Probar que

$$\oplus^n \mathbf{Z}_{p^\infty} \simeq \oplus^m \mathbf{Z}_{p^\infty} \text{ si, y sólo si, } n = m.$$

Ejercicio 12. ¿Es cierto que todo grupo abeliano es subgrupo de un grupo abeliano libre? ¿Es $\mathbf{Q}$ subgrupo de un grupo abeliano libre? Probar que ningún grupo abeliano *divisible* es subgrupo de un grupo abeliano libre.

Ejercicio 13. Sea $\{A_\alpha\}_{\alpha \in I}$ una familia de R-módulos. Sea $\{A'_\alpha\}_{\alpha \in I}$ una familia tal que para todo $\alpha \in I$, A'_α es submódulo de A_α.

i) Definir una identificación *natural* de

$$\oplus_{\alpha \in I} A'_\alpha \text{ a un submódulo de } \oplus_{\alpha \in I} A_\alpha.$$

ii) Probar la existencia de un isomorfismo natural

$$\oplus_\alpha \frac{A_\alpha}{A'_\alpha} \simeq (\oplus_\alpha A_\alpha)/(\oplus_\alpha A').$$

iii) Sea $\{n_\alpha\}_\alpha, n_\alpha \in \mathbf{N}$. Probar un isomorfismo

$$\frac{\oplus_\alpha \mathbf{Z}}{\oplus_\alpha \langle n_\alpha \rangle} \simeq \oplus_\alpha \mathbf{Z}_{n_\alpha}.$$

iv) Sea $n \in \mathbf{N}$. Probar un isomorfismo

$$\frac{\oplus_\alpha \mathbf{Z}}{n \cdot (\oplus_\alpha \mathbf{Z})} \simeq \oplus_\alpha \mathbf{Z}_n.$$

v) Analizar las mismas situaciones para Π.

Ejercicio 14. Sea P el conjunto de todos los primos racionales. Sea P' un subconjunto no vacío de P. Con la identificación natural

$$\mathbf{Q}/\mathbf{Z} = \bigoplus_{p \in P} \mathbf{Z}_{p^\infty}$$

determinar un subgrupo H de $\mathbf{Q}$, tal que el morfismo canónico $\mathbf{Q} \to \mathbf{Q}/\mathbf{Z}$ aplique H sobre

$$\bigoplus_{p \in P'} \mathbf{Z}_{p^\infty}.$$

Analizar el caso $P' = \{p\}$.

Ejercicio 15. Sea K un cuerpo y $R = \mathbf{M}_n(K)$ el anillo completo de matrices de $n \times n$ con coeficientes en K. Sea sobre R la estructura de R-módulo a la izquierda. Sean J_i, $i = 1, \ldots, n$ los ideales a la izquierda en columnas

$$J_i = \{((a_{st}))/a_{st} = 0 \text{ si } t \neq i\}.$$

i) Probar que J_i es un módulo simple (o sea, 0 y J_i son sus únicos submódulos).

ii) Probar que $R = J_1 \oplus \ldots \oplus J_n$ (como R-módulos a la izquierda).

iii) Sea J un ideal a la izquierda de R. Probar que J es sumando directo de R (o sea, existe un ideal H de R, tal que $R = J \oplus H$) (sugerencia: sea J un ideal a la izquierda de R, sea $H = J_{i_1} \oplus \ldots \oplus J_{i_k}$ (de ii) con las propiedades $J \cap H = 0$ y k maximal con esta propiedad. Si $J + H \neq R$, por ii) algún J_s no está contenido en H. Como $J_s \cap H$ es submódulo de J_s debe ser necesariamente 0. Pero, entonces, $(J_{i_1} \oplus \ldots \oplus J_{i_k} \oplus J_s) \cap \cap H = 0$, contrario a la maximalidad de k. Se sigue que $J \oplus H = R$).

iv) Sea L un ideal a la izquierda de R. Probar que R/L es isomorfo a un sumando directo de R. Deducir que todo módulo simple sobre R es isomorfo a un ideal de R. Probar que $J_i \simeq J_s$ si $i, s \in [1, n]$. Probar
142 que sobre R existe un único (salvo isomorfismos) módulo simple.

Nota. Es posible probar que *todo* R-módulo es suma directa de módulos simples, y que para todo R-módulo, todo submódulo es sumando directo. (Véase (3b) y (16).)

v) Sea S un R-módulo *simple*. Probar que el anulador de S es 0.

vi) Probar que 0 y R son los únicos ideales *bilateros* de R. (Sugerencia: sea $\alpha \neq R$ un ideal bilátero de R. Existe entonces un ideal a la izquierda J, tal que $R = \alpha \oplus J$. Adviértase que $\alpha \cdot J \subset \alpha \cap J = 0$. Como J es suma directa de módulos simples, $J = \oplus S_i$, $\alpha \cdot S_i = 0$. Por v) debe ser $\alpha = 0$).

Ejercicio 16. Sea R un anillo con identidad. Se dice que R es un anillo de *von Neumann*, si para todo $a \in R$ existe $x \in R$, tal que $a \cdot x \cdot a = a$. Probar:

i) R es un anillo de von Neumann si, y sólo si, todo ideal principal es sumando directo de R.

ii) R es un anillo de von Neumann si, y sólo si, todo ideal a la izquierda de tipo finito es sumando directo. Nótese que por la misma definición de R, son válidas afirmaciones idénticas para ideales a la derecha.

iii) Si R es un anillo de Boole (o sea, $a^2 = a$ cualquiera que sea $a \in R$), entonces R es un anillo de von Neumann.

iv) Si K es un cuerpo, $\mathbf{M}_n(K)$ es anillo de von Neumann. (O, más generalmente, K es un anillo de von Neumann si, y sólo si, así lo es $\mathbf{M}_n(K)$).

Ejercicio 17. Determinar *todos* los elementos ídempotentes de los anillos siguientes:

i) $\mathbf{Z}_8$, $\mathbf{Z}_{15}$, $\mathbf{Z}_{24}$, $\mathbf{Z}_{23}$, $\mathbf{Z}_{30}$.

ii) $\mathbf{Z}_{p.q}$, p y q primos distintos.

iii) $\mathbf{Z}_{p^2.q}$, p y q primos distintos.

Ejercicio 18. Determinar todos los elementos ídempotentes del anillo $R = \mathrm{End}(\mathbf{Z} \oplus \mathbf{Z})$.

Ejercicio 19. Sea R un anillo conmutativo. Sea $\mathrm{End}_R(M)$ el anillo de R-endomorfismos de M. ¿Qué propiedad de M traducen los elementos ídempotentes de $\mathrm{End}_R(M)$?

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 4

Ejercicio 1. Probar que un submódulo de $\mathbf{Q}$ (como $\mathbf{Z}$-módulo) es libre si, y sólo si, es cíclico.

Ejercicio 2. Probar que no existe ningún epimorfismo de $\mathbf{Q}$ sobre un módulo libre.

Ejercicio 3. ¿Qué anillos R satisfacen la siguiente propiedad: todo R-módulo a la izquierda es libre?.

Ejercicio 4. Sea R un anillo con identidad. Probar que todo módulo M es imagen mórfica de un módulo libre. (Sugerencia: sea X un conjunto de generadores de M, sea para cada $x \in X$, R^x un módulo isomorfo a R. Sea A la suma directa $\bigoplus_{x \in X} R^x$. Definir ahora una aplicación conveniente de A sobre M).

Ejercicio 5. Sean A y L, R-módulos. Probar que si L es libre todo epimorfismo $f : A \to L$ se *parte*, es decir existe un morfismo $h : L \to A$, tal que $f \cdot h = id_L$ y $A = \mathrm{Nu}(f) \oplus \mathrm{Im}(h)$. Probar que todo morfismo $f : A \to \mathbf{Z}$ de $\mathbf{Z}$-módulos se parte.

Ejercicio 6. Probar que no existe ninguna sucesión exacta (de $\mathbf{Z}$-módulos)

$$0 \to \mathbf{Z} \to L \to \mathbf{Q} \to 0$$

con L libre.

Ejercicio 7. Sea D un dominio de integridad y sea J un ideal de D. Probar que D/J es un D-módulo libre si, y sólo si, $J = 0$ ó $J = D$. ¿Vale el mismo resultado para D solamente conmutativo?

Ejercicio 8. Sea R un anillo conmutativo. Sea L un R-módulo libre. ¿Es cierto que todo conjunto linealmente independiente en L se extiende

a una base de L? Probar que n elementos $a_i = (a_{i1}, \ldots, a_{in})$ de $\mathbf{Z}^n$ forman una base si, y sólo si, $\det((a_{ij})) = \pm 1$. ¿Cómo se generalizaría esta afirmación a un dominio de integridad?

Ejercicio 9. ¿Es cierto que todo sumando directo de un módulo libre es libre? (Sugerencia: sea $R = \mathbf{Z} \oplus \mathbf{Z}$ con la estructura de anillo definida por $(x, y) \cdot (x', y') = (x \cdot x', y \cdot y')$. Considere el módulo libre R.)

Ejercicio 10. Probar que una suma directa arbitraria de módulos libres es un módulo libre. ¿Es la misma afirmación válida en el caso de un producto directo?

Ejercicio 11. Un R-módulo (a la izquierda) M se dirá *proyectivo* si para toda situación

$$\begin{array}{ccccc} & & M & & \\ & & \downarrow g & & \\ A & \xrightarrow{f} & A' & \longrightarrow & 0 \end{array}$$

con fila exacta, existe un morfismo $h : M \to A$, tal que $g = f \cdot h$.

i) Probar que todo módulo libre es proyectivo.

ii) Probar que todo sumando directo de un módulo libre es proyectivo.

ii') Recíprocamente, probar que si M es proyectivo, entonces M es sumando directo de un módulo libre.

iii) Sea $R = \mathbf{Z}_n$. Sea $n = r \cdot r'$, $(r, r') = 1$. Probar que $r \cdot \mathbf{Z}_n$ es un $\mathbf{Z}_n$-módulo proyectivo, pero no libre.

iv) Dar ejemplos de anillos, tales que todo ideal (a la izquierda) sea proyectivo. ¿Tienen los anillos de von Neumann esa propiedad?

v) Un anillo R con identidad se dice *semisimple* (clásico), si todo ideal es sumando directo de R. Probar que un anillo R es semisimple si, y sólo si, todo módulo cíclico es proyectivo. Determinar todos los anillos $\mathbf{Z}_n$ que sean semisimples. ¿Es $\mathbf{Z}$ semisimple? ¿Es $\mathbf{M}_n(K)$ semisimple, si K es un cuerpo? ¿Es $M_n(\mathbf{Z})$ semisimple?

vi) El siguiente resultado es válido, aunque no es fácil de demostrar. Sea D un dominio principal. Entonces todo submódulo de un módulo libre es libre. Como consecuencia, se sigue que un D-módulo es proyectivo si, sólo si, es libre. Los módulos proyectivos parecen ser la generalización *útil* de los espacios vectoriales. Decimos útil, puesto que la generalización *natural* de la noción de espacio vectorial es la de módulo libre. En la actualidad el desarrollo importante de una parte del álgebra y está centrado sobre este concepto.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 5

Ejercicio 1. Sea K un cuerpo. Probar que las condiciones siguientes sobre un K-módulo V son equivalentes entre sí:

i) V es un módulo artiniano.

ii) V es un módulo noetheriano.

iii) V posee dimensión finita como espacio vectorial sobre K.

Ejercicio 2. Sea K^n el K-espacio vectorial de n-uplas $(x_1, \ldots, x_n)$ con coeficientes en K. Calcular la dimensión y una base de los siguientes subespacios de V:

i) $\{(x_1, \ldots, x_n)/x_1 + \ldots + x_n = 0\}$

ii) $\{(x_1, \ldots, x_n)/x_1 + 2 \cdot x_2 + n \cdot x_n = 0\}$, si $1 < n$

iii) $\{(x_1, \ldots, x_n)/x_1 = x_2, 3x_2 = x_1\}$, si $1 < n$

iv) $\{(x_1, \ldots, x_n)/\sum_{i=1}^{n} (-1)^i \cdot x_i = 0\}$.

Ejercicio 3. Sea $K^{n \times n}$ el espacio vectorial sobre K de matrices de $n \times n$ con coeficientes en K. Calcular la dimensión y una base de los siguientes subespacios de V:

i) $\{((a_{ij}))/\sum_{i=1}^{n} a_{ii} = 0\}$

ii) $\{((a_{ij}))/\sum_{i=1}^{n} a_{ij} = 0,\ j = 1, \ldots, n\}$

iii) $\{((a_{ij}))/a_{ij} = -a_{ji},\ \sum_{j=1}^{n} a_{ij} = 0\}$.

Ejercicio 4. Sea R considerado como espacio vectorial sobre $\mathbf{Q}$.

i) Sea $d \in \mathbf{Q}$, tal que d no es cubo de ningún número racional. Probar que el conjunto $1, \sqrt[3]{d}, \sqrt[3]{d^2}$ es linealmente independiente sobre $\mathbf{Q}$.

ii) Sean $a, b, c, d \in \mathbf{Q}$. Probar que $a + \sqrt[3]{b} = c + \sqrt[3]{d}$ implica $u)$ $a = c$ y $b = d$ ó $v)$ b y d son cubos perfectos.

iii) Probar que $\mathbf{R}$ no posee dimensión finita sobre $\mathbf{Q}$.

Ejercicio 5. Sea V un espacio vectorial sobre un cuerpo K de dimensión finita. Probar que para un endomorfismo f de V las condiciones siguientes son equivalentes:

i) f es un automorfismo

ii) f es un monomorfismo

iii) f es un epimorfismo.

¿Es esencial la hipótesis sobre la dimensión de V?

Ejercicio 6. Sea V un espacio vectorial real de dimensión 2. Sea $\{e_1, e_2\}$ una base de V y sea θ un endomorfismo de V tal que

$$\theta(e_1) = 2e_1 - e_2, \ \theta(e_2) = e_1 + 3e_2.$$

Probar que no existe ningún vector $v \neq 0$ en V y ningún escalar $r \in \mathbf{R}$, tal que $\theta(v) = r \cdot v$.

Ejercicio 7. Sea $t = (t_1, \ldots, t_n) \in K^n$. Sea $\theta_t : K^{n\times n} \to K^{n\times n}$ la aplicación

$$\theta_t((a_{ij})) = ((\ (t_i - t_j) \cdot a_{ij})).$$

i) Probar que θ_t es un endomorfismo de $K^{n\times n}$

ii) Estudiar el núcleo de θ_t.

iii) Calcular $\mathrm{Nu}(\theta_t)$ en las situaciones siguientes $n=4$, $t=(1, 1, 2, 3)$, $t = (1, -1, 0, 2)$, $t = (1, 2, 2, 1)$.

iv) ¿Es para algún $t \in K^n$, θ_t un isomorfismo.

v) Probar que la aplicación $\theta : K^n \to \mathrm{End}_K(K^{n\times n})$, $\theta(t) = \theta_t$ es un morfismo. Calcular $\mathrm{Nu}(\theta)$ e $\mathrm{Im}(\theta)$.

Ejercicio 8. Sea θ un endomorfismo de un espacio vectorial V sobre un cuerpo K.

i) Sea $r \in K$. Sea $V_r = \{x / \theta(x) = r \cdot x\}$. Probar que V_r es un subespacio de V.

ii) Probar que si $r \neq s$, entonces $V_r \cap V_s = 0$.

iii) Sea $V = K^2$ y sea $\theta(e_1) = a_{11} \cdot e_1 + a_{12} \cdot e_2$, $\theta(e_2) = a_{21} \cdot e_1 + a_{22} \cdot e_2$, $a_{ij} \in K$, y donde e_1, e_2 es una base de V. Probar que $V_r \neq 0$ si, y sólo si, r es raíz del polinomio $X^2 - (a_{11} + a_{22}) \cdot X + (a_{11} \cdot a_{22} - a_{12} \cdot a_{21}) = 0$. Caracterizar los endomorfismos de K^2, tales que $K^2 = V_r \oplus V_s$.

Ejercicio 9. Sea U y V espacios vectoriales sobre el cuerpo K. Sea $\mathrm{Hom}_K(U, V)$ el K-espacio vectorial de K-endomorfismos de U en V. Probar que si U y V poseen ambos dimensión finita, entonces $\mathrm{Hom}_K(U, V)$ poseen dimensión finita igual a $\dim_K(U) \cdot \dim_K(V)$.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 6

Ejercicio 1. Probar que un dominio de integridad *finito* es un cuerpo.

Ejercicio 2. Probar que un dominio de integridad con un número finito de ideales es un cuerpo.

Ejercicio 3. Probar que los únicos dominios de integridad artinianos (es decir que como módulos sobre sí mismos son artinianos) son los cuerpos.

Ejercicio 4. Sea K un cuerpo de característica $\neq 2$. Probar que no existen en $K[X]$ polinomios u y v, tales que $(X^2 + 1) \cdot u^2 = v^2$.

Ejercicio 5. Sea R un anillo conmutativo con identidad $1 \neq 0$. Sea $R[X]$ el anillo de polinomios en la indeterminada X con coeficientes en R. Sea Y una indeterminada sobre $R[X]$. Sea $R[X][Y]$ el anillo de polinomios en Y con coeficientes en $R[X]$.

i) Probar que todo elemento de $R[X][Y]$ se escribe unívocamente en la forma $\sum_{i=0}^{n} a_i(X) \cdot Y^i$, donde $a_i(X) \in R[X]$.

ii) Sea X una indeterminada sobre $R[Y]$. Probar que la especialización $X \mapsto Y$, $Y \mapsto X$ de $R[X][Y] \to R[Y][X]$ es un isomorfismo *de anillos*. Por el mismo se identifica $R[X][Y]$ con $R[Y][X]$ y se escribe $R[X, Y]$.

iii) Probar que $R[X, Y]$ es un módulo R-libre con base $\{X^i \cdot Y^j\}$ $i, j \in \mathbf{N} \cup \{0\}$.

iv) Probar que $R[X, Y]$ es un dominio de integridad si, y sólo si, R lo es.

v) Sea K un cuerpo. Probar que $K[X, Y]$ *no* es un dominio principal.

vi) Probar que en $K[X, Y]$ existen ideales primos no maximales.

vii) ¿Cuáles son las unidades de $K[X, Y]$?.

Nota. Es posible probar que si K es un cuerpo, entonces $K[X, Y]$ es un dominio de factorización única (aun cuando no es principal).

viii) ¿Cuáles de los siguientes elementos de $\mathbf{Q}[X, Y]$ son extremales?

a) $2X^2 - 3XY - 9Y^2$

b) $X^2 + Y^2$

c) $2X - 4Y^2$

d) $X \cdot Y + 1$.

ix) Sea $\mathbf{C}$ el cuerpo complejo. ¿Es cierto que los únicos polinomios de $\mathbf{C}[X, Y]$ extremales son de la forma $aX + bY$, $a, b \in \mathbf{C}$?

x) Describir los anillos cocientes $\mathbf{Q}[X, Y]/\alpha$, donde α es el ideal generado por

a) X^2

b) X, Y

c) $X^2 - Y^2 - 1$

d) X.

Ejercicio 6. Sea p un primo racional. Sea $\mathfrak{p} = \mathrm{End}_{\mathbf{I}}(\mathbf{Z}_{p^\infty})$ el anillo de endomorfismos de $\mathbf{Z}_{p^\infty}$.

i) Sea $\mathcal{P}$ la totalidad de morfismos $f \in \mathfrak{p}$, tales que $\mathrm{Nu}(f) \neq 0$. Probar que $\mathcal{P}$ es un ideal bilátero.

ii) Probar que $\mathfrak{p}$ es un anillo conmutativo.

iii) Probar que si α es un ideal de $\mathfrak{p}$, entonces $\alpha \subset \mathcal{P}$, o sea $\mathfrak{p}$ es un *anillo local* de ideal maximal $\mathcal{P}$.

iv) Probar que $\mathfrak{p}$ es un dominio de integridad.

v) Sea $f \in \mathfrak{p}$. Sea, para cada $i \in \mathbf{N}$, e_i un generador de $\mathbf{Z}_{p^i}$, tal que $e_i = p \cdot e_{i+1}$. Entonces $f(e_i) = f_i \cdot e_i$, $f_i \in \mathbf{Z}$. Probar que f esta unívocamente determinado por la familia de enteros

$$f_1, f_2, \ldots, f_n, \ldots$$

con la propiedad

$$f_{i+1} \equiv f_i \mod p^i.$$

vi) Probar que todo elemento f de $\mathfrak{p}$ se escribe unívocamente en la forma $f = (a_0, a_1, \ldots)$ con $0 \leq a_i < p$. Se suele escribir $f = \sum_{i=0}^{\infty} a_i \cdot p^i$ (formalmente).

vii) Probar que los elementos de $\mathfrak{p}$, con $a_0 = 0$, caracterizan $\mathcal{P}$.

viii) Probar que el elemento $p = 0 + 1 \cdot p + 0 \cdot p^2 + \ldots$ es generador de $\mathcal{P}$ y, además, que los únicos ideales de $\mathcal{P}$ son de la forma

$$\mathcal{P} = \langle p \rangle \supset \mathcal{P}^2 = \langle p^2 \rangle \supset \mathcal{P}^3 = \langle p^3 \rangle \supset \ldots$$

Deducir que $\mathfrak{p}$ es un dominio principal. Probar que $\mathfrak{p}/\mathcal{P}^i \simeq \mathbf{Z}p^i$, $i \in \mathbf{N}$.

Nota. $\mathfrak{p}$ se denomina el anillo de enteros p-ádicos. Su cuerpo de cocientes se denomina el *cuerpo p-ádico*. Es imposible exagerar la importancia de las estructuras p-ádicas en la teoría algebraica de números y geometría algebraica. Referencias (2), (21b).

Ejercicio 7. Es cierto que en un dominio de integridad, todo elemento extremal genera un ideal primo? (Sugerencia: sea $D = \mathbf{Z}[\sqrt{-5}]$, notar que $2 \cdot 3 = 6 = (1 - \sqrt{-5}) \cdot (1 + \sqrt{-5})$.)

Ejercicio 8. ¿Existen dominios de integridad sin elementos extremales?

Ejercicio 9. Determinar, en $\mathbf{Z}[i]$, el máximo común divisor de

i) $3 - i$ y $2 + 5i$;

ii) 4 y $2i$

iii) 1 e i

iv) $1 + i$ y $2i$

v) $2 + 3i$ y $12 + 5i$.

Ejercicio 10. ¿Contradicen las factorizaciones

$$13 = (2 + 3i) \cdot (2 - 3i) = (-3 - 2i) \cdot (-3 - 2i)$$

el carácter de dominio de factorización única de $\mathbf{Z}[i]$?.

Ejercicio 11. Analizar el carácter extremal de

i) $1 + i$, $1 - i$, 67, 97 en $\mathbf{Z}[i]$

ii) $1 + \sqrt{2}$, $\sqrt{2}$, 41, $3 + 2\sqrt{2}$ en $\mathbf{Z}[\sqrt{2}]$

Ejercicio 12. Escribir $1 + 2 \cdot \sqrt{-2}$ como producto de elementos extremales en $\mathbf{Z}[\sqrt{-2}]$.

Ejercicio 13. Llevar, por operaciones de filas y columnas, a la forma diagonal canónica (o sea $\mathrm{diag}(d_1, \ldots, d_n)$, $d_i \neq 0$, $i \leq j \Rightarrow d_i / d_j$) las matrices

i) En $\mathbf{Z}$:

$$\begin{Vmatrix} 2 & 0 \\ 0 & 3 \end{Vmatrix}, \quad \begin{Vmatrix} -1 & -2 \\ 1 & 0 \end{Vmatrix}, \quad \begin{Vmatrix} 0 & 1 \\ 0 & 0 \end{Vmatrix}, \quad \begin{Vmatrix} 2 & 4 \\ 6 & 10 \end{Vmatrix}$$

ii) En $\mathbf{Z}[i]$

$$\begin{Vmatrix} i & 1+i \\ -2 & 2 \end{Vmatrix}, \quad \begin{Vmatrix} 2 & -i \\ 3 & i \end{Vmatrix}, \quad \begin{Vmatrix} 1+i & 1 \\ 1 & 1-i \end{Vmatrix}$$

iii) En $\mathbf{Q}[X]$

$$\begin{Vmatrix} X-1 & 1 \\ 3 & X-1 \end{Vmatrix}, \quad \begin{Vmatrix} X^2+1 & 0 \\ 0 & X+1 \end{Vmatrix}, \quad \begin{Vmatrix} X-4 & 0 \\ 3 & X+5 \\ 3 & 6 \end{Vmatrix}, \quad \begin{Vmatrix} 0 \\ 0 \\ X-1 \end{Vmatrix},$$

$$\begin{Vmatrix} X & 1 & 0 \\ 0 & X & 1 \\ 0 & 0 & X \end{Vmatrix}$$

Ejercicio 14. Sea $A = \prod_{i \in N} \mathbf{Z}_{p^i}$, p primo racional. Caracterizar tA. Probar que $\bigoplus_{i \in N} \mathbf{Z}_{p^i} \subset tA$. ¿Es estricta la inclusión? Es el cociente

$$\frac{\prod_{i \in N} \mathbf{Z}_{p^i}}{\bigoplus_{i \in N} \mathbf{Z}_{p^i}}$$

un grupo abeliano divisible? Probar que $\bigoplus_{i \in N} \mathbf{Z}_{p^i}$ no es sumando directo de $\prod_{i \in N} \mathbf{Z}_{p^i}$. (Sug.: En el cociente hay elementos $\neq 0$ divisibles por p^n, para todo $n \in N$.)

Ejercicio 15. Sea π un elemento extremal de un dominio de integridad D. Sea A un π-módulo. Probar que si π' es un elemento extremal de D con $\pi \neq \pi'$, entonces la homotecia $h_{\pi'}$ de A en un epimorfismo. Deducir que A es divisible por todo elemento extremal $\neq \pi$.

Ejercicio 16. Sea A un módulo divisible. Probar que tA es un módulo divisible. (Ignoramos si en general tA es sumando directo de A, aunque todo módulo divisible sobre un dominio principal es sumando directo de todo módulo que lo contiene como submódulo.)

Ejercicio 17. Sea A un grupo abeliano divisible. Sea $tA = 0$. Probar que A es suma directa de subgrupos abelianos todos isomorfos a $\mathbf{Q}$. (Sugerencia: Sea $q \in \mathbf{Z}$, $q \neq 0$. La homotecia h_q es un automorfismo. Definiendo $\frac{m}{q} \cdot a = m \cdot h_q^{-1}(a)$, se obtiene sobre A una estructura de $\mathbf{Q}$-espacio vectorial. Usar ahora el hecho que todo espacio vectorial posee una base.) Por lo tanto, los grupos abelianos divisibles sin torsión están caracterizados por su dimensión como $\mathbf{Q}$-espacio vectorial.

Ejercicio 18. Sea D un dominio de integridad. Sean A y C, D-módulos. Probar

i) Si A es divisible, entonces $\mathrm{Hom}_D(A, C)$ es sin torsión.

ii) Si C es sin torsión, entonces $\mathrm{Hom}_D(A, C)$ es sin torsión.

iii) Si A es de torsión, entonces $\mathrm{Hom}_D(A, C)$ es reducido.

iv) Si C es reducido, entonces $\mathrm{Hom}_D(A, C)$ es reducido.

v) Si A es divisible y C reducido, entonces $\mathrm{Hom}_D(A, C) = 0$.

vi) Si A es de torsión y C es sin torsión, entonces $\mathrm{Hom}_D(A, C) = 0$.

Ejercicio 19. Sean $\mathbf{Q}^* = U(\mathbf{Q})$, $C^* = U(C)$ los grupos multiplicativos de unidades de $\mathbf{Q}$ y C. P la totalidad de primos racionales.

i) Probar que C^* es (en notación multiplicativa) un grupo abeliano divisible.

ii) Probar que no existe ningún epimorfismo de C^* en $\mathbf{Q}^*$.

iii) Probar que $\mathbf{Q}^*$ es (en notación multiplicativa) isomorfo a $\mathbf{Z}_2 \oplus (\oplus_P \mathbf{Z})$ (Sugerencia: Utilizar el teorema fundamental de la aritmética.) Por lo tanto, $t\mathbf{Q}^* \simeq \mathbf{Z}_2$.

iv) Probar que el único morfismo de C^* en $\mathbf{Q}^*$ es el trivial.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 7

Ejercicio 1. Un módulo A se dice indescomponible, si 0 y A son sus únicos sumandos directos. Probar que si D es un dominio principal y A es un módulo de tipo finito, entonces A es indescomponible si, y sólo si, A es isomorfo a uno de los módulos siguientes $D/\langle \pi^1 \rangle$, π extremal o D.

Ejercicio 2. Un módulo de tipo finito sobre un dominio principal D es tal que todo submódulo del mismo es sumando directo si, y sólo si, es isomorfo a una suma directa finita de módulos del tipo $D/\langle \pi \rangle$ con π extremal.

Ejercicio 3. Determinar los divisores elementales y los factores invariantes de los grupos abelianos siguientes

i) $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$

ii) $\mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_{10}$

iii) $\mathbf{Z}_8 \oplus \mathbf{Z}_8 \oplus \mathbf{Z}_{11}$

iv) $\mathbf{Z}_{21} \oplus \mathbf{Z}_{18}$

v) $\mathbf{Z}_2 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_7 \oplus \mathbf{Z}_{70}$.

Ejercicio 4. Determinar los factores invariantes de los grupos abelianos siguientes

i) $\mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z} \oplus \mathbf{Z}$

ii) $\mathbf{Z}_4 \oplus \mathbf{Z}_8 \oplus \mathbf{Z}_9 \oplus \mathbf{Z} \oplus \mathbf{Z}$

iii) $\mathbf{Z}_{12} \oplus \mathbf{Z}_{21} \oplus \mathbf{Z}$.

Ejercicio 5. Determinar los factores invariantes de los grupos abelianos definidos por generadores y relaciones siguientes:

i) A es el grupo abeliano con generadores $\{e_1, e_2\}$, que satisfacen las relaciones $3e_1 = 4e_2$.

ii) A es el grupo abeliano con generadores e_1, e_2, e_3, que satisfacen las relaciones $2e_1 + 2e_2 + 2e_3 = 0$, $3e_1 = 6e_3$.

iii) A es el grupo abeliano con generadores e_1, e_2, e_3, que satisfacen las relaciones $3e_1 = e_2$, $e_2 = 3e_3$.

Ejercicio 6. Determinar todas las clases de isomorfismos de grupos abelianos de órdenes 8, 16, 180, 210, respectivamente.

Ejercicio 7. Sea A un grupo abeliano de orden n.

i) Si r es divisor de n, $r \in \mathbf{N}$, entonces A posee subgrupos de orden r. Si r es primo, entonces A posee elementos de orden r.

ii) Si $a \in A$ posee orden maximal (entre las posibles órdenes de elementos de A), entonces a genera un sumando directo de A.

iii) Si n es libre de cuadrados, vale decir, si d^2/n implica $d^2 = 1$, entonces A es cíclico.

Ejercicio 8. Sean A y B grupos abelianos de tipo finito. Probar que si existe un isomorfismo $A \oplus A \simeq B \oplus B$, entonces $A \sim B$.

Ejercicio 9. Sean A, B, C grupos abelianos de tipo finito. Probar que si existe un isomorfismo $A \oplus B \simeq A \oplus C$, entonces $B \simeq C$.

Ejercicio 10. Sean A y B grupos abelianos de tipo finito. Probar que si existen monomorfismos $f: A \to B$, $g: B \to A$, entonces A y B son isomorfos. Analizar el caso infinito con $A = \oplus^N \mathbf{Z}_4$, $B = \mathbf{Z}_2 \oplus (\oplus^N \mathbf{Z}_4)$.

Ejercicio 11. Sea A un grupo abeliano. Probar que si en A hay elementos de órdenes n y m, entonces A contiene un elemento de orden $[n,m]$.

Ejercicio 12. Probar que si p es primo, todo sumando directo $\neq 0$ de $\mathbf{Z}_{p^n} \oplus \ldots \oplus \mathbf{Z}_{p^n}$ es isomorfo a una suma directa de $\mathbf{Z}_{p^n}$.

Ejercicio 13. Sea K un cuerpo finito de característica p. Sea $K^* = K - \{0\} = U(K)$.

152

i) Probar que K posee p^n elementos. (Sugerencia: Notar que K es un $\mathbf{Z}_p$- espacio vectorial.)

ii) Probar que K^* es un grupo cíclico.

iii) Sea $n \in N$. Calcular el orden del subgrupo K^{*n} de K^* de potencias n-simas (o sea, el subgrupo imagen por la aplicación $x \to x^n$ de K^* en K^*). (Sugerencia: Analice la situación aditiva $n \cdot \mathbf{Z}_n$.) Hallar el orden del subgrupo de K^* de raíces n-simas de 1. Calcule K^{*2}, K^*/K^{*2}.

iv) Probar que en $\mathbf{Z}_p$, $x^2 = -1$ si, y sólo si, p es primo de la forma $4m + 1$ ó $p = 2$. Probar que si un primo racional impar es suma de dos cuadrados en $\mathbf{Z}$, entonces p es de la forma $4m + 1$. La recíproca es también cierta.

v) Construir cuerpos de 4 y 9 elementos y determinar los subgrupos K^{*n}.

vi) Probar que dos cuerpos finitos son isomorfos si, y sólo si, poseen el mismo número de elementos.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 8

En esta sección, K denotará un cuerpo conmutativo. Los espacios vectoriales serán de dimensión finita sobre K.

Ejercicio 1. Sea $0 \neq p(X) \in K[X]$, grado $p(X) = m$. Probar que $K[X]/\langle p(X)\rangle$, como K-espacio vectorial posee dimensión m. Probar que las clases de $1, X, \ldots, X^{m-1}$ forman una base.

Ejercicio 2. Sea $\theta : \Omega^2 \to \Omega^2$ un endomorfismo, tal que respecto de una base e_1, e_2 de Ω^2

$$\theta(e_1) = e_2, \quad \theta(e_2) = 2e_1 - e_2.$$

Calcular m_θ, χ_θ. Determinar todos los submódulos de $(\Omega^2)_\theta$. Es $(\Omega^2)_\theta$ un módulo cíclico?

Ejercicio 3. Un endomorfismo de un espacio vectorial V sobre K se dice *semisimple*, si todo subespacio estable posee un subespacio estable suplementario (o sea, si W es estable, existe U estable con $V = U \oplus W$). Caracterizar los endomorfismos semisimples de Ω^2, Ω^3, Ω^4. Probar que si σ es un endomorfismo nilpotente (o sea, $\sigma^m = 0$ para algún $m \in \mathbf{N}$) y es, además, semisimple, entonces $\sigma = 0$.

Ejercicio 4. Dar una condición necesaria y suficiente para que un endomorfismo σ de un espacio vectorial satisfaga $m_\sigma = \chi_\sigma$. Ilustrar con ejemplos en $V = \Omega^2$.

Ejercicio 5. Sea V un espacio vectorial sobre el cuerpo complejo $\mathbf{C}$. Sea un $\mathbf{C}$-endomorfismo, tal que $\sigma^n = \mathrm{id}$. Probar que existe en V una base respecto de la cual σ es diagonal.

Ejercicio 6. Sea σ un endomorfismo de Ω^3, tal que respecto de alguna base se representa en forma matricial

$$\begin{Vmatrix} 4 & 6 & 0 \\ -3 & -5 & 0 \\ -3 & -6 & 1 \end{Vmatrix}.$$

Hallar la forma canónica clásica y la forma canónica de Jordan de σ. Resolver el mismo problema para las situaciones siguientes

$$\begin{Vmatrix} 3 & 0 & 8 \\ -3 & 0 & -5 \\ 3 & -1 & 6 \end{Vmatrix} \quad \begin{Vmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{Vmatrix} \quad \begin{Vmatrix} 2 & 1 & -1 \\ 0 & 3 & 1 \\ 0 & 0 & -2 \end{Vmatrix}$$

Ejercicio 7. Dar ejemplos de espacios vectoriales V y endomorfismos σ y τ de V, tales que $m_\sigma = m_\tau$, $\chi_\sigma = \chi_\tau$, pero V_σ y V_τ no son isomorfos.

Ejercicio 8. Determinar todas las clases de isomorfismos de módulos sobre $\mathbf{C}[X]$ que como espacio vectorial complejo poseen dimensión 2. Análogo problema para dimensiones 3 y 4.

Ejercicio 9. Determinar todas las clases de isomorfismos de módulos sobre $\mathbf{Q}[X]$, definidos por endomorfismos nilpotentes, que como espacios vectoriales sobre $\mathbf{Q}$ poseen dimensión 2. Análogo problema para dimensiones 3 y 4.

Ejercicio 10. Hallar la forma canónica clásica y la forma canónica de Jordan de un endomorfismo nilpotente.

Ejercicio 11. Sea σ un endomorfismo de un espacio vectorial V sobre un cuerpo de característica 0. Probar que σ es nilpotente si, y sólo si, $\mathrm{Tr}(\sigma^i) = 0$ para $i = 1, \ldots, \dim_K(V)$.

Ejercicio 12. Determinar todas las formas canónicas de Jordan de endomorfismos de $\mathbf{Q}^2, \mathbf{R}^2, \mathbf{C}^2, \mathbf{C}^3, \mathbf{C}^4$. Análogamente para $\mathbf{Z}_2^2, \mathbf{Z}_2^3, \mathbf{Z}_2^4, \mathbf{Z}_5^2$.

ÍNDICE DE NOTACIONES

N, Z, Q, R, C : conjuntos de números naturales, enteros, racionales, reales, complejos, respectivamente.

$[\![1, n]\!], n \in \mathbf{N}$: intervalo natural inicial, $[\![1, n]\!] = \{t \mid t \in \mathbf{N} \text{ y } 1 \leq t \leq n\}$.

n/m : n divide a m.

$n \not/ m$: n no divide a m.

(n, m) : máximo común divisor de n y m.

$[n, m]$: mínimo común múltiplo de n y m.

δ_{ij} : delta de Kronecker $\delta_{ij} = 0$ si $i \neq j$, $\delta_{ii} = 1$.

$\mathbf{Q}/\mathbf{Z}$: grupo abeliano cociente de $\mathbf{Q}$ por el subgrupo $\mathbf{Z}$.

$\mathbf{Z}_n$: anillo de restos módulo n.

$\mathbf{Z}_{p^\infty}$: grupo abeliano límite de la cadena $\mathbf{Z}_p \subset \mathbf{Z}_{p^2} \subset \mathbf{Z}_{p^3} \subset \ldots$

$\mathbf{U}(R)$: grupo de unidades del anillo R.

$\mathbf{M}_n(R)$: anillo completo de matrices de n filas por n columnas con coeficientes en R.

$I_n \in \mathbf{M}_n(R)$: matriz identidad.

$\det(a)$: determinante de a.

$\mathrm{Tr}(a)$: traza de a.

$\mathrm{diag}(a_1, \ldots, a_n) \in \mathbf{M}_n(R)$: matriz diagonal, $a_{ij} = 0$ si $i \neq j$, $a_{ii} = a_i$.

$\mathbf{GL}(n, R)$: grupo general lineal de grado n sobre R.

Sea $f : A \to B$ una aplicación. Sea $A' \subset A$. Entonces $f \mid A'$ denota la restricción de f a A'.

id_A : aplicación identidad de A.

$\mathrm{Nu}(f)$: núcleo de f.

$\mathrm{Im}(f)$: imagen de f.

$\mathrm{Hom}_R(A, B)$: conjunto de R-morfismos de A en B.

$\mathrm{End}_R(A)$: conjunto de R-morfismos de A en A.

$\langle a \rangle$: submódulo generado por a.

$\langle a_1, \ldots, a_n \rangle$: submódulo generado por $a_1, \ldots, a_n$.

$\sum_i A_i$: suma de la familia $\{A_i\}$.

$\sum_{i \oplus} A_i$: suma directa interna.

$\oplus_\iota A_\iota$: suma directa externa de la familia A_ι.

$\prod_\iota A_\iota$: producto directo de la familia A_ι.

$A_1 \oplus \ldots \oplus A_n$: suma directa de la familia finita $A_1, \ldots, A_n$.

$A^n = A \oplus \ldots \oplus A$: (n sumandos).

D : dominio de integridad.

Q : cuerpo de cocientes de D.

π : elemento extremal.

P : totalidad de elementos extremales de D.

A_π : componente π-primaria.

tA : submódulo de torsión.

δA : submódulo de elementos divisibles.

$K[X]$: anillo de polinomios en X con coeficientes en K.

$\mathbf{Z}[i]$: anillo de enteros de Gauss.

$\mathbf{Q}(\sqrt{a})$: extensión cuadrática de $\mathbf{Q}$.

$\mathbf{Z}[\sqrt{a}]$: anillo de enteros algebraicos de $\mathbf{Q}(\sqrt{a})$.

$N(z)$: norma de z.

$m^i(k)$, p^{ij}, $t^{ij}(k)$: matrices elementales.

D_{π^i} : módulo cociente $D/\langle \pi^i \rangle$.

D_{π^∞} : módulo límite de la cadena $D_\pi \subset D_{\pi^2} \subset D_{\pi^3} \subset \ldots$

V_σ : estructura de $K[X]$-módulo definida sobre V por $\sigma \in \in \mathrm{End}_K(V)$.

$m_\sigma(X)$: polinomio minimal de σ.

$\chi_\sigma(X)$: polinomio característico de σ.

BIBLIOGRAFÍA

(1) BASS, H. Algebraic K-theory, Benjamin, Nueva York, N. Y. (1968).

(2) BOREVICH, Z. y SHAFAREVICH, I. Number Theory, Academic, Nueva York, N. Y. (1966).

(3) BOURBAKI, N. a) Algèbre, Modules sur les Anneaux principaux, Chap. VII, Hermann, París (1964).

b) Algèbre, Modules et Anneaux semisimples, Chap. VIII, Hermann, París (1958).

c) Algèbre, Algèbre linéaire, Chap. II, Hermann, París (1967).

(4) CARTAN, H. y EILENBERG, S. Homological Algebra, Princeton University Press, Princeton, Nueva Jersey (1956).

(5) CHEVALLEY, C. Fundamental Concepts of Algebra, Academic, Nueva York, N. Y. (1956).

(6) CURTISS, CH. y REINER, I. Representation Theory of Finite Groups and Associative Algebras, Interscience, Nueva York, N. Y. (1962).

(7) FUCHS, L. a) Abelian Groups. Pergamon, Londres (1960).
b) Infinite Abelian Groups, Vol. I., Academic, Nueva York, N.Y. (1970).

(8) GENTILE, E.R. a) Estructuras Algebraicas, monografía científica No. 3, serie de matemática, Organización de los Estados Americanos, Washington, D.C. (1967).

b) Notas de Álgebra, Cursos y Seminarios de Matemática, Universidad de Buenos Aires, Buenos Aires, Argentina (1965).

(9) GODEMENT, R. Cours d'Algèbre, Hermann, París (1963).

(10) GRIFFITH, A. Infinite Abelian Group Theory, University of Chicago Press, Chicago, Illinois (1970).

(11) HARDY, G. y WRIGHT, E. An Introduction to the Theory of Numbers, Oxford University Press, Londres (1960).

(12) HOFFMAN, K. y KUNZE, R. Linear Algebra, Prentice Hall, Englewood Cliffs, Nueva Jersey (1962).

(13) JACOBSON, N. Lectures in Abstract Algebra, Vols. I y II, Van Nostrand, Princeton, Nueva Jersey (1953).

(14) JANS, J. Rings and Homology, Holt, Rinehart & Winston, Nueva York, N. Y. (1964).

(15) KAPLANSKY, I. Infinite Abelian Groups, University of Michigan Press, Ann Arbor, Michigan (1956).

(16) LANG, S. Algebra, Addison-Wesley, Reading, Massachusetts (1965).

(17) MACLANE, S. y BIRKHOFF, G. Algebra, MacMillan, Nueva York, N.Y. (1967).

(18) POLLARD, H. The Theory of Algebraic Numbers, Carus Mathematical Monographs No.9, Mathematical Association of America (1950).

(19) ROBINSON, A. Numbers and Ideals, Holden-Day, San Francisco, California (1965).

(20) SAMUEL, P. Théorie algébrique des Nombres, Collection Méthodes, Hermann, París (1967).

(21) SERRE, J.P. a) Representations lineaires des Groupes finis, Collection Méthodes, Hermann, París (1967).

b) Cours d'Arithmétique, Presses Universitaires de France, (1970).

(22) VAN DER WAERDEN, B. Modern Algebra, Vols. I y II, Ungar, Nueva York, N.Y. (1949).

(23) WEISS, E. Algebraic Number Theory, McGraw, Nueva York, N.Y. (1963).

(24) ZARISKI, O. y SAMUEL, P. Commutative Algebra, Vol. I, Van Nostrand, Princeton, Nueva Jersey (1958).

Notas sobre la Bibliografía

La teoría general de módulos está expuesta sistemáticamente en las obras citadas en las referencias (3c), (5), (9) que pueden servir además para ampliar los conocimientos sobre el tema. Para tratamientos más formales y que utilizan las nociones de categorías y funtores, consúltese (1) y también (17). Para estudiar el producto tensorial, se aconseja (3c), (5) y (7b). En (8b) se trata el producto tensorial de grupos abelianos.

Se recomienda al lector que luego de la lectura de la monografía estudie con cuidado dos temas importantes: a) grupos abelianos, para lo cual las obras citadas en (15), (7a) y (7b) son excelentes referencias, y b) teoría algebraica de números, como fuente de ejemplos importantes de anillos (además de sus amplias cualidades intrínsecas). Para ello véase (20), (19), (18), (2), (21b) y (23), así como (24) y (16). La teoría de módulos sobre un dominio principal se estudia en el volumen II de (13) y en (3a), al igual que sus aplicaciones a la teoría de una transformación lineal. Respecto a esto último, véase también (12).

COLECCIÓN DE MONOGRAFÍAS CIENTÍFICAS

Publicadas

Serie de matemática

N° 1. La Revolución en las Matemáticas Escolares, por el Consejo Nacional de Maestros de Matemáticas de los Estados Unidos de América.
N° 2. Espacios Vectoriales y Geometría Analítica, por Luis A. Santaló.
N° 3. Estructuras Algebraicas, por Enzo R. Gentile.
N° 4. Historia de las Ideas Modernas en la Matemática, por José Babini.
N° 5. Álgebra Lineal, por Orlando Villamayor.
N° 6. Álgebra Linear e Geometria Euclidiana, por Alexandre Augusto Martins Rodrigues.
N° 7. El Concepto de Número, por César A. Trejo.
N° 8. Funciones de Variable Compleja, por José I. Nieto.
N° 9. Introducción a la Topología General, por Juan Horváth.
N° 10. Funções Reais, por Djairo G. de Figueiredo.
N° 11. Probabilidad e Inferencia Estadística, por Luis A. Santaló.
N° 12. Estructuras Algebraicas, II, por Enzo R. Gentile.

Serie de física

N° 1. Concepto Moderno del Núcleo, por D. Allan Bromley.
N° 2. Panorama de la Astronomía Moderna, por Félix Cernuschi y Sayd Codina.
N° 3. La Estructura Electrónica de los Sólidos, por Leopoldo M. Falicov.
N° 4. Física de Partículas, por Igor Saavedra.
N° 5. Experimento, Razonamiento y Creación en Física, por Félix Cernuschi.
N° 6. Semiconductores, por George Bemski.
N° 7. Aceleradores de Partículas, por Fernando Alba Andrade.
N° 8. Física Cuántica, por Onofre Rojo y Harold McIntosh.

Serie de química

N° 1. Cinética Química Elemental, por Harold Behrens Le Bas.
N° 2. Bioenergética, por Isais Raw y Walter Colli.
N° 3. Macromoléculas, por Alejandro Paladini y M. Burachik.
N° 4. Mecanismo de las Reacciones Orgánicas, por Jorge A. Brieux.
N° 5. Elementos Encadenados, por Jacobo Gómez Lara.
N° 6. Enseñanza de la Química Experimental, por Francisco Giral.

Serie de biología

N° 1. La Genética y la Revolución en las Ciencias Biológicas, por José Luis Reissig.

N° 2. Bases Ecológicas de la Explotación Agropecuaria en la América Latina, por Guillermo Mann F.
N° 3. La Taxonomía y la Revolución en las Ciencias Biológicas, por Elías R. de la Sota.
N° 4. Principios Básicos para la Enseñanza de la Biología, por Oswaldo Frota-Pessoa.
N° 5. A Vida da Célula, por Renato Basile.
N° 6. Microorganismos, por J. M. Gutiérrez-Vázquez.
N° 7. Principios Generales de Microbiología, por Norberto J. Palleroni.
N° 8. Los Virus, por Enriqueta Pizarro-Suárez y Gamba.

En preparación

Serie de matemática

La Revolución en las Matemáticas Escolares (Segunda Fase), por Howard F. Fehr y colaboradores.
Teoría de los Grupos, por Horacio O'Brien.

Serie de física

Radiación Cósmica, por Gastón Mejía y Carlos Aguirre.

Serie de química

Temas Modernos de Química Inorgánica, por Rubén Levitus.
Complejos, por Carlos Andrade.
Fotoquímica de Moléculas Sencillas, por Ralf Penzhorn.
Introducción a la Geoquímica, por Félix González Bonorino.

Serie de biología

Biosíntesis de Proteínas y el Código Genético, por Jorge E. Allende.
Elementos de Inmunología e Inmunoquímica, por Félix Córdoba y Sergio Estrada-Parra.
Introducción a la Ecología del Bentos Marino, por Manuel Vegas Vélez.
Inventario de Vegetación de Biomas, por Jorge Morello.
Los Sistemas Ecológicos y el Hombre, por Francesco di Castri.
Biogeografía de América Latina, por Angel L. Cabrera y Abraham Willink.
Introdução a Genética Humana, por P. H. Saldanha.
La Selva Tropical, por Arturo Gómez-Pompa.
Fermentaciones, por Carlos del Río E.
Procesos Microbianos Aerobios de Importancia Industrial, por Carlos Casas Campillo.

Nota. Las personas interesadas en adquirir estas obras deben dirigirse a la División de Ventas y Promoción, Organización de los Estados Americanos, Washington, D. C. 20006, o a las Oficinas Nacionales de la OEA en el país respectivo.