TEOREMA DE DESCOMPOSICIÓN DE MÓDULOS SOBRE DOMINIOS DE IDEALES PRINCIPALES

LINA PAOLA ARTEAGA GENES

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE CIENCIAS BÁSICAS
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
MONTERÍA
2020

TEOREMA DE DESCOMPOSICIÓN DE MÓDULOS SOBRE DOMINIOS DE IDEALES PRINCIPALES

LINA PAOLA ARTEAGA GENES

Trabajo presentado como requisito parcial para optar al título de
Matemático

Asesor:
M. Sc. RICARDO MIGUEL GUZMÁN NAVARRO

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE CIENCIAS BÁSICAS
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
MONTERÍA
2020

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE CIENCIAS BÁSICAS
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA

Los jurados abajo firmantes certifican que han leído y que aprueban el trabajo de grado titulado: **TEOREMA DE DESCOMPOSICIÓN DE MÓDULOS SOBRE DOMINIOS DE IDEALES PRINCIPALES** , el cual es presentado por el estudiante **LINA PAOLA ARTEAGA GENES**.

Fecha: Mayo de 2020

Asesor: Ricardo Guzman
M. Sc. RICARDO MIGUEL GUZMÁN NAVARRO

Jurado: Jerson Borja S.
JERSON MANUEL BORJA SOTO

Jurado:
LUIS ENRIQUE BENÍTEZ BABILONIA

A Dios por manifestarse en mi vida como un padre lleno de misericordia

Y a mis padres: Carmen Maria Genes Oviedo, Fabio Enrique Arteaga Herrera

Resumen

En este trabajo se realiza un estudio introductorio a la teoría de módulos, una estructura definida de manera análoga a la de espacio vectorial, reemplazando al cuerpo por un anillo.

En primer lugar se conocerán definiciones, notaciones, resultados claves y necesarios que nos ayudarán a entender la estructura de los módulos finitamente generados (M.F.G) sobre dominios de ideales principales (D.I.P). Este proyecto se centrará más que todo en la teoría de módulos, usando como herramienta principal la teoría de anillos y teoría de grupos.

Finalmente veremos una aplicación del teorema de descomposición de módulos sobre D.I.P en la forma canónica de Jordan y Racional. Es decir, se hará una relación de un resultado importante de la teoría de módulos a estructuras que hacen parte del álgebra lineal.

Abstract

In this work an introductory study of module theory is made. A module is a structure defined analogously to a vectorial space but replacing the field by a ring. First, we provide some definitions, notations, and key necessary results which are going to help us with the understanding of the structure of finite generated modules (F.G.M) over a principal ideal domain (P.I.D). The focus of this project is the study of module theory, principally by using tools like ring theory and group theory. Finally, an application of the module decomposition theorem over P.I.D. to the Jordan and rational normal forms is presented, i.e. we are going to establish a connection between an important theorem of module theory and some linear algebra structures.

Agradecimientos

Primero que todo, quiero darle gracias a Dios, por manifestarse en mi vida como un padre lleno de bondad y misericordia, por haber puesto en mi camino personas que de una u otra forma contribuyeron con este logro. A mis padres CARMEN MARÍA GENES OVIEDO Y FABIO ENRIQUE ARTEAGA HERRERA, los cuales fueron, son y serán mi fuente de inspiración, motivación, ejemplo a seguir; ellos que siempre me enseñaron a levantarme en cada caída y siempre insisten en mostrarme el mundo real, el mundo donde te estrellas 100 veces y debes pararte 101. A mis hermanos Vanessa, Arnaldo, Yulis y Key, ellos nunca perdieron la fé en mi y siempre me dan una voz de aliento; a Consuelo Hoyos mi segunda madre. A la institución UNIVERSIDAD DE CÓRDOBA que a pesar de no ser la más lujosa, la calidad humana y académica abundan. Hablando de calidad académica, quiero agradecer a los profesores del Departamento de Matemáticas y Estadística de la Facultad de Ciencias Básicas de la Universidad de Córdoba y en especial al profesor RICARDO MIGUEL GUZMÁN NAVARRO por haber creído en mí, por ser ese guía, amigo, compañero idóneo e incondicional, a los profes Segio Avilez, Reyes, Lloreda, Benitez, Borja, Banquet, Galeano y todos aquellos que pusieron ese granito de arena para que este sueño sea una realidad, como olvidarme de Taima Miranda siempre apoyando nuestro crecimiento. Por último, pero no menos importante, mis amigos en especial a Lina Delvis, mi Lu, mi Pao, mi Mary, Herlunchis, mi Camy, Mayito, Martha Villegas, la familia Hodeg Peña, Gomez Oviedo y bueno la lista es larga no terminaré de mensionarlos a todos, con ellos he vivido los mejores momentos de mi vida

Montería, Colombia LINA PAOLA ARTEAGA GENES

Mayo de 2020

Índice general

Introducción

En este trabajo queremos determinar la estructura de los módulos finitamente generados (M.F.G) sobre dominios de ideales principales (D.I.P). Se dará a conocer que todo M.F.G puede ser descompuesto de dos formas como suma directa de submódulos cíclicos. Cada una de las descomposiciones genera un conjunto de invariantes para el módulo en estudio, es decir, dos módulos son isomorfos si y sólo si comparten los mismos factores invariantes. Cada método de descomposición lleva a una clasificación completa de los M.F.G sobre D.I.P (salvo isomorfismos).

Aclaramos que los módulos a considerar son unitarios.

El cuerpo del trabajo está compuesto por tres capítulos. El primer capítulo se centra más que todo en la teoría de anillos. Seguiremos con la definición formal de los módulos, submódulos y cuando un submódulo es finitamente generado, notaremos la importancia de los homomorfismos de módulos y como podemos escribir a un módulo como suma directa de submódulos. También estudiando los módulos libres sobre D.I.P.

En el segundo capítulo, encontraremos resultados análogos al orden de un elemento en un grupo y un subgrupo de torsión, descomponiendo a un M.F.G sobre D.I.P como suma de un módulo de torsión y un módulo libre de rango finito. De igual manera, descompondremos un submódulo de torsión como suma de submódulos, lo cual implica que cada elemento en ellos tiene orden una potencia de un primo p en el anillo, luego enlazando resultados previos para ver que estos módulos los podemos escribir como suma directa de módulos cíclicos.

Finalmente en el capítulo tres, estudiaremos una aplicación del teorema de descomposición de módulos sobre D.I.P en dos de las formas cánonicas (racional y de Jordan).

Capítulo 1

PRELIMINARES Y MÓDULOS

En este capítulo, encontraremos algunos resultados que han sido de gran importancia para el estudio del teorema de descomposición de módulos sobre dominios de ideales principales, sin embargo, no enfatizaremos tanto en la demostración de dichos resultados; tal es el caso del lema de zorn que será tomado como un axioma, asimismo encontraremos las definiciones y notaciones necesarias para mayor claridad en este proyecto.

1.1. LEMA DE ZORN

Definición 1.1. *Un* ***orden parcial*** *en un conjunto A está dado por una relación $\leq$ definida para ciertos pares ordenados de elementos de A tal que se satisfacen las siguientes condiciones:*

(i) $a \leq a$ *para todos los* $a \in A$ *(**ley reflexiva**).*

(ii) Si $a \leq b$ *y* $b \leq a$*, entonces* $a = b$ *(**ley antisimétrica**).*

(iii) Si $a \leq b$ *y* $b \leq c$*, entonces* $a \leq c$ *(**ley transitiva**).*

En estas condiciones $(A, \leq)$ *es un* ***conjunto parcialmente ordenado****.*

En un conjunto parcialmente ordenado no por fuerza son **comparables** cada par de elementos, esto es, para $a, b \in A$ no necesariamente se tiene $a \leq b$ o $b \leq a$. Un conjunto

parcialmente ordenado A en el que cualquier par de elementos son comparables es un **conjunto totalmente ordenado** y $\leq$ es un **orden total** en A. Escribir $a < b$ denota $a \leq b$, pero $a \neq b$.

Un subconjunto C de un conjunto parcialmente ordenado A es una **cadena** si cada par de elementos a y b en C son comparables, esto es, si $a \leq b$ o $b \leq a$ (o ambos). Sea $B \subseteq A$, un elemento $u \in A$ es una **cota superior** de B si $b \leq u$ para todas las $b \in B$. Un elemento $m \in A$ es **maximal** si no existe $a \in A$ tal que $m < a$.

Sea B un subconjunto de un conjunto parcialmente ordenado $(A, \leq)$. Un elemento $e \in B$ es un **elemento mínimo** de B si $e \leq b$ para todo $b \in B$. Si todo subconjunto no vacío de A tiene elemento mínimo, entonces decimos que A está **bien ordenado**.

Teorema 1.1. *Sea A un conjunto no vacío. Entonces existe un orden total $\leq$ en A tal que $(A, \leq)$ es bien ordenado.*

Demostración. Véase [1] Hungerford página 14. ■

Teorema 1.2. *Sea $(A, \leq)$ un conjunto totalmente ordenado. El **sucesor inmediato** de $a \in A$ es el elemento mínimo del conjunto $\{x \in A : a < x\}$ (cuando exista tal mínimo). Si A está bien ordenado por $\leq$, entonces a lo más un elemento de A no tiene sucesor inmediato.*

Demostración. Véase [1] Hungerford página 15. ■

Lema 1.1 (Lema de Zorn)**.** *Si S es un conjunto parcialmente ordenado tal que toda cadena en S tiene una cota superior en S, entonces S tiene al menos un elemento maximal.*

El Lema de Zorn no se prueba, no se trata de eso, lo tomamos aquí como un axioma, este se usará con frecuencia cuando se quiera mostrar la existencia de una estructura mayor o maximal de algún tipo.

1.2. ANILLOS

Definición 1.2. *Un **Anillo** es un conjunto no vacío R, acompañado de dos operaciones binarias llamadas suma y multiplicación (usualmente denotadas por (+) y (.)*

(notación yuxtapuesta, respectivamente) tales que:

(*i*) $(R, +)$ *es un grupo abeliano.*

(*ii*) $(ab)c = a(bc)$ *para todo* $a, b, c \in R$.

(*iii*) $a(b + c) = ab + ac$ *y* $(a + b)c = ac + bc$ *para todo* $a, b, c \in R$.

Definición 1.3. *Un anillo* R *tal que*

$$ab = ba$$

para todo $a, b \in R$, *es llamado un* ***anillo conmutativo****.*

El símbolo 0 denotará al elemento identidad aditiva en cualquier anillo R y $-r$ al inverso aditivo de $r \in R$.

Definición 1.4. *Un anillo* R *que contiene un elemento* $1 \neq 0$ *tal que*

$$1a = a1 = a$$

para todo $a \in R$, *es llamado un* ***anillo con unitario****.*

Sea A un conjunto no vacío. El símbolo 1_A denotará la función identidad

$$\begin{array}{rccc} 1_A & : & A & \longrightarrow & A \\ & & a & \longmapsto & a \end{array}$$

Teorema 1.3. *Sea* R *un anillo. Entonces*

(*i*) $0r = r0 = 0$ *para todo* $r \in R$.

(*ii*) $(-r)s = r(-s) = -(rs)$ *para todo* $r, s \in R$.

(*iii*) *Sean* $a \in R$ *y* $n \in \mathbb{Z}$. *Definamos la multiplicación de* n *por* a *como:* $na = a + a + \cdots + a$ *(*n *veces* a*). Mostrar que* $(nr)s = r(ns) = n(rs)$ *para todo* $r, s \in R$.

Demostración. Véase [1] Hungerford página 115. ■

Definición 1.5. *Un elemento $a \neq 0$ en un anillo conmutativo R es un* ***divisor de cero****, si existe un $b \neq 0 \in R$ tal que $ab = ba = 0$.*

Definición 1.6. *Un anillo conmutativo con unitario R tal que $1 \neq 0$ y sin divisores de cero, es llamamdo un* ***dominio entero.***

Definición 1.7. *Sea R un anillo conmutativo con unitario. Decimos que un elemento $a \in R - \{0\}$ es* ***invertible*** *o una* ***unidad*** *si existe $a^{-1} \in R$ tal que $aa^{-1} = 1$.*

Definición 1.8. *Un dominio entero R tal que todo elemento de $R - \{0\}$ es una unidad, es llamado un* ***campo****.*

Definición 1.9. *Sean R y S anillos. Una función $\varphi : R \longrightarrow S$ tal que*

$$f(r_1 + r_2) = f(r_1) + f(r_2)$$

y

$$f(r_1 r_2) = f(r_1) f(r_2)$$

para todo $r_1, r_2 \in R$ la llamaremos un ***homomorfismo de anillos****.*

A un homomorfismo de anillos inyectivo lo llamaremos un **monomorfismo de anillos**. A un homomorfismo de anillos sobreyectivo lo llamaremos un **epimorfismo de anillos.** A un homomorfismo de anillos que es biyectivo lo llamaremos un **isomorfismo de anillos**. Si $\varphi : R \longrightarrow S$ es un isomorfismo de anillos, entonces diremos que R y S son **isomorfos** y lo denotamos por el símbolo $R \cong S$.

Definición 1.10. *Sea R un anillo conmutativo. Un subconjunto no vacío I de R es un* ***ideal*** *si:*

(*i*) $i_1 - i_2 \in I$ *para todo* $i_1, i_2 \in I$.

(*ii*) $ri \in I$ *e* $ir \in I$ *para todo* $r \in R$ *y todo* $i \in I$.

Lema 1.2. *Sea $\{A_i : i \in I\}$ una familia de ideales de un anillo conmutativo R. Entonces $\bigcap_{i \in I} A_i$ también es un ideal de R.*

Demostración. Véase [1] Hungerford página 123. ■

Definición 1.11. *Sean X un subconjunto no vacío de un anillo conmutativo R y $\{A_i : i \in I\}$ la familia de ideales de R que contienen a X. Entonces $\bigcap_{i\in I} A_i$ es el* ***ideal de*** *R* ***generado por*** *X y se denotará por el símbolo $\langle X\rangle$. Un ideal $\langle x\rangle$ generado por un solo elemento $x \in R$ es llamado un* ***ideal principal****.*

Teorema 1.4. *Sea X un subconjunto no vacío de un anillo R conmutativo con unitario. Entonces el ideal $\langle X\rangle$ consiste de todas las sumas finitas*

$$r_1x_1 + \cdots + r_nx_n$$

donde n es un entero positivo, los $r_i \in R$ y los $x_i \in X$. En particular, si $s \in R$, entonces $\langle s\rangle = Rs = \{rs : r \in R\}$. $\langle s\rangle$ es llamado el ***ideal principal*** *de R generado por s.*

Demostración. Véase [1] Hungerford página 124. ■

Definición 1.12. *Un anillo conmutativo con unitario R es un* ***anillo de ideales principales*** *si todo ideal en R es un ideal principal.*

Definición 1.13. *Un anillo de ideales principales que también es un dominio entero es llamado un* ***dominio de ideales principales (D.I.P)****.*

Lema 1.3. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos. Entonces el* ***Kernel*** *de φ*

$$Ker(\varphi) = \{r \in R : \varphi(r) = 0\}$$

es un ideal de R y la ***imagen*** *de φ*

$$Im(\varphi) = \{\varphi(r) : r \in R\}$$

es un ideal de S.

Demostración. Véase [1] Hungerford página 125. ■

Teorema 1.5. *Sean R un anillo conmutativo con unitario e I un ideal de R. Entonces el grupo cociente aditivo R/I también es un anillo conmutativo con unitario con la multiplicación dada por*

$$(r + I)(s + I) = rs + I.$$

Demostración. Véase [1] Hungerford página 125. ■

Teorema 1.6. *Sean R un anillo conmutativo con unitario e I un ideal de R. Entonces la función*

$$\pi : R \longrightarrow R/I$$

dada por $\pi(r) = r + I$ para todo $r \in R$ es un epimorfismo de anillos.

Demostración. Véase [1] Hungerford página 125. ■

Teorema 1.7. *Si $\varphi : R \longrightarrow S$ es un homomorfismo de anillos, entonces*

$$R/Ker(\varphi) \cong Im(\varphi).$$

Demostración. Véase [1] Hungerford página 126. ■

Definición 1.14. *Sea R un anillo. Un ideal M de R es un **ideal maximal** si $M \neq R$ y para todo ideal N tal que $M \subseteq N \subseteq R$, tenemos que $N = M$ ó $N = R$.*

Teorema 1.8. *Sea M un ideal maximal en un anillo conmutativo R con unitario. Entonces el anillo cociente R/M es un campo.*

Demostración. Véase [1] Hungerford página 129. ■

Definición 1.15. *Sea R un anillo con unitario. Un elemento $a \in R$ es una **unidad**, si existe $b \in R$ tal que $ab = 1 = ba$.*

Definición 1.16. *Un elemento $a \neq 0$ en un anillo conmutativo R, **divide** a, $b \in R$, si existe $c \in R$ tal que $ac = b$, (se usará la notación $a \mid b$ para indicar que a divide a b). Los elementos $a, b \in R$ son llamados **asociados** si $a \mid b$ y $b \mid a$.*

Teorema 1.9. *Sean a, b elementos de un anillo R conmutativo con unitario. Entonces a y b son asociados si y sólo si $\langle a \rangle = \langle b \rangle$.*

Demostración. Véase [1] Hungerford página 136. ■

Definición 1.17. *Sea R un anillo conmutativo con unitario. Un elemento $p \in R$ es **primo** si:*

(*i*) *p es no cero y p no es una unidad;*

(*ii*) *Si* $p \mid ab$, *entonces* $p \mid a$ *o* $p \mid b$ *donde a y b son elementos de R .*

Definición 1.18. *Sea R un anillo conmutativo con unitario. Un elemento c de R es* ***irreducible*** *si:*

(*i*) *c es no cero y c no es unidad;*

(*ii*) *Si* $c = ab$, *entonces a o b es una unidad, donde a y b son elementos de R*

Teorema 1.10. *Sean p y c elementos no cero en un dominio R. Entonces*

(*i*) *c es irreducible si y sólo si* $\langle c \rangle$ *es un ideal maximal de R.*

(*ii*) *Si R es un dominio de ideales principales, entonces p es primo si y sólo si p es irreducible.*

Demostración. Véase [1] Hungerford página 136. ■

Definición 1.19. *Un dominio entero R es un* ***dominio de factorización única*** *si:*

(*i*) *para cada elemento* $a \in R$ *no cero y no unidad, a puede escribirse como* $a = c_1 c_2 \dots c_n$, *con* $c_1, \dots, c_n$ *irreducibles;*

(*ii*) *si* $a = c_1 c_2 \dots c_n$ *y* $a = d_1 d_2 \dots d_m$ *(*c_i, d_i *irreducibles), entonces* $n = m$ *y para alguna permutación* σ *de* $\{1, 2, \dots, n\}$, c_i *y* $d_{\sigma(i)}$ *son asociados para cada i.*

Teorema 1.11. *Todo dominio de ideales principales R es un dominio de factorización única.*

Demostración. Véase [1] Hungerford página 138. ■

Definición 1.20. *Sea X un conjunto no vacío de un anillo conmutativo R. Un elemento* $d \in R$ *es un* ***máximo común divisor*** *de X si:*

(*i*) $d \mid a$ *para todo* $a \in X$;

(*ii*) *Si* $c \in R$ $c \mid a$ *para todo* $a \in X$, *entonces* $c \mid d$.

Definición 1.21. *Sean* R *un anillo conmutativo con identidad y* $r_1, \ldots, r_k$ *elementos de* R. *Si* $r_1, \ldots, r_k$ *tienen a* 1 *como máximo común divisor, entonces* $r_1, \ldots, r_k$ *son* ***primos relativos***.

Teorema 1.12. *Sean* $r_1, ..., r_k$ *elementos de un dominio de ideales principales, entonces existe al menos un máximo común divisor de* $r_1, ..., r_k$ *y todo máximo común divisor de* $r_1, ..., r_k$ *es de la forma*

$$s_1 r_1 + \cdots + s_k r_k.$$

Demostración. Véase [1] Hungerford página 140. ■

Sea R un anillo. Un **polinomio** $f(x)$ con coeficientes en R es una suma finita

$$r_0 + r_1 x + \cdots + r_n x^n$$

donde $r_i \in R$, n es un entero no negativo y x es una indeterminada. Los r_i son **los coeficientes** de $f(x)$. Si $r_n \neq 0$, entonces n es el **grado** de $f(x)$. Si $r_1 = \cdots = r_n = 0$, entonces $f(x)$ es cero.

La suma y multiplicación de polinomios con coeficientes en un anillo R están definidas de la manera que nos es formalmente conocida.

Escribiremos $R[x]$ para denotar al conjunto de todos los polinomios en una indeterminada x con coeficientes en un anillo R.

Teorema 1.13. *Sea* R *un anillo. Entonces* $R[x]$ *es un anillo bajo la suma y multiplicación polinomial. Si* R *es conmutativo, entonces también lo es* $R[x]$ *y si* R *tiene unitario* 1, *entonces* $R[x]$ *también tiene a* 1 *como unitario.*

Demostración. Véase [3] Fraleigh página 268. ■

Definición 1.22. *Sea* F *un anillo. Un polinomio no constante* $f(x) \in F[x]$ *es* ***irreducible*** *si* $f(x)$ *no puede expresarse como un producto* $g(x)h(x)$ *de dos polinomios* $g(x)$ *y* $h(x)$ *en* $F[x]$, *ambos de grado menor que el grado de* $f(x)$.

Teorema 1.14. *Sean F un anillo,*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

con $a_n \neq 0$ y

$$g(x) = b_m x^m + \cdots + b_1 x + b_0$$

con $b_m \neq 0$, $m > 0$, polinomios de $F[x]$. Entonces existen $q(x), r(x) \in F[x]$ tales que

$$f(x) = g(x)q(x) + r(x)$$

donde $r(x) = 0$ o el grado de $r(x)$ es menor que m.

Demostración. Véase [3] Fraleigh página 277. ■

Teorema 1.15. *Sea K un campo. Entonces $K[x]$ es un dominio de ideales principales.*

Demostración. Véase [3] Fraleigh página 285. ■

1.3. MÓDULOS

Definición 1.23. *Sea R un anillo. Un $R-$**módulo** es un grupo abeliano A (con operación binaria $+$) junto a una operación*

$$\begin{array}{ccc} R \times A & \longrightarrow & A \\ (r, a) & \longmapsto & ra \end{array}$$

tal que para todo $r, s \in R$ y todo $a, b \in A$:

(i) $r(a + b) = ra + rb$.

(ii) $(r + s)a = ra + sa$.

(iii) $r(sa) = (rs)a$.

Si R tiene elemento unitario 1 y tenemos que

(iv) $1a = a$ *para todo $a \in A$, entonces A es llamado un $R-$**módulo unitario**.*

Definición 1.24. *Si R es un campo y es A un $R-$módulo unitario, entonces A es un* ***espacio vectorial****.*

Si A es un módulo con elemento identidad aditiva 0_A sobre un anillo con identidad aditiva 0_R, entonces para toda $r \in R$ y toda $a \in A$ tenemos que

$$r0_A = 0_A \quad \text{y} \quad 0_R a = 0_A.$$

Como el contexto será claro, entonces utilizaremos el mismo símbolo 0 para 0_R y 0_A. Es fácil verificar que para todo $r \in R$, para todo $n \in \mathbb{Z}$ y para todo $a \in A$,

$$(-r)a = r(-a) = -(ra) \quad \text{y} \quad n(ra) = r(na).$$

Definición 1.25. *Sea R un anillo y A, B $R-$módulos. Una función*

$$\varphi : A \longrightarrow B$$

es un ***homomorfismo de $R-$módulos*** *si para todo $a, c \in A$ y todo $r \in R$*

$$\varphi(a + c) = \varphi(a) + \varphi(c) \qquad y \qquad \varphi(ra) = r\varphi(a).$$

Si además φ es una función inyectiva, entonces φ es un ***monomorfismo de $R-$módulos****, φ es una función sobreyectiva, entonces φ es un* ***epimorfismo de $R-$módulos****, φ es una función biyectiva, entonces φ es un* ***isomorfismo de $R-$módulos****. En este último caso A y B son $R-$**módulos isomorfos** y lo denotamos $A \cong B$.*

Definición 1.26. *Sean $\varphi : A \longrightarrow B$ un homomorfismo de $R-$módulos y $a \in A$. Definimos el* ***kernel de*** *φ denotado por $Ker(\varphi)$ como el conjunto donde todas las imagenes de a bajo φ son cero, es decir,*

$$Ker(\varphi) = \{a \in A : \varphi(a) = 0\}$$

y la ***imagen de*** *φ denotada por $Im(\varphi)$ como el conjunto de todas las imagenes de a bajo φ, esto es,*

$$Im(\varphi) = \{\varphi(a) : a \in A\}$$

Lema 1.4. *Sea $\varphi : A \longrightarrow B$ es un homomorfismo de $R-$módulos. Entonces φ es un monomorfismo de $R-$módulos si y sólo si $Ker(\varphi) = \{0\}$.*

Demostración. Véase Hunherford página 170. ■

Definición 1.27. *Sean R un anillo, A un $R-$módulo y B un subconjunto no vacío de A. Entonces B es un* ***submódulo*** *de A si:*

(i) $b_1 - b_2 \in B$ *para todo* $b_1, b_2 \in B$.

(ii) $rb \in B$ *para todo* $r \in R$ *y todo* $b \in B$.

Teorema 1.16. *Sean R un anillo, A un $R-$módulo y $a \in A$. Entonces*

$$Ra = \{ra : r \in R\}$$

es un submódulo de A y si $a \neq 0$

$$\begin{array}{rccc} \varphi & : & R & \longrightarrow & Ra \\ & & r & \longmapsto & ra \end{array}$$

es un epimorfismo de $R-$módulos.

Demostración. Véase [1] Hungerford página 171. ■

Lema 1.5. *Sea $\{A_i : i \in I\}$ una familia de submódulos de un $R-$módulo A. Entonces $\bigcap_{i \in I} A_i$ es también un submódulo de A.*

Demostración. Véase [1] Hungerford página 171. ■

Definición 1.28. *Si X es un subconjunto de un $R-$módulo A, entonces la intersección de todos los submódulos de A que contienen a X es llamado el* ***submódulo generado por*** *X. Tal submódulo lo denotaremos por el símbolo $\langle X \rangle$.*

Definición 1.29. *Sean A un $R-$módulo y B un submódulo de A tal que B es el submódulo generado por un subconjunto finito $X = \{x_1, ..., x_n\}$ de A, entonces diremos que B es* ***finitamente generado****, tal submódulo lo denotaremos por $B = \langle x_1, ..., x_n \rangle$. Si $X = \{x\}$, entonces el submódulo $\langle x \rangle$ es el* ***submódulo cíclico generado por*** *x.*

Definición 1.30. *Sean A un $R-$módulo y $\{A_i : i \in I\}$ una familia de submódulos de A. El submódulo de A generado por $\bigcup_{i \in I} A_i$ es llamado la* ***suma de los submódulos*** *A_i. El submódulo generado por $\bigcup_{i \in I} A_i$ lo denotaremos por $\sum_{i \in I} A_i$.*

Teorema 1.17. *Sean R un anillo con identidad, A un $R-$módulo unitario y $\{A_i : i \in I\}$ una familia de submódulos de A. Entonces $\sum_{i\in I} A_i$ consiste de todas las sumas finitas $a_{i_1} + \cdots + a_{i_n}$, donde $n \in \mathbb{Z}^+$ y $a_{i_1} \in A_{i_1}, ..., a_{i_n} \in A_{i_n}$ para ciertos $A_{i_1}, ..., A_{i_n}$ de la familia $\{A_i : i \in I\}$.*

Demostración. Véase [1] Hungerford página 172. ■

Teorema 1.18. *Sea B un submódulo de un módulo A sobre un anillo R. Entonces el grupo cociente A/B es un $R-$módulo con la acción de R sobre A/B dada por*

$$r(a + B) = ra + B$$

para todo $r \in R$ y todo $a \in A$. La función $\pi : A \longrightarrow A/B$ dada por $a \longmapsto a + B$ es un epimorfismo de $R-$módulos.

Demostración. Véase [1] Hungerford página 172. ■

Lema 1.6. *Sean R un anillo y $\varphi : A \longrightarrow B$ un homomorfismo de $R-$módulos. Entonces $Ker(\varphi)$ es un submódulo de A e $Im(\varphi)$ es un submódulo de B.*

Teorema 1.19. *Sean R un anillo y $\varphi : A \longrightarrow B$ un homomorfismo de $R-$módulos. Entonces*

$$A/Ker(\varphi) \cong Im(\varphi).$$

Demostración. Véase [1] Hungerford página 172. ■

Teorema 1.20. *Sean B y C submódulos de un módulo A sobre un anillo R. Entonces*

$$B/(B \cap C) \cong (B + C)/C,$$

como $R-$módulos.

Demostración. Véase [1] Hungerford página 173. ■

Definición 1.31. *Sea R un anillo, M y N dos $R-$módulos. Definimos la **suma directa externa** de los $R-$módulos M y N denotada por $M \bigoplus N$ como el conjunto de pares ordenados (x, y) con $x \in M$, $y \in N$, con la siguiente suma y acción de R:*

Si $(x_1, y_1),\ (x_2, y_2) \in M \bigoplus N$ *y* $a \in R$, *entonces*

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$$

y

$$a(x_1, y_1) := (ax_1, ay_1).$$

De manera general, si $\{M_1, M_2, \ldots, M_n\}$ *es un conjunto finito de* $R-$*módulos, su suma directa externa* $M_1 \bigoplus M_2 \bigoplus \cdots \bigoplus M_n$ *es la totalidad de* $n-$*tuplas ordenadas* $(x_1, x_2, \ldots, x_n)$ *con* $x_i \in M_i$ *para todo* $i = \{1, 2, \ldots, n\}$, *donde la suma y la acción de* R *se definen entrada por entrada.*

Teorema 1.21. *Sea* R *un anillo y* $\{A_i : i \in I\}$ *una familia de submódulos de un* $R-$*módulo* A *tal que*

(*i*) A *es la suma de la familia* $\{A_i : i \in I\}$ *y*

(*ii*) *para cada* $k \in I$, $A_k \cap A_k^* = \{0\}$, *donde* A_k^* *es la suma de la familia* $\{A_i : i \in I \text{ y } i \neq k\}$.

Entonces $A \cong \sum_{i \in I} A_i$.

Demostración. Véase [1] Hungerford página 175. ■

Definición 1.32. *Un módulo* A *es llamado la* ***suma directa interna*** *de una familia de submódulos* $\{A_i : i \in I\}$, *si* A *y* $\{A_i : i \in I\}$ *satisfacen las hipótesis del Teorema 1.21. Esto lo denotaremos por la expresión* $A = \bigoplus_{i \in I} A_i$.

Usaremos la misma notación de suma directa externa con la suma directa interna, ya que estas son isomorfas. En adelante, no se distinguirá entre suma directa 'externa' e 'interna', sino que el contexto indicará el caso.

Definición 1.33. *Una secuencia finita de homomorfismos de módulos,*

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} A_n,$$

es ***exacta*** *si* $Im(f_i) = Ker(f_{i+1})$ *para* $i = 1, 2, ..., n-1$.

Nótese que para cualquier módulo A, existen homomorfismo de módulos únicos $0 \longrightarrow A$ y $A \longrightarrow 0$.

Definición 1.34. *Una secuencia exacta de la forma*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

es llamada una secuencia exacta corta.

Definición 1.35. *Dos secuencias exactas cortas son* ***isomorfas*** *si existe un diagrama conmutativo de homomorfismos de módulos*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

tal que f, g y h son isomorfismos.

Teorema 1.22. *Sean R un anillo y*

$$0 \longrightarrow A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \longrightarrow 0$$

una secuencia exacta corta de homomorfismos de $R-$módulos. Las siguientes condiciones son equivalentes.

(*i*) *Existe un homomorfismo de $R-$módulos $h : A_2 \longrightarrow B$ tal que $g \circ h = 1_{A_2}$.*

(*ii*) *Existe un homomorfismo de $R-$módulos $k : B \longrightarrow A_1$ tal que $k \circ f = 1_{A_1}$.*

(*iii*) *La secuencia dada es isomorfa a la secuencia exacta corta*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{i_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & a_1 & \longmapsto & (a_1, 0) & & & & \\ & & & & (a_1, a_2) & \longmapsto & a_2 & & \end{array},$$

en particular, $B \cong A_1 \oplus A_2$.

Demostración. Véase [1] Hungerford página 177. ■

Definición 1.36. *Una secuencia exacta corta que satisface las condiciones presentes en el Teorema 1.22 es llamada una* ***secuencia split exacta****.*

Teorema 1.23. *Sean $f : A \longrightarrow B$ y $g : B \longrightarrow A$ homomorfismos de $R-$módulos tales que $g \circ f = 1_A$. Entonces $B = Im(f) \oplus Ker(g)$.*

Demostración. Véase [1] Hungerford página 180. ■

Definición 1.37. *Un módulo P sobre un anillo es un* ***módulo proyectivo*** *si dado cualquier diagrama de homomorfismos de $R-$módulos*

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow f & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

donde g es epimorfismo, entonces existe un homomorfismo de $R-$módulos

$$h : P \longrightarrow A$$

tal $g \circ h = f$.

Definición 1.38. *Sea R un anillo con identidad. Un $R-$módulo unitario F es un* ***módulo libre*** *si F tiene una base.*

Teorema 1.24. *Todo módulo libre F sobre un anillo R con identidad 1 es proyectivo.*

Demostración. Véase [1] Hungerford página 191. ■

Teorema 1.25. *Sean R un anillo y P un $R-$módulo, P es proyectivo si y sólo si toda secuencia exacta corta*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$$

es split exacta.

Demostración. Véase [1][192]. ■

Definición 1.39. *Un subconjunto X de un $R-$módulo A es* ***linealmente independiente*** *si para cualquier subconjunto finito de elementos distintos $x_1, ..., x_n \in X$ y $r_1, ..., r_n \in R$,*

$$r_1x_1 + \cdots + r_nx_n = 0 \quad implica \quad r_1 = \cdots = r_n = 0.$$

Definición 1.40. *Sean A un $R-$módulo y X un subconjunto no vacío de A. Se dice que X es una* ***base*** *de A si X es linealmente independiente y además X genera a A como $R-$módulo.*

Definición 1.41. *Sea R un anillo con identidad tal que para todo $R-$módulo libre F, cualquiera dos bases de F tienen la misma cardinalidad. Entonces R tiene la* ***propiedad de rango invariante*** *y el número cardinal de cualquier base de F lo llamaremos el* ***rango*** *de F sobre R ($rank(F)$).*

Teorema 1.26. *Sean E y F módulos libres sobre un anillo R que tiene la propiedad de rango invariante. Entonces $E \cong F$ si y sólo si E y F tienen el mismo rango.*

Demostración. Véase [1] Hungerford página 185. ■

Lema 1.7. *Todo anillo comnutativo con unitario tiene la propiedad de rango invariante.*

Demostración. Véase [1] Hungerford página 186. ■

Lema 1.8. *Sean F un módulo libre sobre un dominio de ideales principales R y $\{x_i : i \in I\}$ una base de F. Entonces para todo $i \in I$, Rx_i es isomorfo a R como $R-$módulos.*

Demostración. Sea $i \in I$. Consideremos a R y Rx_i como $R-$módulos y definamos

$$\begin{array}{rccc} \varphi & : & R & \longrightarrow & Rx_i \\ & & r & \longmapsto & rx_i \end{array}$$

donde rx_i es la multiplicación en F. Veamos que φ es un isomorfirmo de $R-$módulos. En efecto, sean $r_1, r_2 \in R$, entonces

$$\varphi(r_1 + r_2) = (r_1 + r_2)x_i = r_1x_i + r_2x_i = \varphi(r_1) + \varphi(r_2).$$

Ahora, sean $r \in R$ y $r_1 \in R$, entonces

$$\varphi(rr_1) = (rr_1)x_i = r(r_1x_i) = r\varphi(r_1).$$

Si $y \in Rx_i$, entonces $y = rx_i$ para algún $r \in R$. Así, $y = \varphi(r)$. Finalmente, sean $r_1, r_2 \in R$ tales que $\varphi(r_1) = \varphi(r_2)$, entonces $r_1x_i = r_2x_i$, así las cosas $(r_1 - r_2)x_i = 0$,

de donde se infiere que $r_1 - r_2 = 0$ porque el conjunto $\{x_i : i \in I\}$ es linealmente independiente. Por lo tanto $r_1 = r_2$. Por todo lo anterior φ es un isomorfismo de $R-$módulos y $R \cong Rx_i$. ■

Lema 1.9. *Sean F un módulo libre sobre un dominio de ideales principales R y $\{x_i : i \in I\}$ una base de F. Entonces*

$$F = \bigoplus_{i \in I} Rx_i.$$

Demostración. Como $Rx_i \subseteq F$ para todo $i \in I$ y F es un $R-$módulo, entonces $\sum_{i \in I} Rx_i \subseteq F$. Ahora, sea $x \in F$. Entonces existen $i_1, ..., i_t \in I$ y $r_{i_1}, ..., r_{i_t} \in R$ tales que

$$x = r_{i_1}x_{i_1} + \cdots + r_{i_t}x_{i_t} \in \sum_{i \in I} Rx_i.$$

Luego $F \subseteq \sum_{i \in I} Rx_i$. Por todo lo anterior $F = \sum_{i \in I} Rx_i$.
Finalmente, sean $j \in I$ y $x \in Rx_j \cap \sum_{i \in I - \{j\}} Rx_i$. Entonces existen

$$i_1, ..., i_n \in I - \{j\}$$

distintos y $r, r_{i_1}, ..., r_{i_n} \in R$ tales que

$$rx_j = x = r_{i_1}x_{i_1} + \cdots + r_{i_n}x_{i_n}.$$

Luego,

$$0 = rx_j - r_{i_1}x_{i_1} - \cdots - r_{i_n}x_{i_n}.$$

Pero $\{x_i : i \in I\}$ es una base de F, por lo tanto $r = r_{i_1} = \cdots = r_{i_n} = 0$ y $x = 0x_j = 0$. Así, $Rx_j \cap \sum_{i \in I - \{j\}} Rx_i = \{0\}$. Por todo lo visto, $F = \bigoplus_{i \in I} Rx_i$. ■

Capítulo 2

MÓDULOS SOBRE D.I.P

En este capítulo estudiaremos más a fondo los módulos sobre D.I.P. Se dará a conocer la relación que existe entre el rango de un módulo libre y un submódulo, también encontraremos la definición de un módulo libre de torsión, el orden de un módulo sobre D.I.P. y al finalizar el capítulo tendremos el teorema de descomposición de módulos sobre D.I.P. el cual nos dice que podemos escribir a un módulo sobre D.I.P, como suma directa de sunmódulos cíclicos, siendo este el objeto de estudio de este trabajo.

2.1. RESULTADOS PREVIOS

Definición 2.1. *Sean A un módulo sobre un dominio entero R y $a \in A$. Definimos*

$$\mathcal{O}_a = \{s \in R : sa = 0\}.$$

Definición 2.2. *Sea A un módulo sobre un dominio entero R. Definimos*

$$A_t = \{a \in A : \mathcal{O}_a \neq \{0\}\}.$$

Teorema 2.1. *Sean A un módulo sobre un dominio entero R y $a \in A$. Entonces*

(*i*) *$\mathcal{O}_a$ es un ideal de R.*

(*ii*) *A_t es un submódulo de A.*

(*iii*) $R/\mathcal{O}_a \cong Ra = \{ra : r \in R\}$.

(*iv*) *Si R es un dominio de ideales principales, p un elemento primo de R y $p^i a = 0$, entonces*

$$\mathcal{O}_a = \left\langle p^j \right\rangle$$

con $0 \leq j \leq i$.

(*v*) *Si R es un dominio de ideales principales, p un elemento primo de R y $\mathcal{O}_a = \langle p^i \rangle$, entonces $p^j a \neq 0$ para todo j tal que $0 \leq j \leq i$.*

Demostración. (*i*) Sabemos que

$$0 = 0a - 0a = (0 - 0)a = 0a,$$

por tanto $0 \in \mathcal{O}_a$ y así $\mathcal{O}_a$ es no vacío. Ahora, sean $s_1, s_2 \in \mathcal{O}_a$. Entonces

$$(s_1 - s_2)a = s_1 a - s_2 a = 0 - 0 = 0,$$

así $s_1 - s_2 \in \mathcal{O}_a$. Finalmente, sean $r \in R$ y $s \in \mathcal{O}_a$. Entonces

$$(sr)a = (rs)a = r(sa) = r0 = r(0 - 0) = r0 - r0 = 0.$$

Por todo lo anterior, $\mathcal{O}_a$ es un ideal de R.
(*ii*) Notar que

$$(1)(0) = 1(0 - 0) = (1)(0) - (1)(0) = 0,$$

por tanto $1 \in \mathcal{O}_0$ y $\mathcal{O}_0 \neq \{0\}$. Así, $0 \in A_t$ y A_t es no vacío. Sean $b_1, b_2 \in A_t$, entonces existen $r_1 \in \mathcal{O}_{b_1}$ y $r_2 \in \mathcal{O}_{b_2}$ donde $r_1, r_2 \in R - \{0\}$. Como R es un dominio entero tenemos que $r_1 r_2 = r_2 r_1$ y $r_1 r_2 \neq 0$. Luego,

$$\begin{aligned}(r_1 r_2)(b_1 - b_2) &= (r_1 r_2)b_1 - (r_1 r_2)b_2 = (r_2 r_1)b_1 - (r_1 r_2)b_2 \\ &= r_2(r_1 b_1) - r_1(r_2 b_2) = r_2 0 - r_1 0 = 0 - 0 \\ &= 0,\end{aligned}$$

por tanto $r_1 r_2 \in \mathcal{O}_{b_1 - b_2}$ y $\mathcal{O}_{b_1 - b_2} \neq \{0\}$. Así, $b_1 - b_2 \in A_t$. Finalmente, sean $r \in R$ y $b \in A_t$, entonces existe $s \in R - \{0\}$ tal que $sb = 0$, por tanto

$$s(rb) = (sr)b = (rs)b = r(sb) = r0 = 0,$$

consecuentemente $s \in \mathcal{O}_{rb}$, así las cosas $\mathcal{O}_{rb} \neq \{0\}$ y entonces $rb \in A_t$. Por todo lo anterio, A_t es un submódulo de A.

(iii) Sea

$$\begin{array}{rccc} \varphi & : & R & \longrightarrow & Ra \\ & & r & \longmapsto & ra \end{array}$$

Si $r_1, r_2 \in R$, entonces

$$\varphi(r_1 + r_2) = (r_1 + r_2)a = r_1a + r_2a = \varphi(r_1) + \varphi(r_2).$$

Si $s \in R$ y $r \in R$

$$\varphi(sr) = (sr)a = s(ra) = s\varphi(r),$$

luego, φ es un homomorfismo de $R-$módulos. Si $r \in R$, entonces $ra = \varphi(r)$. Por lo tanto, φ es sobreyectivo ($\mathrm{Im}(\varphi) = Ra$). Finalmente, $r \in \ker(\varphi)$ si, y sólo si, $\varphi(r) = 0$ si, y sólo si, $ra = 0$ si, y sólo si $r \in \mathcal{O}_a$. Así, $\ker(\varphi) = \mathcal{O}_a$. Por Teorema 1.19,

$$R/\mathcal{O}_a = R/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

(iv) Como $\mathcal{O}_a$ es un ideal de R y R es un dominio de ideales principales, $\mathcal{O}_a = \langle r \rangle$ para algún $r \in R$. Como $p^i a = 0$, tenemos que $p^i \in \mathcal{O}_a = \langle r \rangle$, por lo tanto, r divide a p^i. Por lo tanto $r = p^j u$ con u una unidad y $0 \leq j \leq i$. Ahora, si $s \in \langle p^j u \rangle$, existe $t \in R$ tal que $s = (p^j u)t = p^j(ut)$, entonces $s \in \langle p^j \rangle$. Si $v \in \langle p^j \rangle$, existe $w \in R$ tal que

$$v = p^j w = p^j u u^{-1} w = (p^j u)(u^{-1} w),$$

entonces $v \in \langle p^j u \rangle$. Por lo anterior,

$$\mathcal{O}_a = \langle r \rangle = \left\langle p^j u \right\rangle = \left\langle p^j \right\rangle.$$

(v) Si $j = 0$, entonces $p^j a = p^0 a = 1a = a \neq 0$. Si $0 < j < i$ y $p^j a = 0$, entonces $p^j \in \mathcal{O}_a = \langle p^i \rangle$. Así, p^i divide a p^j, por lo tanto, existe $r \in R$ tal que $p^j = p^i r$. Por Teorema 1.10 p es irreducible. Ahora, p^j no es cero, porque $p \neq 0$ y R es dominio entero. Además p^j no es una unidad porque, si p^j fuese unidad implicaría que

$$a = 1a = (p^j)^{-1} p^j a = (p^j)^{-1} 0 = 0,$$

lo cual es contradictorio. Luego, p^j es no cero y no unidad. Como R es un dominio de ideales principales, entonces por Teorema 1.11 R es un dominio de factorización única. Por lo tanto, $p^j = p^i r$ implica que p^j se puede expresar como producto de j irreducibles y como producto de más de j irreducibles (por lo menos i), lo cual es contradictorio con el hecho de que R es un dominio de factorización única. Luego, $p^j a \neq 0$. ■

Definición 2.3. *Sean A un módulo sobre un dominio entero R. Se dice que A es* ***libre de torsión*** *si $A_t = \{0_A\}$.*

Definición 2.4. *Sean A un módulo sobre un dominio entero R. Se dice que A es un* ***módulo de torsión*** *si $A = A_t$*

Nótese que cuando un módulo A sobre un dominio entero R es libre de torsión, $a \in A - \{0\}$ y $r \in R$, entonces $ra = 0$ si y sólo si $r = 0$.

Definición 2.5. *Sean A un módulo sobre un dominio de ideales principales R y $a \in A$. Si $\mathcal{O}_a = \langle r \rangle$, entonces decimos que a tiene* ***orden*** *r. El submódulo cíclico Ra generado por a es llamado un* ***submódulo cíclico de orden*** *r.*

Teorema 2.2. *Un módulo finitamente generado y libre de torsión $A \neq 0$ sobre un dominio de ideales principales R es libre y de rango finito.*

Demostración. Sea X un conjunto finito generador de A que no contiene a 0 y $x \in X$. Luego, $rx = 0$ si y sólo si $r = 0$, porque A es libre de torsión. Por lo tanto, existe un subconjunto linealmente independiente de X,

$$S = \{x_1, ..., x_k\},$$

tal que todo subconjunto linealmente independiente de X tiene un número de elementos menor o igual que k. Así, S es una base del submódulo F de A generado por S (F es entonces un módulo libre de rango finito). Si $y \in X - S$, entonces el conjunto $\{x_1, ..., x_k, y\}$ no es linealmente independiente, por tal motivo existen $r_1, ..., r_k, r_y \in R$, no todos cero, tales que

$$r_1 x_1 + \cdots + r_k x_k + r_y y = 0,$$

de donde,

$$r_y y = -r_{1i}x_1 - \cdots - r_{ki}x_k \in F$$

y aquí se vé que $r_y \neq 0$, ya que de lo contrario (por ser $\{x_1, ..., x_k\}$ linealmente independiente) $r_1 = \cdots = r_k = 0$, contradiciendo el hecho de que no todos en la lista $r_1, ..., r_k, r_y$ son cero, luego, para todo $y \in X - S$, existe $r_y \in R$ tal que $r_y y \in F$. Como X es finito, existe $r \in R - \{0\}$ (A saber $r = \prod_{y \in X-S} r_y$) tal que $rX = \{rx : x \in X\}$ está contenido en F, por lo tanto $rA \subseteq F$. Finalmente, consideremos la función

$$\begin{array}{rccc} \varphi & : & A & \longrightarrow & A \\ & & a & \longmapsto & ra \end{array}$$

Entonces, para todo $a, b \in A$

$$\varphi(a+b) = r(a+b) = ra + rb = \varphi(a) + \varphi(b).$$

Además, para todo $a \in A$ y para todo $s \in R$

$$\varphi(sa) = r(sa) = (rs)a = (sr)a = s(ra) = s\varphi(a).$$

Luego, φ es un homomorfismo de $R-$módulos. Por la definición de φ es claro que $\mathrm{Im}(\varphi) = rA$, y por lo realizado antes de definir a φ tenemos que $\mathrm{Im}(\varphi) \subseteq F$. Pero como A es libre de torsión y $r \neq 0$, entonces $ra = 0$ con $a \in A$ se tiene si y sólo si $a = 0$, así $Ker(\varphi) = \{0\}$. Por Teorema 1.19

$$A \cong A/\{0\} = A/Ker(\varphi) \cong \mathrm{Im}(\varphi) \subseteq F.$$

Por lo tanto A es isomorfo a un submódulo del módulo libre F de rango finito, lo cual implica por Teorema **??** que A es libre y de rango finito. ■

Lema 2.1. *Sea R un dominio de ideales principales y sea A un $R-$módulo finitamente generado. Entonces A/A_t es un $R-$módulo finitamente generado.*

Demostración. Por Teorema 1.18 A/A_t es un $R-$módulo. Si $A = \langle a_1, ..., a_n \rangle$, entonces $A/A_t = \langle a_1 + A_t, ..., a_n + A_t \rangle$. ■

Teorema 2.3. *Sea A un módulo finitamente generado sobre un dominio de ideales principales R tal que $A_t \subsetneq A$. Entonces $A \cong A_t \oplus F$, donde $F = A/A_t$ es un $R-$módulo libre de rango finito.*

Demostración. El módulo cociente A/A_t es libre de torsión. En efecto, sea $a \in A$ tal que $a + A_t \in (A/A_t)_t$, entonces

$$\begin{aligned}
\mathcal{O}_{a+A_t} \neq \{0\} &\implies \exists r \in R - \{0\} \text{ tal que } r \in \mathcal{O}_{a+A_t} \\
&\implies \exists r \in R - \{0\} \text{ tal que } r(a + A_t) = A_t \\
&\implies \exists r \in R - \{0\} \text{ tal que } ra + A_t = A_t \\
&\implies \exists r \in R - \{0\} \text{ tal que } ra \in A_t \\
&\implies \exists r \in R - \{0\} \text{ tal que } \mathcal{O}_{ra} \neq \{0\} \\
&\implies \exists r, s \in R - \{0\} \text{ tal que } s(ra) = 0 \\
&\implies \exists r, s \in R - \{0\} \text{ tal que } (sr)a = 0.
\end{aligned}$$

Como R es un dominio entero y $r, s \in R - \{0\}$, entonces $rs \neq 0$, así $\mathcal{O}_a \neq \{0\}$ y en consecuencia $a \in A_t$. Luego, $a + A_t = A_t$, por tanto $(A/A_t)_t = \{A_t\}$, entonces A/A_t es libre de torsión. De otro lado, por Lema 2.1, A finitamente generado implica A/A_t finitamente generado. Ahora bién, como $A_t \subsetneqq A$ tenemos que A/A_t es un módulo no nulo, además A/A_t libre de torsión y finitamente generado, por Teorema 2.2, A/A_t es libre y de rango finito. Sea $\{a_1 + A_t, ..., a_n + A_t\}$ una base de A/A_t, entonces si $a + A_t \in A/A_t$ existen $r_1, ..., r_n \in R$ únicos tales que

$$\begin{aligned}
a + A_t &= r_1(a_1 + A_t) + \cdots + r_n(a_n + A_t) \\
&= (r_1a_1 + \cdots + r_na_n) + A_t.
\end{aligned}$$

Luego, la función

$$\begin{array}{rccc}
h & : & A/A_t & \longrightarrow & A \\
 & & a + A_t & \longmapsto & r_1a_1 + \cdots + r_na_n
\end{array}$$

donde $a + A_t = (r_1a_1 + \cdots + r_na_n) + A_t$ está bién definida. Veamos que h es un homomorfismo de $R-$módulos. En efecto, sean $a+A_t, b+A_t \in A/A_t$, entonces existen $r_1, ..., r_n, s_1, ..., s_n \in R$ únicos tales que

$$a + A_t = (r_1a_1 + \cdots + r_na_n) + A_t \text{ y } b + A_t = (s_1a_1 + \cdots + s_na_n) + A_t,$$

así

$$\begin{aligned} h((a+A_t)+(b+A_t)) &= h((a+b)+A_t) \\ &= h(((r_1+s_1)a_1+\cdots+(r_n+s_n)a_n)+A_t) \\ &= (r_1+s_1)a_1+\cdots+(r_n+s_n)a_n \\ &= (r_1a_1+\cdots+r_na_n)+(s_1a_1+\cdots+s_na_n) \\ &= h(a+A_t)+h(b+A_t). \end{aligned}$$

Ahora, si $r \in R$, entonces

$$\begin{aligned} h(r(a+A_t)) &= h(r(r_1a_1+\cdots+r_na_n)+A_t) \\ &= h((rr_1a_1+\cdots+rr_na_n)+A_t) \\ &= rr_1a_1+\cdots+rr_na_n \\ &= r(r_1a_1+\cdots+r_na_n) \\ &= rh(a+A_t). \end{aligned}$$

Definamos ahora la función

$$\begin{array}{rccc} \varphi & : & A_t \oplus (A/A_t) & \longrightarrow & A \\ & & (c\,,\, a+A_t) & \longmapsto & c+h(a+A_t) \end{array}.$$

Veamos que φ es un isomorfismo de $R-$módulos. En efecto, sean $r \in R$, $c_1, c_2 \in A_t$ y $a+A_t, b+A_t \in A/A_t$, entonces existen $r_1, ..., r_n, s_1, ..., s_n \in R$ únicos tales que

$$a+A_t = (r_1a_1+\cdots+r_na_n)+A_t \;\text{ y }\; b+A_t = (s_1a_1+\cdots+s_na_n)+A_t,$$

así

$$\begin{aligned} \varphi((c_1\,,\, a+A_t)+(c_2\,,\, b+A_t)) &= \varphi((c_1+c_2\,,\, (a+b)+A_t)) \\ &= (c_1+c_2)+(r_1+s_1)a_1+\cdots+(r_n+s_n)a_n \\ &= (c_1+r_1a_1+\cdots+r_na_n) \\ &\quad +(c_2+s_1a_1+\cdots+s_na_n) \\ &= \varphi((c_1\,,\, a+A_t))+\varphi((c_2\,,\, b+A_t)) \end{aligned}$$

y

$$\begin{aligned}\varphi(r(c_1\,,\,a+A_t)) &= \varphi((rc_1\,,\,ra+A_t))\\ &= rc_1 + rr_1a_1 + \cdots + rr_na_n\\ &= r(c_1 + r_1a_1 + \cdots + r_na_n)\\ &= r\varphi((c_1\,,\,a+A_t)).\end{aligned}$$

Así, φ es un homorfismo de $R-$módulos.
Si $\varphi((c_1\,,a+A_t)) = \varphi((c_2\,,b+A_t))$, entonces

$$c_1 + r_1a_1 + \cdots + r_na_n = c_2 + s_1a_1 + \cdots + s_na_n,$$

entonces

$$(c_1 + r_1a_1 + \cdots + r_na_n) + A_t = (c_2 + s_1a_1 + \cdots + s_na_n) + A_t,$$

entonces

$$(r_1a_1 + \cdots + r_na_n) + A_t = (s_1a_1 + \cdots + s_na_n) + A_t$$

porque $c_1, c_2 \in A_t$, entonces

$$r_1(a_1 + A_t) + \cdots + r_n(a_n + A_t) = s_1(a_1 + A_t) + \cdots + s_n(a_n + A_t),$$

entonces

$$(r_1 - s_1)(a_1 + A_t) + \cdots + (r_n - s_n)(a_n + A_t) = A_t,$$

pero como $\{a_1 + A_t, ..., a_n + A_t\}$ es una base de A/A_t, entonces$r_1 = s_1 = \cdots = r_n = s_n = 0$ y por lo tanto $r_1 = s_1, ..., r_n = s_n$.

Así,

$$c_1 + r_1a_1 + \cdots + r_na_n = c_2 + r_1a_1 + \cdots + r_na_n,$$

de donde tenemos que $c_1 = c_2$. Por lo anterior,

$$\begin{aligned}(c_1\,,\,a+A_t) &= (c_1\,,\,(r_1a_1 + \cdots + r_na_n) + A_t)\\ &= (c_2\,,\,(s_1a_1 + \cdots + s_na_n) + A_t)\\ &= (c_2\,,\,b+A_t),\end{aligned}$$

así φ es un monomorfismo de $R-$módulos.

Finalmente, si $c \in A$, entonces existen $t_1, ..., t_n \in R$ únicos tales que

$$t_1(a_1 + A_t) + \cdots + t_n(a_n + A_t) = c + A_t,$$

entonces

$$(t_1a_1 + \cdots + t_na_n) + A_t = c + A_t,$$

entonces

$$c - (t_1a_1 + \cdots + t_na_n) \in A_t.$$

Luego,

$$\begin{aligned}\varphi(c - (t_1a_1 + \cdots + t_na_n)\,,\, c + A_t) &= c - (t_1a_1 + \cdots + t_na_n) \\ &\quad + (t_1a_1 + \cdots + t_na_n) \\ &= c.\end{aligned}$$

Así, φ es un epimorfismo de $R-$módulos.

Por todo lo anterior, φ es un isomorfismo de $R-$módulos, por lo tanto

$$A \cong A_t \oplus F,$$

donde $F = A/A_t$ es un $R-$módulo libre de rango finito. ■

Teorema 2.4. *Sean R un dominio de ideales principales, A un $R-$módulo de torsión e $I = \{p \in R : p \text{ es primo}\}$. Para cada $p \in I$ definimos*

$$A(p) = \{a \in A : a \text{ tiene orden una potencia de } p\}.$$

Entonces:

(*i*) *$A(p)$ es un submódulo de A, para todo $p \in R$ primo.*

(*ii*) $A = \bigoplus_{p \in I} A(p)$

(*iii*) *Si A es finitamente generado, sólo un número finitos de los $A(p)$ son no nulos.*

Demostración. (i) Sea $p \in R$ un primo. Luego,

$$\mathcal{O}_0 = \{r \in R : r0 = 0\} = R = \langle 1 \rangle = \left\langle p^0 \right\rangle,$$

por lo que $0 \in A(p)$ y así $A(p)$ es no vacío. Sean $a, b \in A(p)$, entonces existen m, n enteros no negativos tales que $\mathcal{O}_a = \langle p^m \rangle$ y $\mathcal{O}_b = \langle p^n \rangle$. Como

$$p^{m+n}(a-b) = p^{m+n}a - p^{m+n}b = p^n(p^m a) - p^m(p^n b) = p^n 0 - p^m 0 = 0,$$

por Teorema 2.1 parte (iv) $\mathcal{O}_{a-b} = \left\langle p^k \right\rangle$ para algún entero k que cumple $0 \leq k \leq m+n$. Así, $a - b \in A(p)$. Ahora, sean $a \in A(p)$ y $r \in R$, entonces existe m entero no negativo tal que $\mathcal{O}_a = \langle p^m \rangle$. Además,

$$p^m(ra) = (p^m r)a = (rp^m)a = r(p^m a) = r0 = 0.$$

Por Teorema 2.1 parte (iv) $\mathcal{O}_{ra} = \left\langle p^k \right\rangle$ para algún entero k que cumple $0 \leq k \leq m$. Así, $ra \in A(p)$. Por todo lo anterior $A(p)$ es un submódulo de A.
(ii) Sea $a \neq 0 \in A$ con $\mathcal{O}_a = \langle r \rangle$. Como R es un dominio factorización única (por Teorema 1.11), entonces $r = p_1^{n_1} \cdots p_k^{n_k}$, para ciertos primos distintos p_i de R y ciertos enteros no negativos n_i. Para cada $i \in \{1, ..., k\}$, sea

$$r_i = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k},$$

entonces, $r_1, ..., r_k$ son primos relativos. Por definición de primos relativos y por Teorema 1.12, existen $s_1, ..., s_k$ en R tales que

$$s_1 r_1 + \cdots + s_k r_k = 1.$$

Así,

$$a = 1a = (s_1 r_1 + \cdots + s_k r_k)a = s_1 r_1 a + \cdots + s_k r_k a.$$

Pero, para cada $i \in \{1, ..., k\}$

$$\begin{aligned} p^{n_i} s_i r_i a &= p^{n_i} s_i p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} a \\ &= s_i p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p^{n_i} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} a \\ &= s_i r a = s_i 0 \\ &= 0, \end{aligned}$$

entonces $s_i r_i a \in A(p_i)$. Por lo tanto A es la suma de la familia $\{A(p) : p \in I\}$. Es decir, tal familia cumple la hipótesis (i) del Teorema 1.21. Veamos que dicha familia también cumple la hipótesis (ii) del mismo teorema. En efecto, sea $q \in R$ primo y $A^*(q)$ la suma de la familia

$$\{A(p) : p \text{ es primo en } R \text{ y } p \neq q\}.$$

Si $a \in A(q) \cap A^*(q)$, entonces $a \in A(q)$, por lo tanto $q^m a = 0$ para algún entero no negativo m. Además, como también $a \in A^*(q) \subseteq A$ existen $A(p_1), ..., A(p_t)$ en la familia $\{A(p) : p \in I \text{ y } p \neq q\}$ con $p_1, ..., p_t$ distintos y elementos

$$a_1 \in A(p_1), ..., a_t \in A(p_t),$$

tales que

$$a = a_1 + \cdots + a_t.$$

Entonces existen enteros no negativos $m_1, ..., m_t$ tales que

$$p_1^{m_1} a_1 = 0, ..., p_t^{m_t} a_t = 0.$$

Luego,

$$\begin{aligned}
(p_1^{m_1} \cdots p_t^{m_t})a &= (p_1^{m_1} \cdots p_t^{m_t})(a_1 + \cdots + a_t) \\
&= (p_1^{m_1} \cdots p_t^{m_t})a_1 + \cdots + (p_1^{m_1} \cdots p_t^{m_t})a_t \\
&= (p_2^{m_2} \cdots p_t^{m_t})p_1^{m_1} a_1 + \cdots + (p_1^{m_1} \cdots p_{t-1}^{m_{t-1}})p_t^{m_t} a_t \\
&= (p_2^{m_2} \cdots p_t^{m_t})0 + \cdots + (p_1^{m_1} \cdots p_{t-1}^{m_{t-1}})0 \\
&= 0.
\end{aligned}$$

Ahora, si $d = p_1^{m_1} \cdots p_t^{m_t}$, tenemos que d y q^m son primos relativos, luego por Teorema 1.12 existen r, s en R tales que $rq^m + sd = 1$. Así,

$$a = 1a = (rq^m + sd)a = rq^m a + sda = r0 + s0 = 0.$$

Por lo tanto $A(q) \cap A^*(q) = \{0\}$. Concluimos, por Teorema 1.21, que

$$A = \bigoplus_{p \in I} A(p).$$

(*iii*) Si A es finitamente generado, entonces existe un subconjunto finito

$$X = \{a_1, ..., a_n\},$$

de A, tal que $A = \langle X \rangle$. Como $A = \bigoplus_{p \in I} \sum A(p)$, entonces existen

$$p_{11}, ...p_{1k_1}, ..., p_{n1}, ..., p_{nk_n}$$

primos de R tales que

$$a_1 \in \bigoplus_{j=1}^{k_1} A(p_{1j}), ..., a_n \in \bigoplus_{j=1}^{k_n} A(p_{nj}).$$

Luego, existe un conjunto finito $\{p_1, ..., p_s\}$ constituido por primos de R tal que

$$X \subseteq \bigoplus_{j=1}^{s} A(p_j).$$

Como el submódulo de A generado por X es A mismo, tenemos que A es la intersección de todos los submódulos de A que contienen a X y como además el submódulo $\bigoplus_{j=1}^{s} A(p_j)$ de A contiene a X, entonces

$$A \subseteq \bigoplus_{j=1}^{s} A(p_j) \subseteq A.$$

Por lo tanto, tenemos la suma directa $A = \bigoplus_{j=1}^{s} A(p_j)$ y sólo un número finito de los $A(p)$ con p primo en R son no nulos. ■

Definición 2.6. *Sea A un $R-$módulo y $r \in R$. Definimos al conjunto rA como*

$$rA = \{ra : a \in A\}.$$

Para determinar la estructura de los módulos finitamente generados tales que todo elemento tiene orden una potencia de un primo p (como los $A(p)$ en el Teorema 2.4), necesitaremos el siguiente teorema.

Teorema 2.5. *Sean A un módulo sobre un dominio de ideales principales R, p un primo de R tal que $p^n A = \{0\}$ y $p^{n-1} A \neq \{0\}$ para un cierto entero positivo n y $a \in A$ un elemento de orden p^n. Entonces*

(*i*) *Si* $A \neq Ra$, *entonces existe un elemento no cero* $b \in A$ *tal que*

$$Ra \cap Rb = \{0\}.$$

(*ii*) *Existe un submódulo* C *de* A *tal que*

$$A = Ra \oplus C.$$

Demostración. (*i*) Como $A \neq Ra$, existe $c \in A - Ra$. Como $p^n c = 0 \in Ra$ porque $p^n A = \{0\}$, luego existe j el menor entero positivo tal que $p^j c \in Ra$, así $p^{j-1}c \notin Ra$.
Caso 1. Si $p^j c = 0$, entonces $b = p^{j-1}c \notin Ra$. Supongamos que $Ra \cap Rb \neq \{0\}$, entonces existe $s \in R - \{0\}$ tal que $0 \neq sb \in Ra$. Notar que p no divide a s, ya que en caso contrario existiría $r \in R - \{0\}$ tal que

$$0 \neq sb = (rp)b = (rp)(p^{j-1}c) = rp^j c = r0 = 0,$$

lo cual es una contradicción. Como

$$pb = p(p^{j-1}c) = pp^{j-1}c = p^j c = 0,$$

p es irreducible, $s \neq 0$ y p no divide a s, entonces s y p^n son primos relativos y por Teorema 1.12 existen $x, y \in R$ tales que

$$1 = sx + p^n y.$$

Como $p^n A = \{0\}$, tenemos que $1 = sx$. Luego,

$$b = 1b = (sx)b = x(sb) \in Ra,$$

lo cual es una contradicción. Así, $Ra \cap Rb = \{0\}$.
Caso 2. Si $p^j c = ra$ con r unidad. Entonces existe $s \in R - \{0\}$ tal que $sr = 1$. Luego,

$$0 = s0 = s(p^n c) = sp^{n-j}(p^j c) = sp^{n-j}(ra) = (sr)p^{n-j}a = p^{n-j}a,$$

lo cual contradice el resultado del Teorema 2.1 parte (v). Así, $p^j c = ra$ con r unidad es imposible.

Caso 3. Si $p^j c = ra$ con r no cero, r no unidad y p no divide a r.

$$0 = p^n c = p^{n-j}(p^j c) = p^{n-j}(ra) = rp^{n-j}a.$$

Entonces $rp^{n-j} \in \mathcal{O}_a = \langle p^n \rangle$, por lo tanto existe $s \in R - \{0\}$ tal que

$$rp^{n-j} = sp^n.$$

Por Teorema 1.11 R es un dominio de factorización única y por Teorema 1.10 p es irreducible, $j \geq 1$ y p no divide a $r \neq 0$, entonces $rp^{n-j} = sp^n$ es una contradicción. Luego, $p^j c = ra$ con r no cero, no unidad y p no divide a r es imposible.

Caso 4. Si $p^j c = ra$ con r no cero, no unidad y p divide a r. Sea $k \geq 1$ tal que la máxima potencia de p que divide a r es p^k. Luego, $r = s_1 p^k$ para algún $s_1 \in R - \{0\}$ y tal que p no divide a s_1. Ahora,

$$0 = p^n c = p^{n-j}(p^j c) = p^{n-j}(ra) = rp^{n-j}a = s_1 p^k p^{n-j} a = s_1 p^{k+n-j} a.$$

Entonces $s_1 p^{k+n-j} \in \mathcal{O}_a = \langle p^n \rangle$, por lo tanto existe $s_2 \in R - \{0\}$ tal que

$$s_1 p^{k+n-j} = s_2 p^n.$$

Como R es un dominio de factorización única, p es irreducible y p no divide a $s_1 \neq 0$, entonces por Teorema 2.1 parte (v) $k + n - j \geq n$, lo cual implica que $k \geq j \geq 1$. Así, $b = p^{j-1}c - s_1 p^{k-1}a$ es un elemento bien definido de A. Ahora, $b \neq 0$ porque $p^{j-1}c \notin Ra$ y $s_1 p^{k-1}a \in Ra$. Además,

$$pb = p(p^{j-1}c - s_1 p^{k-1}a) = p^j c - s_1 p^k a = p^j c - p^j c = 0.$$

Supongamos ahora que $Ra \cap Rb \neq \{0\}$, entonces existe $s_3 \in R$ tal que $s_3 b \in Ra - \{0\}$. Como $s_3 b \neq 0$ y $pb = 0$, entonces p no divide a s_3. Luego, s_3 y p^n son primos relativos y por Teorema 1.12 existen $x, y \in R$ tales que

$$1 = s_3 x + p^n y = s_3 x.$$

Así,

$$b = 1b = s_3 x b = x(s_3 b) \in Ra.$$

Consecuentemente,

$$p^{j-1}c = b + s_1 p^{k-1}a \in Ra. \tag{2.1}$$

Si $j-1 \neq 0$, entonces la igualdad en (2.1) contradice la minimalidad de j, y si $j-1=0$, entonces la igualdad en (2.1) contradice el hecho de que $c \notin Ra$. Por lo tanto, $Ra \cap Rb = \{0\}$.

(ii) Si $A = Ra$, entonces se puede tomar $C = \{0\}$. Si $A \neq Ra$, entonces sea $\mathcal{S}$ el conjunto de todos los submódulos B de A tal que $Ra \cap B = \{0\}$. Por (i) existe $b \in A$ tal que $Ra \cap Rb = \{0\}$, por lo tanto $\mathcal{S}$ es no vacío. Como $\mathcal{S}$ está parcialmente ordenado por inclusión y toda cadena en $\mathcal{S}$ tiene una cota superior en $\mathcal{S}$. Por Lema de Zorn existe un submódulo C de A que es maximal en $\mathcal{S}$. Consideremos el módulo cociente A/C. Claramente $p^n(A/C) = \{C\}$ y $p^n(a+C) = \{C\}$. Como $Ra \cap C = \{0\}$ y $p^{n-1}a \neq 0$, tenemos que $p^{n-1}(a+C) \neq C$, de dónde $a+C$ tiene orden p^n en A/C y $p^{n-1}(A/C) \neq \{C\}$. Ahora, si A/C no es el $R-$módulo cíclico generado por $a+C$ (esto es, $A/C \neq R(a+C)$), entonces por (i) existe $d+C \in A/C$ tal que $d+C \neq C$ y $R(a+C) \cap R(d+C) = \{C\}$. Como $Ra \cap C = \{0\}$, se sigue que $Ra \cap (Rd+C) = \{0\}$. Como $d \notin C$, $Rd+C$ está en $\mathcal{S}$ y contiene propiamente a C, lo cual contradice la maximalidad de C. Por lo tanto, A/C es el $R-$módulo cíclico generado por $a+C$ (esto es, $A/C = R(a+C)$). Consecuentemente, $A = Ra + C$, entonces $A = Ra \oplus C$ por Teorema 1.21. ■

Teorema 2.6. *Sea A un $R-$módulo finitamente generado sobre un dominio de ideales principales R tal que todo elemento de A tiene orden una potencia de algún primo $p \in R$. Entonces A es una suma directa de $R-$módulos cíclicos de ordenes $p^{n_1}, ..., p^{n_k}$ respectivamente, donde*

$$n_1 \geq n_2 \geq \cdots \geq n_k \geq 1.$$

Demostración. La demostración se hará por inducción sobre el número $r-1$ de generadores de A. El caso $r=1$ es trivial. Si $r>1$, entonces A es generado por elementos $a_1, a_2, ..., a_r$ cuyos ordenes son respectivamente $p^{n_1}, p^{m_2}, ..., p^{m_r}$. Asumamos que

$$n_1 = \text{máx}\{n_1, m_2, ..., m_r\}.$$

Entonces $p^{n_1}A = \{0\}$ y $p^{n_1-1}A \neq \{0\}$. Por Teorema 2.5 parte (ii) existe un submódulo C de A tal que $A = Ra_1 \oplus C$. Sea

$$\begin{array}{rccc} \pi & : & A = Ra_1 \oplus C & \longrightarrow & C \\ & & a = ra_1 + c & \longrightarrow & c \end{array}.$$

Entonces π es un epimorfismo de $R-$módulos. Como A es generado por $a_1, a_2, ..., a_r$, C debe ser generado por $\pi(a_1), \pi(a_2), ..., \pi(a_r)$. Pero

$$\pi(a_1) = \pi(1a_1 + 0) = 0,$$

de donde C puede ser generado por $r-1$ o menos elementos. La hipótesis de inducción implica que C es una suma directa de $R-$módulos cíclicos de ordenes $p^{n_2}, p^{n_3}, ..., p^{n_k}$ respectivamente, con $n_2 \geq n_3 \geq \cdots \geq n_k \geq 1$. Así, C tiene un elemento de orden p^{n_2}. Como $p^{n_1}A = \{0\}$, tenemos que $p^{n_1}C = \{0\}$, por lo tanto $n_1 \geq n_2$. Como Ra_1 es un $R-$módulo cíclico de orden p^{n_1}, A es una suma directa de $R-$módulos cíclicos de ordenes $p^{n_1}, p^{n_2}, ..., p^{n_k}$ respectivamente, donde $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$. ■

Los Teoremas 2.3, 2.4 y 2.6 determinan una importante descomposición de los módulos finitamente generados sobre dominios de ideales principales. Una segunda descomposición, como suma directa de submódulos cíclicos, de ese tipo de módulos existe y será nuestro siguiente objetivo obtenerla, para ello necesitaremos el siguiente teorema.

Teorema 2.7. *Sean R un dominio de ideales principales y A un $R-$módulo.*

(i) *Si $r \in R$, entonces*

$$rA = \{ra : a \in A\} \quad y \quad A[r] = \{a \in A : ra = 0\}$$

son submódulos de A.

(ii) *Si p es un primo de R, entonces $R/\langle p\rangle$ es un campo y $A[p]$ es un espacio vectorial sobre $R/\langle p\rangle$.*

(iii) *Si n es un entero positivo, entonces*

$$(R/\langle p^n\rangle)[p] \cong R/\langle p\rangle$$

Además, si m es un entero no negativo tal que $0 \leq m < n$

$$p^m(R/\langle p^n\rangle) \cong R/\left\langle p^{n-m}\right\rangle.$$

(*iv*) *Sean $r \in R$ y A_i con $i \in I$ una familia de submódulos de A tales que $A = \bigoplus_{i\in I} A_i$. Entonces*

$$rA = \bigoplus_{i\in I} rA_i \quad y \quad A[r] = \bigoplus_{i\in I} A_i[r].$$

(*v*) *Si B un $R-$módulo tal que $A \cong B$ y p un primo de R, entonces*

$$A_t \cong B_t \quad y \quad A(p) \cong B(p).$$

Demostración. (i) Veamos que rA es un submódulo de A. En efecto,

$$0 = r0 \in rA,$$

por lo tanto rA es no vacío. Sean $a_1, a_2 \in A$, entonces

$$(ra_1) - (ra_2) = r(a_1 - a_2) \in rA.$$

Finalmente, sean $s \in R$ y $a \in A$, entonces

$$s(ra) = (sr)a = (rs)a = r(sa) \in rA,$$

Por lo anterior rA es un submódulo de A.
Veamos que $A[r]$ es un submódulo de A. En efecto, como $r0 = 0$, entonces $0 \in A[r]$, por lo tanto $A[r]$ es no vacío. Sean $a_1, a_2 \in A[r]$, entonces

$$r(a_1 - a_2) = ra_1 - ra_2 = 0 - 0 = 0,$$

así $a_1 - a_2 \in A[r]$. Finalmente, sean $s \in R$ y $a \in A[r]$, entonces

$$r(sa) = (sr)a = s(ra) = s0 = 0,$$

así $sa \in A[r]$. Por lo anterior $A[r]$ es un submódulo de A.
(ii) Veamos que $R/\langle p\rangle$ es un campo. En efecto, por Teorema 1.10 parte (ii) tenemos que p es irreducible, entonces por Teorema 1.10 parte (i) tenemos que $\langle p\rangle$ es un ideal maximal de R, luego por Teorema 1.8 $R/\langle p\rangle$ es un campo.

Veamos que $A[p]$ es un espacio vectorial sobre $R/\langle p\rangle$. En efecto, por (i) $A[p]$ es un submódulo del $R-$módulo A, entonces $A[p]$ es un grupo abeliano con la suma en A restringida a $A[p]$. Ahora, si $a \in A[p]$ y $r \in R$ tenemos que $ra \in A[p]$ porque $A[p]$ es un submódulo de A, y si $r, s \in R$ y $a \in A[p]$ son tales que $r + \langle p\rangle = s + \langle p\rangle$ en $R/\langle p\rangle$, entonces

$$\begin{aligned}
r - s \in \langle p\rangle &\implies r - s = r_1 p \text{ para algún } r_1 \in R \\
&\implies r = r_1 p + s \text{ para algún } r_1 \in R \\
&\implies ra = (r_1 p + s)a \text{ para algún } r_1 \in R \\
&\implies ra = r_1(pa) + sa \text{ para algún } r_1 \in R \\
&\implies ra = r_1(0) + sa \text{ para algún } r_1 \in R \\
&\implies ra = sa.
\end{aligned}$$

Luego, la función

$$\begin{aligned}
R/\langle p\rangle \times A[p] &\longrightarrow A[p] \\
(r + \langle p\rangle, a) &\longmapsto ra
\end{aligned}$$

está bien definida. Consideremos a $r + \langle p\rangle, s + \langle p\rangle \in R/\langle p\rangle$ y $a, b \in A[p]$. Entonces

$$\begin{aligned}
(r + \langle p\rangle)(a + b) &= r(a + b) \\
&= ra + rb \\
&= (r + \langle p\rangle)a + (r + \langle p\rangle)b.
\end{aligned}$$

$$\begin{aligned}
((r + \langle p\rangle) + (s + \langle p\rangle))a &= ((r + s) + \langle p\rangle)a \\
&= (r + s)a \\
&= ra + sa \\
&= ((r + \langle p\rangle)a) + ((s + \langle p\rangle)a).
\end{aligned}$$

$$\begin{aligned}((r+\langle p\rangle)((s+\langle p\rangle)a) &= ((r+\langle p\rangle)((s+\langle p\rangle)a)\\ &= (r+\langle p\rangle)(sa)\\ &= r(sa)\\ &= (rs)a\\ &= (rs+\langle p\rangle)a\\ &= ((r+\langle p\rangle)(s+\langle p\rangle))a.\end{aligned}$$

Además,

$$(1+\langle p\rangle)a = 1a = a.$$

Por lo anterior $A\,[p]$ es un espacio vectorial sobre $R/\langle p\rangle$.

(iii) Consideremos

$$\begin{array}{rccc}\varphi & : & R/\langle p\rangle & \longrightarrow & (R/\langle p^n\rangle)\\ & & r+\langle p\rangle & \longmapsto & rp^{n-1}+\langle p^n\rangle\end{array}.$$

Sean $r, s \in R$ (recordemos que en un dominio entero se cumplen las leyes cancelativas)

$$\begin{aligned}r+\langle p\rangle = s+\langle p\rangle &\iff (r-s)\in\langle p\rangle\\ &\iff r-s = qp \text{ para algún } q\in R\\ &\iff rp^{n-1}-sp^{n-1} = qp^n \in \langle p^n\rangle \text{ para algún } q\in R\\ &\iff rp^{n-1}+\langle p^n\rangle = sp^{n-1}+\langle p^n\rangle\\ &\iff \varphi(r+\langle p\rangle) = \varphi(s+\langle p\rangle).\end{aligned}$$

Luego φ es una función entre $R-$módulos bien definida y además inyectiva. Ahora,

$$\begin{aligned}r+\langle p^n\rangle \in \mathrm{Im}(\varphi) &\implies \varphi(s+\langle p\rangle) = r+\langle p^n\rangle \text{ para algún } s\in R\\ &\implies sp^{n-1}+\langle p^n\rangle = r+\langle p^n\rangle \text{ para algún } s\in R\\ &\implies r-sp^{n-1}\in\langle p^n\rangle \text{ para algún } s\in R\\ &\implies r-sp^{n-1} = qp^n \text{ para ciertos } s,q\in R\\ &\implies r = sp^{n-1}+qp^n = (s+qp)p^{n-1} \text{ para ciertos } s,q\in R\\ &\implies p(r+\langle p^n\rangle) = pr+\langle p^n\rangle = (s+qp)p^n+\langle p^n\rangle = \langle p^n\rangle.\\ &\implies r+\langle p^n\rangle = \langle p^n\rangle\\ &\implies r+\langle p^n\rangle \in (R/\langle p^n\rangle)\,[p].\end{aligned}$$

Así, $\mathrm{Im}(\varphi) \subseteq (R/\langle p^n\rangle)[p]$. Ahora,

$$\begin{aligned}
r+\langle p^n\rangle \in (R/\langle p^n\rangle)[p] &\implies p(r+\langle p^n\rangle) = \langle p^n\rangle \\
&\implies pr+\langle p^n\rangle = \langle p^n\rangle \\
&\implies pr \in \langle p^n\rangle \\
&\implies pr = sp^n \text{ para algún } s \in R \\
&\implies r = sp^{n-1} \text{ para algún } s \in R \\
&\implies r+\langle p^n\rangle = sp^{n-1}+\langle p^n\rangle \text{ para algún } s \in R \\
&\implies r+\langle p^n\rangle = \varphi(s+\langle p\rangle) \text{ para algún } s \in R \\
&\implies r+\langle p^n\rangle \in \mathrm{Im}(\varphi).
\end{aligned}$$

Luego, $(R/\langle p^n\rangle)[p] \subseteq \mathrm{Im}(\varphi)$. Por lo anterior

$$(R/\langle p^n\rangle)[p] = \mathrm{Im}(\varphi).$$

Finalmente, veamos que φ es un homomorfismo de $R-$módulos. En efecto, sean $r+\langle p\rangle$, $s+\langle p\rangle$ en $R/\langle p\rangle$. Entonces

$$\begin{aligned}
\varphi((r+\langle p\rangle)+(s+\langle p\rangle)) &= \varphi((r+s)+\langle p\rangle) \\
&= (r+s)p^{n-1}+\langle p^n\rangle \\
&= (rp^{n-1}+\langle p^n\rangle)+(sp^{n-1}+\langle p^n\rangle) \\
&= \varphi((r+\langle p\rangle)+\varphi((s+\langle p\rangle)).
\end{aligned}$$

Sean $r+\langle p\rangle$ en $R/\langle p\rangle$ y $s \in R$, entonces

$$\begin{aligned}
\varphi(s(r+\langle p\rangle)) = \varphi(sr+\langle p\rangle) = srp^{n-1}+\langle p^n\rangle = s(rp^{n-1}+\langle p^n\rangle) \\
= s\varphi(r+\langle p\rangle).
\end{aligned}$$

Concluimos que

$$(R/\langle p^n\rangle)[p] \cong R/\langle p\rangle.$$

Veamos que $R/\langle p^{n-m}\rangle \cong p^m(R/\langle p^n\rangle)$. Como $R/\langle p^n\rangle = \langle 1+\langle p^n\rangle\rangle$, entonces $p^m(R/\langle p^n\rangle) =$

$\langle p^m + \langle p^n \rangle \rangle$ el cual es un submódulo del $R-$módulo $R/\langle p^n \rangle$. Ahora,

$$\begin{aligned} r \in \mathcal{O}_{p^m+\langle p^n \rangle} &\iff r(p^m + \langle p^n \rangle) = \langle p^n \rangle \\ &\iff rp^m + \langle p^n \rangle = \langle p^n \rangle \\ &\iff rp^m \in \langle p^n \rangle \\ &\iff r = sp^{n-m} \text{ para algún } s \in R \\ &\iff r \in \langle p^{n-m} \rangle . \end{aligned}$$

Así, $\mathcal{O}_{p^m+\langle p^n \rangle} = \langle p^{n-m} \rangle$. Por Teorema 2.1 parte (iii)

$$R/\mathcal{O}_{p^m+\langle p^n \rangle} \cong R(p^m + \langle p^n \rangle).$$

Entonces,

$$R/\left\langle p^{n-m} \right\rangle = R/\mathcal{O}_{p^m+\langle p^n \rangle} \cong R(p^m + \langle p^n \rangle) = \langle p^m + \langle p^n \rangle \rangle = p^m(R/\langle p^n \rangle).$$

(iv) Veamos que $rA = \bigoplus_{i\in I} rA_i$. En efecto, dado que $A = \bigoplus_{i\in I} A_i$, entonces existe un isomorfismo de $R-$módulos $f : A \longrightarrow \bigoplus_{i\in I} A_i$. Si $a \in A$ y

$$f(a) = a_{i_1} + \cdots + a_{i_n}$$

con $n \in \mathbb{Z}^+$, $i_1, ..., i_n \in I$ y $a_{i_1} \in A_{i_1}, ..., a_{i_n} \in A_{i_n}$, entonces

$$f(ra) = rf(a) = r(a_{i_1} + \cdots + a_{i_n}) = ra_{i_1} + \cdots + ra_{i_n} \in \bigoplus_{i\in I} rA_i$$

porque los A_i con $i \in I$ son submódulos de A. Luego, tiene sentido definir

$$\begin{aligned} g \ : \ rA &\longrightarrow \bigoplus_{i\in I} rA_i \\ ra &\longmapsto f(ra). \end{aligned}$$

Si $a, b \in A$,

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

Si $a \in A$ y $s \in S$,

$$\begin{aligned} g(s(ra)) &= g((sr)a) = g((rs)a) = g(r(sa)) \\ &= f(r(sa)) = f((rs)a) = f((sr)a) \\ &= f(s(ra)) = sf(ra) \\ &= sg(ra). \end{aligned}$$

Si $a, b \in A$,

$$\begin{aligned} g(ra) = g(rb) &\implies f(ra) = f(rb) \\ &\implies ra = rb. \end{aligned}$$

Sea $x \in \sum_{i \in I} rA_i$, entonces existen $m \in \mathbb{Z}^+$ y $j_1, ..., j_m \in I$ tales que

$$x = ra_{j_1} + \cdots + ra_{j_m} = r(a_{j_1} + \cdots + a_{j_m})$$

para ciertos $a_{j_1} \in A_{j_1}, ..., a_{j_m} \in A_{j_m}$. Luego, si $c = a_{j_1} + \cdots + a_{j_m}$, entonces $x = rc$ y existe $d \in A$ tal que $f(d) = c$, así

$$g(rd) = f(rd) = rf(d) = rc = x.$$

Por lo anterior g es un isomorfismo de $R-$módulos y así $rA = \bigoplus_{i \in I} rA_i$.
Veamos que $A[r] = \bigoplus_{i \in I} A_i[r]$. En efecto, dado que $A = \bigoplus_{i \in I} A_i$, entonces existe un isomorfismo de $R-$módulos $f : A \longrightarrow \bigoplus_{i \in I} A_i$. Si $a \in A[r]$ tenemos que $ra = 0$ y que existen $i_1, ..., i_n \in I$ tales que $f(a) = a_{i_1} + \cdots + a_{i_n}$, donde $a_{i_1} \in A_{i_1}, ..., a_{i_n} \in A_{i_n}$ y los A_{i_j} son distintos entre si. Luego,

$$0 = f(0) = f(ra) = rf(a) = r(a_{i_1} + \cdots + a_{i_n}) = ra_{i_1} + \cdots + ra_{i_n}.$$

Como los A_i con $i \in I$ son submódulos de A, entonces

$$ra_{i_1} \in A_{i_1}, ..., ra_{i_n} \in A_{i_n}$$

y como la suma $\bigoplus_{i \in I} A_i$ es directa, tenemos que $ra_{i_1} = \cdots = ra_{i_n} = 0$, por lo tanto

$$a_{i_1} \in A_{i_1}[r], ..., a_{i_n} \in A_{i_n}[r]$$

y $f(a) \in \bigoplus_{i\in I} A_i[r]$. Luego, tiene sentido definir

$$\begin{array}{rccc} g & : & A[r] & \longrightarrow & \bigoplus_{i\in I} A_i[r] \\ & & a & \longmapsto & f(a) \end{array}$$

Si $a, b \in A[r]$, entonces

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

Si $a \in A[r]$ y $s \in R$, entonces

$$g(ra) = f(ra) = rf(a) = rg(a).$$

Si $a, b \in A[r]$ son tales que $g(a) = g(b)$, entonces $f(a) = f(b)$, lo cual implica que $a = b$ porque f es un isomorfismo de $R-$módulos.

Si $x \in \bigoplus_{i\in I} A_i[r]$, entonces existen $i_1, ..., i_m \in I$ tales que $x = b_{i_1} + \cdots + b_{i_m}$, donde $b_{i_1} \in A_{i_1}[r], ..., b_{i_m} \in A_{i_m}[r]$. Como f es sobreyectivo, entonces existen $a_{i_1}, ..., a_{i_m} \in A$ tales que $f(a_{i_1}) = b_{i_1}, ..., f(a_{i_m}) = b_{i_m}$. Nótese que para todo $j \in \{1, ..., m\}$,

$$f(ra_{i_j}) = rf(a_{i_j}) = rb_{i_j} = 0.$$

Pero $f(0) = 0$ y f es inyectivo, por lo tanto $ra_{i_j} = 0$ y así $a_{i_j} \in A[r]$. Como $A[r]$ es submódulo de A, entonces $a = a_{i_1} + \cdots + a_{i_m} \in \bigoplus_{i\in I} A[r]$. Luego,

$$\begin{aligned} g(a) = f(a) &= f(a_{i_1} + \cdots + a_{i_m}) = f(a_{i_1}) + \cdots + f(a_{i_m}) \\ &= b_{i_1} + \cdots + b_{i_m} = x. \end{aligned}$$

Por lo anterior g es un isomorfismo de $R-$módulos y así $A[r] = \bigoplus_{i\in I} A_i[r]$.

(v) Como $A \cong B$ existe un isomorfismo de $R-$módulos $f : A \longrightarrow B$.

Veamos que $A_t \cong B_t$. En efecto,

$$\begin{aligned} a \in A_t &\implies \mathcal{O}_a \neq \{0\}, \\ &\implies \exists s \in R - \{0\} : sa = 0, \\ &\implies \exists s \in R - \{0\} : sf(a) = f(sa) = f(0) = 0, \\ &\implies \exists s \in R - \{0\} : s \in \mathcal{O}_{f(a)}, \\ &\implies \mathcal{O}_{f(a)} \neq \{0\}, \\ &\implies f(a) \in B_t. \end{aligned}$$

Luego, tiene sentido definir

$$\begin{array}{rccc} g & : & A_t & \longrightarrow & B_t \\ & & a & \longmapsto & f(a) \end{array}.$$

Si $a, b \in A_t$, entonces

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

Si $r \in R$ y $a \in A_t$, entonces

$$g(ra) = f(ra) = rf(a) = rg(a).$$

Si $a, b \in A_t$ son tales que $g(a) = g(b)$, entonces $f(a) = f(b)$, lo cual implica que $a = b$ porque f es isomorfismo de $R-$módulos.

Finalmente,

$$\begin{aligned} x \in B_t &\implies \mathcal{O}_x \neq \{0\}, \\ &\implies \exists s \in R - \{0\} : sx = 0. \end{aligned}$$

Como f es isomorfismo de $R-$módulos, entonces

$$\begin{aligned} \exists a \in A : f(a) = x &\implies f(sa) = sf(a) = sx = 0, \\ &\implies sa = 0 \text{ porque } f \text{ es isomorfismo de } R - \text{módulos}, \\ &\implies s \in \mathcal{O}_a, \\ &\implies a \in A_t. \end{aligned}$$

Luego, $g(a) = f(a) = x$.

Por lo anterior g es un isomorfismo de $R-$módulos y así $A_t \cong B_t$.

Veamos que $A(p) \cong B(p)$. En efecto,

$$\begin{aligned} a \in A(p) &\implies \mathcal{O}_a = \langle p^n \rangle \text{ para algún entero } n \geq 0, \\ &\implies p^n a = 0, \\ &\implies p^n f(a) = f(p^n a) = f(0) = 0, \\ &\implies \mathcal{O}_{f(a)} = \langle p^j \rangle \ \ 0 \leq j \leq n \text{ por Teorema 2.1 parte } (iv), \\ &\implies f(a) \in B(p). \end{aligned}$$

Luego, tiene sentido definir

$$\begin{array}{rccc} g & : & A(p) & \longrightarrow & B(p) \\ & & a & \longmapsto & f(a) \end{array}$$

Si $a, b \in A(p)$, entonces

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

Si $r \in R$ y $a \in A_t$, entonces

$$g(ra) = f(ra) = rf(a) = rg(a).$$

Si $a, b \in A(p)$ son tales que $g(a) = g(b)$, entonces $f(a) = f(b)$, lo cual implica que $a = b$ porque f es isomorfismo de $R-$módulos.
Finalmente,

$$\begin{array}{rcl} x \in B(p) & \Longrightarrow & \mathcal{O}_x = \langle p^m \rangle \text{ para algún entero } m \geq 0, \\ & \Longrightarrow & p^m x = 0. \end{array}$$

Como f es isomorfismo de $R-$módulos, entonces

$$\begin{array}{rcl} \exists a \in A : f(a) = x & \Longrightarrow & f(p^m a) = p^m f(a) = p^m x = 0, \\ & \Longrightarrow & p^m a = 0 \text{ porque } f \text{ es isomorfismo de } R - \text{módulos}, \\ & \Longrightarrow & \mathcal{O}_a = \left\langle p^k \right\rangle \ 0 \leq k \leq n (\text{ por Teorema 2.1 parte } (iv)), \\ & \Longrightarrow & a \in A(p). \end{array}$$

Luego, $g(a) = f(a) = x$.
Por lo anterior g es un isomorfismo de $R-$módulos y así $A(p) \cong B(p)$. ■

Teorema 2.8. *Sea R un dominio de ideales principales. Si $r \in R$ se puede factorizar como $r = p_1^{n_1} \cdots p_k^{n_k}$ con $p_1, ..., p_k$ primos distintos en R y cada $n_i > 0$ en $\mathbb{Z}$, entonces los $R-$módulos*

$$R/\langle r \rangle \quad y \quad R/\langle p_1^{n_1} \rangle \oplus \cdots \oplus R/\langle p_k^{n_k} \rangle$$

son isomorfos. Consecuentemente, todo $R-$módulo cíclico de orden r es suma directa de k $R-$módulos cíclicos de ordenes $p_1^{n_1}, ..., p_k^{n_k}$ respectivamente.

Demostración. Inicialmente, sean s, t primos relativos en R y veamos que

$$R/\langle st\rangle \cong R/\langle s\rangle \oplus R/\langle t\rangle .$$

En efecto, si $x_1, x_2, y_1, y_2 \in R$ son tales que

$$x_1 + \langle s\rangle = x_2 + \langle s\rangle \quad \text{y} \quad y_1 + \langle t\rangle = y_2 + \langle t\rangle .$$

Entonces $x_1 - x_2 \in \langle s\rangle$ y $y_1 - y_2 \in \langle t\rangle$, por lo tanto existen $x_3, y_3 \in R$ tales que

$$x_1 - x_2 = x_3 s \quad \text{y} \quad y_1 - y_2 = y_3 t,$$

así

$$tx_1 - tx_2 = x_3 st \quad \text{y} \quad sy_1 - sy_2 = y_3 st,$$

luego

$$\begin{array}{ll} tx_1 - tx_2 + sy_1 - sy_2 & \\ = x_3 st + y_3 st & \Longrightarrow \quad (tx_1 + sy_2) - (tx_2 + sy_2) = (x_3 + y_3)st \\ & \Longrightarrow \quad (tx_1 + sy_2) - (tx_2 + sy_2) \in \langle st\rangle \\ & \Longrightarrow \quad (tx_1 + sy_2) + \langle st\rangle = (tx_2 + sy_2) + \langle st\rangle . \end{array}$$

Entonces la función

$$\begin{array}{rccc} \varphi \ : & R/\langle s\rangle \oplus R/\langle t\rangle & \longrightarrow & R/\langle st\rangle \\ & (x + \langle s\rangle \ , \ y + \langle t\rangle) & \longmapsto & (tx + sy) + \langle st\rangle \end{array}$$

está bien definida.

Si $x_1, x_2, y_1, y_2 \in R$, entonces

$$\begin{aligned} &\varphi((x_1 + \langle s\rangle \ , \ y_1 + \langle t\rangle) + (x_2 + \langle s\rangle \ , \ y_2 + \langle t\rangle)) \\ &= \varphi((x_1 + x_2) + \langle s\rangle \ , \ (y_1 + y_2) + \langle t\rangle) \\ &= (t(x_1 + x_2) + s(y_1 + y_2)) + \langle st\rangle \\ &= ((tx_1 + sy_1) + (tx_2 + sy_2)) + \langle st\rangle \\ &= ((tx_1 + sy_1) + \langle st\rangle) + ((tx_2 + sy_2) + \langle st\rangle) \\ &= \varphi(x_1 + \langle s\rangle \ , \ y_1 + \langle t\rangle) + \varphi(x_2 + \langle s\rangle \ , \ y_2 + \langle t\rangle). \end{aligned}$$

Si $x, y, z \in R$, entonces

$$\begin{aligned}\varphi(z(x + \langle s\rangle \ , \ y + \langle t\rangle)) &= \varphi(zx + \langle s\rangle \ , \ zy + \langle t\rangle) \\ &= (tzx + szy) + \langle st\rangle \\ &= z((tx + sy) + \langle st\rangle) \\ &= z\varphi(x + \langle s\rangle \ , \ y + \langle t\rangle).\end{aligned}$$

Si $x_1, x_2, y_1, y_2 \in R$ son tales que

$$\varphi(x_1 + \langle s\rangle \ , \ y_1 + \langle t\rangle) = \varphi(x_2 + \langle s\rangle \ , \ y_2 + \langle t\rangle),$$

así

$$(tx_1 + sy_1) + \langle st\rangle = (tx_2 + sy_2) + \langle st\rangle \,,$$

luego

$$(tx_1 + sy_1) - (tx_2 + sy_2) \in \langle st\rangle \,,$$

entonces existe $x_3 \in R$ tal que

$$(tx_1 + sy_1) - (tx_2 + sy_2) = x_3 st,$$

por lo tanto

$$t(x_1 - x_2) = (x_3 t + (y_2 - y_1))s \quad \text{y} \quad s(y_1 - y_2) = (x_3 s + (x_2 - x_1))t.$$

Como s, t son primos relativos, tenemos que existen $x_4, x_5 \in R$ tales que

$$x_1 - x_2 = x_4 s \quad \text{y} \quad y_1 - y_2 = x_5 t,$$

entonces

$$x_1 - x_2 \in \langle s\rangle \quad \text{y} \quad y_1 - y_2 \in \langle t\rangle \,,$$

así las cosas

$$x_1 + \langle s\rangle = x_2 + \langle s\rangle \quad \text{y} \quad y_1 + \langle t\rangle = y_2 + \langle t\rangle \,,$$

consecuentemente

$$(x_1 + \langle s\rangle \ , \ y_1 + \langle t\rangle) = (x_2 + \langle s\rangle \ , \ y_1 + \langle t\rangle).$$

Para finalizar con esta parte, como s, t son primos relativos, entonces por Teorema 1.12 existen $u, v \in R$ tales que

$$tv + su = 1.$$

Si $z \in R$, entonces $z = suz + tvz$ y

$$\varphi(vz + \langle s \rangle \ , \ uz + \langle t \rangle) = (tvz + suz) + \langle st \rangle = z + \langle st \rangle .$$

Por lo anterior, φ es un isomorfismo de $R-$módulos y

$$R/\langle st \rangle \cong R/\langle s \rangle \oplus R/\langle t \rangle .$$

. Si $r = p_1^{n_1} \cdots p_k^{n_k}$ con $p_1, ..., p_k$ primos distintos en R y cada $n_i > 0$ en $\mathbb{Z}$, entonces por Teorema 1.11 y aplicación reiterada del resultado que probamos al inicio de esta demostración, tenemos que

$$\begin{aligned} R/\langle r \rangle &= R/\langle p_1^{n_1} \cdots p_k^{n_k} \rangle \\ &\cong R/\left\langle p_1^{n_1} \cdots p_{k-1}^{n_{k-1}} \right\rangle \oplus R/\langle p_k^{n_k} \rangle \\ &\vdots \\ &\cong R/\langle p_1^{n_1} \rangle \oplus \cdots \oplus R/\langle p_k^{n_k} \rangle . \end{aligned}$$

Finalmente, si A es un $R-$módulo y $a \in A$ es tal que $\mathcal{O}_a = \langle r \rangle$, entonces por Teorema 2.1 parte (iii) el $R-$módulo cíclico Ra es isomorfo a $R/\mathcal{O}_a$. Luego,

$$Ra \cong R/\mathcal{O}_a \cong R/\langle r \rangle \cong R/\langle p_1^{n_1} \rangle \oplus \cdots \oplus R/\langle p_k^{n_k} \rangle . \blacksquare$$

2.2. TEOREMA DE DESCOMPOSICIÓN DE MÓDULOS

En esta sección encontraremos el teorema de descomposición de módulos sobre dominio de ideales principales, el cual es el objeto de estudio de este trabajo, con su respectiva demostración de manera detallada.

Teorema 2.9. *Sea A un módulo finitamente generado sobre un dominio de ideales principales R. Entonces*

(*i*) *A es isomorfo a un módulo de la forma*

$$R/\langle d_1\rangle \oplus \cdots \oplus R/\langle d_m\rangle \oplus R^n,$$

para ciertos m, n *enteros no negativos y donde* $d_1 \mid d_2 \mid \cdots \mid d_m$ *en* R.

(*ii*) *A también es isomorfo a un módulo de la forma*

$$A(p_1) \oplus \cdots \oplus A(p_k) \oplus R^n, \tag{2.2}$$

donde $p_1, ..., p_k$ *son elementos primos de* R *que dividen a algún* d_i *y*

$$A(p_i) = R/\langle p_i^{\alpha_{i1}}\rangle \oplus \cdots \oplus R/\left\langle p_i^{\alpha_{ic_i}}\right\rangle,$$

$\alpha_{i1} \geq \cdots \geq \alpha_{ic_i}$, $i = 1, ..., k$. *Además, las descomposiciones son únicas.*

Demostración. Por Teorema 2.3,

$$A \cong A_t \oplus F,$$

donde $F = A/A_t$ es un $R-$módulo libre de rango finito. Por Teorema 2.4,

$$A_t \cong A(p_1) \oplus \cdots \oplus A(p_k),$$

donde $p_1, ..., p_k$ son primos en R. Luego,

$$A \cong A(p_1) \oplus \cdots \oplus A(p_k) \oplus F.$$

Por Teorema 2.6 tenemos que para cada $i \in \{1, ..., k\}$ existen $a_{1i}, ..., a_{c_i i} \in R$ tales que

$$A(p_i) \cong Ra_{1i} \oplus \cdots \oplus Ra_{c_i i},$$

donde tenemos que los $R-$módulos cíclicos $Ra_{i1}, ..., Ra_{ic_i}$ son de ordenes $p_i^{\alpha_{i1}}, ..., p_i^{\alpha_{ic_i}}$ respectivamente, y $\alpha_{i1} \geq \cdots \geq \alpha_{ic_i} \geq 1$. Por Teorema 2.1 parte (*iii*) tenemos que para $j \in \{1, ..., c_j\}$

$$Ra_{ij} \cong R/\left\langle p_i^{\alpha_{ij}}\right\rangle.$$

Así,

$$A \cong A(p_1) \oplus \cdots \oplus A(p_k) \oplus F$$

y para cada $i \in \{1, ..., k\}$

$$A(p_i) = R/\langle p_i^{\alpha_{i1}} \rangle \oplus \cdots \oplus R/\left\langle p_i^{\alpha_{ic_i}} \right\rangle,$$

con $\alpha_{i1} \geq \cdots \geq \alpha_{ic_i}$. Ahora, si $\{x_1, ..., x_n\}$ es una base de F, entonces para todo $t \in \{1, ..., n\}$, por Lema 1.8, $Rx_t \cong R$ como $R-$módulos, y por Lema 1.9

$$\begin{aligned} F &\cong Rx_1 \oplus \cdots \oplus Rx_n \\ &\cong R \oplus \cdots \oplus R \\ &= R^n. \end{aligned}$$

Por lo tanto,

$$A \cong A(p_1) \oplus \cdots \oplus A(p_k) \oplus R^n$$

y para cada $i \in \{1, ..., k\}$

$$A(p_i) = R/\langle p_i^{\alpha_{i1}} \rangle \oplus \cdots \oplus R/\left\langle p_i^{\alpha_{ic_i}} \right\rangle,$$

con $\alpha_{i1} \geq \cdots \geq \alpha_{ic_i}$.

Ahora, construimos una matriz de tamaño $m \times k$ donde $m = máx\{c_1, ..., c_k\}$ con los p_i^{ij} antes descritos y completando (si es que es necesario) la parten inferior de algunas columnas con entradas de la forma p_i^0. Así,

$$\begin{bmatrix} p_1^{\alpha_{11}} & p_2^{\alpha_{21}} & \cdots & p_k^{\alpha_{k1}} \\ p_1^{\alpha_{12}} & p_2^{\alpha_{22}} & \cdots & p_k^{\alpha_{k2}} \\ \vdots & \vdots & & \vdots \\ p_1^{\alpha_{1m}} & p_2^{\alpha_{2m}} & \cdots & p_k^{\alpha_{km}} \end{bmatrix}. \tag{2.3}$$

Sean

$$\begin{aligned} d_1 &= p_1^{\alpha_{1m}} p_2^{\alpha_{2m}} \cdots p_k^{\alpha_{km}}, \\ d_2 &= p_1^{\alpha_{1(m-1)}} p_2^{\alpha_{2(m-1)}} \cdots p_k^{\alpha_{k(m-1)}}, \\ &\vdots \\ d_m &= p_1^{\alpha_{11}} p_2^{\alpha_{21}} \cdots p_k^{\alpha_{k1}}. \end{aligned}$$

Por construcción de la matriz en (2.3) y porque $\alpha_{i1} \geq \cdots \geq \alpha_{ic_i}$ para cada $i \in \{1, ..., k\}$, entonces $d_1 \mid d_2 \mid \cdots \mid d_m$. Tenemos que,

$$A \cong A(p_1) \oplus \cdots \oplus A(p_k) \oplus R^n$$

y para cada $i \in \{1, 2, \dots k\}$

$$A(p_i) = R/\langle p_i^{\alpha_{i1}} \rangle \oplus \cdots \oplus R/\left\langle p_i^{\alpha_{ic_i}} \right\rangle,$$

con $\alpha_{i1} \geq \cdots \geq \alpha_{ic_i}$, entonces

$$A(p_1) = R/\langle p_1^{\alpha_{11}} \rangle \oplus \cdots \oplus R/\left\langle p_1^{\alpha_{1c_1}} \right\rangle,$$

$$\vdots$$

$$A(p_k) = R/\langle p_k^{\alpha_{k1}} \rangle \oplus \cdots \oplus R/\left\langle p_k^{\alpha_{kc_k}} \right\rangle,$$

así,

$$A \cong R/\langle p_1^{\alpha_{11}} \rangle \oplus \cdots \oplus R/\left\langle p_1^{\alpha_{1c_1}} \right\rangle \oplus \cdots \oplus R/\langle p_k^{\alpha_{k1}} \rangle \oplus \cdots \oplus R/\left\langle p_k^{\alpha_{kc_k}} \right\rangle \oplus R^n$$

conmutando y asociando adecuadamente tenemos,

$$A \cong R/\langle p_1^{\alpha_{11}} \rangle \oplus \cdots \oplus R/\left\langle p_k^{\alpha_{kc_k}} \right\rangle \oplus \cdots \oplus R/\left\langle p_1^{\alpha_{1c_1}} \right\rangle \oplus \cdots \oplus R/\left\langle p_k^{\alpha_{kc_k}} \right\rangle \oplus R^n$$

conmutando y aplicando el Teorema 2.8 tenemos que

$$A \cong R/\langle d_1 \rangle \oplus \cdots \oplus R/\langle d_m \rangle \oplus R^n..$$

■

Capítulo 3

FORMA CANÓNICA RACIONAL Y DE JORDAN

En este capítulo veremos una aplicación del teorema de descomposición de módulos sobre dominios de ideales principales (Teorema 2.9) a través de las formas canónica racional y de Jordan.

3.1. FORMA CANÓNICA RACIONAL Y FORMA CANÓNICA DE JORDAN

En esta sección utilizaremos el teorema de descomposición de módulos sobre D.I.P. para deducir la forma canónica racional y la forma canónica de jordan, es decir, veremos una aplicación de los $R-$módulos sobre D.I.P. en un campo algebraicamente cerrado. En nuestro caso, trabajaremos en el campo $\mathbb{C}^n$.

Para deducir estas formas canónicas, comenzaremos enunciando definiciones y resultados previos que nos ayudarán a obtener las hipótesis del teorema a aplicar.
Sean V un espacio vectorial de dimensión finita sobre un campo K y

$$\varphi \ : \ V \ \longrightarrow \ V$$

una transformación lineal, entonces podemos dotar a V de una estructura de $K\left[x\right]-$módulos

si definimos:

$$\begin{array}{rccc} \cdot & : & K[x] \times V & \longrightarrow & V \\ & & (p(x), v) & \longmapsto & p(x) \cdot v = (p(\varphi))(v) \end{array}$$

para todo $p(x) \in K[x]$ y $v \in V$. Nótese que

$$x \cdot v = \varphi(v)$$

y sí $k \in K$, $q(x) = k \in K[x]$, entonces

$$q(x) \cdot v = k \cdot v = kv,$$

este último es el producto en el espacio vectorial V.

Lema 3.1. *El $K[x]-$módulo V es finitamente generado.*

Demostración. Toda base de V, como espacio vectorial sobre K, es un conjunto finito generador de V como $K[x]-$módulo. ■

Definición 3.1. *En **anulador** del $K[x]-$módulo V es el conjunto*

$$\{t(x) \in K[x] : t(x) \cdot v = 0 \text{ para todo } v \in V\}.$$

Lema 3.2. *El anulador del $K[x]-$módulo V es un ideal no cero de $K[x]$.*

Demostración. Claramente el anulador del $K[x]-$módulo V es un ideal de $K[x]$. Veamos que tal anulador es no cero. En efecto, sea $\alpha = \{v_1, ..., v_n\}$ una base para V, entonces $\{v_1, ..., v_n\}$ es un conjunto finito de generadores del $K[x]-$módulo V. Además, para ciertos elementos $a_{ij} \in K$.

$$\begin{array}{rcl} x \cdot v_1 & = & \varphi(v_1) = a_{11}v_1 + \cdots + a_{1n}v_n \\ & \vdots & \\ x \cdot v_n & = & \varphi(v_n) = a_{n1}v_1 + \cdots + a_{nn}v_n \end{array} .$$

Luego, las igualdades anteriores las podemos escribir en forma matricial así:

$$\begin{bmatrix} a_{11} - x & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} - x \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{3.1}$$

Si llamamos $\mathbf{A}$ a la matriz $n \times n$ que aparece en la igualdad (3.1), entonces

$$(Adj\mathbf{A})\mathbf{A} \cdot \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \det(\mathbf{A})\mathbf{I}_n \cdot \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = (Adj\mathbf{A}) \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

y así, $\det(\mathbf{A}) \cdot v_i = 0$ para todo $i = 1, ..., n$. Ahora, si

$$p(x) = (-1)^n \det(\mathbf{A}) = x^n + a_{n-1}x^n + \cdots + a_1 x + a_0 \neq 0,$$

entonces $p(x) \cdot v = 0$ para todo $v \in V$. ■

Por Teorema 1.15 $K[x]$ es un dominio de ideales principales, entonces el anulador del $K[x]-$módulo V está generado por un polinomio $q(x) \neq 0$. El polinomio $q(x)$ puede escogerse mónico y en este caso es único y se conoce como el **polinomio minimal** de φ.

Lema 3.3.

$$V \cong \frac{K[x]}{\langle d_1(x) \rangle} \oplus \cdots \oplus \frac{K[x]}{\langle d_m(x) \rangle},$$

donde $d_1(x) \mid d_2(x) \mid \cdots \mid d_m(x)$ *en* $K[x]$ *y los polinomios* $d_i(x)$ *son mónicos.*

Demostración. El Teorema 2.9 parte (i) aplicado a esta situación nos dice que existe un isomorfismo de $K[x]-$módulos

$$f : V \longrightarrow \frac{K[x]}{\langle d_1(x) \rangle} \oplus \cdots \oplus \frac{K[x]}{\langle d_m(x) \rangle} \oplus (K[x])^n, \tag{3.2}$$

donde $d_1(x) \mid d_2(x) \mid \cdots \mid d_m(x)$ en $K[x]$ y los polinomios $d_i(x)$ pueden tomarse mónicos. Si la potencia n que aparece en (3.2) fuera mayor que cero, entonces se tendría que $f^{-1}(0, ..., 0, 1, 0, ..., 0)$ (donde el 1 está en la posición $m + 1$) sería un elemento de V sin torsión, es decir, para todo $r(x) \neq 0$ en $K[x]$,

$$r(x) \cdot f^{-1}(0, ..., 0, 1, 0, ..., 0) \neq 0,$$

lo cual es imposible ya que existe un polinomio $q(x) \neq 0$ (el polinomio minimal de φ) que anula a V. ■

Para $i = 1, ..., m$ sea $w_i = f^{-1}(0, 0, ..., 0, 1 + \langle d_i(x)\rangle, 0, ..., 0)$. Como f^{-1} es un isomorfismo, entonces $f^{-1}\left(\frac{K[x]}{\langle d_i(x)\rangle}\right) = \langle w_i\rangle$ es un submódulo de V y además

$$V = \langle w_1\rangle \oplus \cdots \oplus \langle w_m\rangle$$

Para $i = 1, ..., m$, una base $\langle w_i\rangle$ como espacio vectorial sobre K está dada por

$$\left\{w_i, x \cdot w_i, x^2 \cdot w_i, ..., x^{|d_i(x)|-1} \cdot w_i\right\},$$

donde $|d_i(x)|$ denota el grado del polinomio $d_i(x)$. Probar que este conjunto es una base de $\langle w_i\rangle$, equivale a demostrar que

$$\beta^i = \left\{1 + \langle d_i(x)\rangle, x + \langle d_i(x)\rangle, ..., x^{|d_i(x)|-1} + \langle d_i(x)\rangle\right\}$$

es una base para el $K-$espacio vectorial $\frac{K[x]}{\langle d_i(x)\rangle}$. Dado cualquier $t(x)+\langle d_i(x)\rangle$ en $\frac{K[x]}{\langle d_i(x)\rangle}$, por Teorema 1.14, $t(x) = d_i(x)q_i(x) + t_i(x)$, con $0 < |p_i(x)| < |d_i(x)|$ ó $t_i(x) = 0$. Si $t_i(x) = 0$, entonces

$$t(x) + \langle d_i(x)\rangle = \langle d_i(x)\rangle \in \left\langle 1 + \langle d_i(x)\rangle, x + \langle d_i(x)\rangle, ..., x^{|d_i(x)|-1} + \langle d_i(x)\rangle\right\rangle.$$

Ahora, si $0 < |t_i(x)| < |d_i(x)|$, tenemos que

$$t(x) + \langle d_i(x)\rangle = (d_i(x)q_i(x) + t_i(x)) + \langle d_i(x)\rangle = t_i(x) + \langle d_i(x)\rangle.$$

Veamos que $t_i(x) + \langle d_i(x)\rangle \in \left\langle 1 + \langle d_i(x)\rangle, x + \langle d_i(x)\rangle, ..., x^{|d_i(x)|-1} + \langle d_i(x)\rangle\right\rangle$. Supongamos que $t_i(x) = k_0 + k_1x + \cdots + k_{|d_i(x)|-1}x^{|d_i(x)|-1}$, donde los k_j están en K. Entonces

$$\begin{aligned} t_i(x) + \langle d_i(x)\rangle &= (k_0 + k_1x + \cdots + k_{|d_i(x)|-1}x^{|d_i(x)|-1}) + \langle d_i(x)\rangle \\ &= (k_0 + \langle d_i(x)\rangle) + (k_1x + \langle d_i(x)\rangle) + \cdots \\ &\quad + (k_{|d_i(x)|-1}x^{|d_i(x)|-1} + \langle d_i(x)\rangle) \\ &= k_0(1 + \langle d_i(x)\rangle) + k_1(x + \langle d_i(x)\rangle) + \cdots \\ &\quad + k_{|d_i(x)|-1}(x^{|d_i(x)|-1} + \langle d_i(x)\rangle). \end{aligned}$$

Luego β^i genera a $\frac{K[x]}{\langle d_i(x)\rangle}$ como espacio vectorial sobre K. Por otro lado, si

$$k_0(1 + \langle d_i(x)\rangle) + k_1(x + \langle d_i(x)\rangle) + \cdots + k_{|d_i(x)|-1}(x^{|d_i(x)|-1} + \langle d_i(x)\rangle) = \langle d_i(x)\rangle,$$

entonces $d_i(x) \mid (k_0 + k_1x + \cdots + k_{|d_i(x)|-1}x^{|d_i(x)|-1})$. Como $|d_i(x)| > |d_i(x)| - 1$ tenemos que

$$k_0 + k_1x + \cdots + k_{|d_i(x)|-1}x^{|d_i(x)|-1} = 0,$$

lo que implica que $k_j = 0$ para $j = 1, ..., |d_i(x)| - 1$. Por tanto β^i es un conjunto linealmente independiente en el espacio vectorial $\frac{K[x]}{\langle d_i(x)\rangle}$ sobre K. Lo anterior implica que una base para V está dada por

$$\beta = \left\{w_1, x \cdot w_1, ..., x^{|d_1(x)|-1} \cdot w_1, ..., w_m, x \cdot w_m, \cdots, x^{|d_m(x)|-1} \cdot w_m\right\}.$$

Ahora, si $d_i(x) = a_{0i} + a_{1i}x + \cdots + a_{(|d_i(x)|-1)i}x^{|d_i(x)|-1} + x^{|d_i(x)|}$, entonces como $d_i(x)$ anula a w_i tenemos que

$$\begin{aligned} 0 &= d_i(x) \cdot w_i \\ &= a_{0i} \cdot w_i + a_{1i}x \cdot w_i + \cdots + a_{(|d_i(x)|-1)i}x^{|d_i(x)|-1} \cdot w_i + x^{|d_i(x)|} \cdot w_i, \end{aligned}$$

de donde se sigue que

$$x^{|d_i(x)|} \cdot w_i = -a_{0i} \cdot w_i - a_{1i}x \cdot w_i - \cdots - a_{(|d_i(x)|-1)i}x^{|d_i(x)|-1} \cdot w_i.$$

Por lo anterior, la matriz que representa a φ en la base β, denotada $[\varphi]_{\beta\beta}$, es

$$\begin{bmatrix} \begin{bmatrix} 0 & 0 & \cdots & -a_{01} \\ 1 & 0 & \cdots & -a_{11} \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{(|d_1(x)-1|)1} \end{bmatrix} & & \\ & \ddots & \\ & & \begin{bmatrix} 0 & 0 & \cdots & -a_{0m} \\ 1 & 0 & \cdots & -a_{1m} \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{(|d_1(x)-1|)m} \end{bmatrix} \end{bmatrix}.$$

La matriz $[\varphi]_{\beta\beta}$ se dice que está en **forma canónica racional**.

3.2. FORMA CANÓNICA DE JORDAN

Sea V el $K[x]-$módulo de la sección anterior. Entonces por Teorema 2.9 parte (ii),

$$V \cong \frac{K[x]}{\langle (p_1(x))^{\alpha_{11}} \rangle} \oplus \cdots \oplus \frac{K[x]}{\langle (p_1(x))^{\alpha_{1c_1}} \rangle} \oplus \cdots \oplus \frac{K[x]}{\langle (p_k(x))^{\alpha_{k1}} \rangle} \oplus \cdots \oplus \frac{K[x]}{\langle (p_k(x))^{\alpha_{kc_k}} \rangle}$$

con potencias $\alpha_{11} \geq \alpha_{12} \geq \cdots \geq \alpha_{1c_1}, \alpha_{k1} \geq \alpha_{k2} \geq \cdots \geq \alpha_{kc_k}$. Lo anterior induce una descomposición de V en la forma:

$$V = (\langle v_{11} \rangle \oplus \cdots \oplus \langle v_{1c1} \rangle) \oplus \cdots \oplus (\langle v_{k1} \rangle \oplus \cdots \oplus \langle v_{kc_k} \rangle).$$

Supongamos que $\langle v \rangle \subset V$ y $\langle v \rangle \approx \frac{K[x]}{\langle (p(x))^{\eta} \rangle}$, $\eta > 0$ con $p(x)$ primo en $K[x]$, entonces por Teorema 1.10 parte (ii) $p(x)$ es irreducible en $K[x]$. Si K es algebraicamente cerrado (es decir, todo polinomio no constante de $K[x]$ se puede factorizar en factores lineales), entonces $p(x) = x - \alpha$, para algún $\alpha \in K$. Veamos ahora que

$$\beta' = \left\{ v, (x-\alpha) \cdot v, (x-\alpha)^2 \cdot v, ..., (x-\alpha)^{\eta-1} \cdot v \right\}$$

es una base para $\langle v \rangle$ como espacio vectorial sobre K. En efecto, todo elemento $t(x) \cdot v \in \langle v \rangle$ se puede escribir de la forma $t_1(x) \cdot v$, con $0 < |t_1(x)| < \eta$ ó $t_1(x) = 0$, ya que por Teorema 1.14, $t(x) = (x-a)^{\eta} \cdot l(x) + t_1(x)$, para un cierto $l(x)$ en $K[x]$ y con $0 < |t_1(x)| < \eta$ ó $t_1(x) = 0$. Entonces

$$t(x) \cdot v = l(x) \cdot ((x-a)^{\eta} \cdot v) + t_1(x) \cdot v.$$

Pero, existe un isomorfismo de espacios vectoriales dado por:

$$h : \langle v \rangle \longrightarrow \frac{K[x]}{\langle (x-\alpha)^{\eta} \rangle} = \langle 1 + \langle (x-\alpha)^{\eta} \rangle \rangle$$

Luego, $h(v) = 1 + \langle (x-\alpha)^{\eta} \rangle$ implica que

$$h((x-\alpha)^{\eta} \cdot v) = (x-\alpha)^{\eta} + \langle (x-\alpha)^{\eta} \rangle = \langle (x-\alpha)^{\eta} \rangle .$$

De aquí se sigue que $(x-\alpha)^{\eta} \cdot v = 0$ y por lo tanto,

$$t(x) \cdot v = l(x) \cdot 0 + t_1(x) \cdot v = t_1(x) \cdot v.$$

Ahora, si $t_1(x) = b_0 + b_1x + \cdots + b_tx^t$, con $t < \eta$, entonces

$$t_1(x) = b_0^{'} + b_1^{'}(x-\alpha) + \cdots + b_t^{'}(x-\alpha)^t$$

para ciertos $b_j^{'} \in K$. Luego,

$$t_1(x) \cdot v = b_0^{'}(1 \cdot v) + b_1^{'}((x-\alpha) \cdot v) + \cdots + b_t^{'}((x-\alpha)^t \cdot v).$$

Los elementos de β' son linealmente independientes, ya que si existieran $b_0, b_1, \cdots, b_{\eta-1} \in K$, no todos cero, tales que

$$0 = b_0v + b_1((x-\alpha) \cdot v) + \cdots + b_{\eta-1}((x-\alpha)^{\eta-1} \cdot v),$$

entonces $b_0 + b_1(x-\alpha) + \cdots + b_{\eta-1}(x-\alpha)^{\eta-1}$ sería un polinomio no nulo de grado menor que η que anularía a $\langle v \rangle$. Este polinomio también anularía a $\frac{K[x]}{\langle (x-\alpha)^\eta \rangle}$, lo cual es absurdo. Ahora,

$$\begin{aligned}
\varphi(x) &= x \cdot v = (x-\alpha) \cdot v + \alpha \cdot v \\
\varphi((x-\alpha) \cdot v) &= x \cdot (x-\alpha) \cdot v = (x-\alpha)(x-\alpha) \cdot v + \alpha(x-\alpha) \cdot v \\
&\vdots \\
\varphi((x-\alpha)^k \cdot v) &= x \cdot (x-\alpha)^j \cdot v = (x-\alpha)^{j+1} \cdot v + \alpha(x-\alpha)^j \cdot v.
\end{aligned}$$

Luego,

$$\left[\varphi_{|\langle v \rangle}\right]_{\beta'\beta'} = \begin{bmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 1 & \alpha & 0 & \cdots & 0 \\ 0 & 1 & \alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha \end{bmatrix} = J_\eta(\alpha).$$

Luego, $J_\eta(\alpha)$ es llamada el **bloque de Jordan** asociado a α de tamaño $\eta \times \eta$. La descomposición

$$V = (\langle v_{11} \rangle \oplus \cdots \oplus \langle v_{1c1} \rangle) \oplus \cdots \oplus (\langle v_{k1} \rangle \oplus \cdots \oplus \langle v_{kc_k} \rangle),$$

nos permite tomar una base para el espacio vectorial V sobre K

$$\beta = (\beta_{11} \cup \cdots \cup \beta_{1c_1}) \cup \cdots \cup (\beta_{k1} \cup \cdots \cup \beta_{kc_k}),$$

donde β_{ij} es una base para $\langle v_{ij} \rangle$. Además,

$$[\varphi]_{\beta\beta} = \begin{bmatrix} J_{\alpha_{11}} & & & & & & \\ & \ddots & & & & & \\ & & J_{\alpha_{1c_1}} & & & & \\ & & & \ddots & & & \\ & & & & J_{\alpha_{k1}} & & \\ & & & & & \ddots & \\ & & & & & & J_{\alpha_{kc_k}} \end{bmatrix}$$

con $\alpha_{11} \geq \cdots \geq \alpha_{1c_1}$, $\alpha_{k1} \geq \cdots \geq \alpha_{kc_k}$. La matriz $[\varphi]_{\beta\beta}$ se dice que está en **forma canónica de Jordan**.

Bibliografía

[1] Thomas W. Hungerford, *Álgebra*, Springer-Verlag, 1974.

[2] Lang Serge, *Álgebra*, Addison-Wesley Publishing Company, 1965.

[3] Fraleigh, *Álgebra*, Addison-Wesley Iberoamericana, 1988.

[4] Thomas W. Hungerford, *Introducción Al Álgebra Abstracta* Addison-Wesley Publishing Company.

[5] AM-Carl D. Meyer, *Matrix Analysisand Applied Linear Algebra*

[6] D. Dummit and R. Foote, *Abstract Algebra*, Second Edition, 1999.

[7] Serge Lang, *Undergraduate Algebra*, Second Edition, 2001.

[8] Sara Raissa Silva Rodrigues, *Introducción a la teoría de módulos* Monografía de Iniciación Científica, Belém, 2013.

[9] Domingues Hygino. Iezzi Gelson, *Álgebra Moderna*. São Paulo, Editora Atual, 2003.

[10] Milies Polcino, *Anéis e Módulos*, IME-USP, 1972.