UNIVERSIDAD DEL BÍO-BÍO

FACULTAD DE EDUCACIÓN Y HUMANIDADES

ESCUELA DE PEDAGOGÍA EN EDUCACIÓN MATEMÁTICA

Teoría de Módulos, Forma Canónica Racional Y De Jordan

AUTOR: DIEGO A. PACHECO PANTOJA

PROFESOR GUÍA: EDGARDO RIQUELME FAUNDEZ

MEMORIA PARA OPTAR AL TÍTULO DE PROFESOR DE EDUCACIÓN MEDIA EN EDUCACIÓN MATEMÁTICA

CHILLÁN

Introducción

Una de las finalidades de esta monografía, es el estudio del álgebra lineal de forma más avanzada, particularmente, enfatizaremos el estudio de temas directamente relacionados con los espacios vectoriales y módulos.

En este trabajo se definirán algunas estructuras que nos permitirán entender de mejor forma el papel que toman las estructuras de módulo y de anillos.

Históricamente el uso de módulos fue iniciado por una de las matemáticas más prominentes de la primera parte del siglo XX, Emmy Noether, quien se abrió camino para demostrar el poder y elegancia que posee esta estructura.

Dentro de este estudio, podremos observar que los espacios vectoriales, son un caso particular de módulos, los cuales surgen cuando un anillo subyacente es un cuerpo. La definición de un R - módulo es similar a la definición de una acción de grupo, donde un anillo R cumple el papel del grupo y el módulo M el papel del conjunto.

Este trabajo tiene un interés teórico, de forma que el lector tenga la oportunidad de poder fortalecer su formación matemática y comprensión de algunos conceptos los cuales muchas veces no son tan simples de entender en los cursos de pregrados o simplemente no se profundiza tanto en algunos que son claves para el desarrollo de una buena formación.

El estudio de valores y vectores propios, es un tema con gran cantidad de aplicaciones y se estudia de manera no tan profunda en los cursos de álgebra lineal, para estos conceptos, profundizaremos tanto de forma teórica como práctica, pues los valores y vectores propios nos sirven para entender de manera más profunda las transformaciones lineales.

Otro tema de gran interés, son las formas canónicas de Jordan y como estas nos ayudan a relacionar las matrices con su polinomio característico (y minimal) y viceversa, donde estos nos pueden ayudar a entender resultados de interés teórico, donde el polinomio característico nos puede entregar bastante información sobre el objeto de estudio.

Para esto, podemos tomar un caso particular donde el anillo R es F[x] de los polinomios con coeficientes en un cuerpo F. Luego tomamos un espacio vectorial V de dimensión finita sobre F de dimensión n y sea T una transformación lineal fija de V. Podemos considerar V como un F[x] - módulo, donde sus elementos actúan sobre V como la transformación lineal T.

Del Teorema Fundamental podemos decir que V es isomorfo como un F[x] - módulo a la suma directa de módulos cíclicos. Esta descomposición de V nos permitirá elegir una base para V respecto a la cual la representación matricial para la transformación lineal T se encuentra en una forma simple específica. Cuando usamos los factores invariantes de V para su descomposición, obtenemos la forma canónica racional para la matriz de T, la cual es casi como una matriz diagonal. La parte de unicidad del Teorema Fundamental garantiza que las formas canónicas racional y de Jordan son únicas.

Así es como estudiaremos la ya nombrada forma canónica de Jordan y veremos algunas de sus aplicaciones como lo son la antes mencionada relación con matrices y sus polinomios característicos.

Índice general

CAPÍTULO 1

Módulos

En este primer capítulo definiremos los conceptos de módulo por la izquierda y por la derecha sobre un anillo que, siempre y cuando no se especifique lo contrario, se dirá que es unitario. También definiremos submódulo, módulo cociente y homomorfismo de módulos, mencionando propiedades y teoremas principales que los caracterizan, también profundizaremos un poco en lo que es la generación de módulos, sumas directas y módulos libres, finalizando con módulos sobre dominios de ideales principales donde se definirán algunas condiciones principales y necesarias para estos últimos, demostrando algunos de los teoremas más usados para este tipo de módulos. A grandes rasgos, podemos ver a los módulos como herramientas para estudiar anillos, donde también nos daremos cuenta que un módulo sobre un anillo es la generalización de la noción de un espacio vectorial sobre un cuerpo.
Este capítulo es basado principalmente en [2].

1.1 Teoría básica

Definición 1.

Sea R un anillo (no necesariamente conmutativo ni unitario). Luego sea M un R-módulo izquierdo o un módulo izquierdo sobre R, un conjunto que cumple las siguientes condiciones:

1. *Una operación binaria $+$ en M, donde M cumple con ser un grupo abeliano.*
2. *Una acción de R sobre M, denotado por rm, para todo $r \in R$ y para todo $m \in M$ que satisfacen los siguientes axiomas:*
   a) *$(r+s)m = rm + sm$, para todo $r, s \in R, m \in M$.*
   b) *$(rs)m = r(sm)$, para todo $r, s \in R, m \in M$.*

c) $r(m+n) = rm + rn$, *para todo* $r \in R, m, n \in M$.

Si el anillo R *contiene una unidad, agregamos el siguiente axioma:*

d) $1m = m$, *para todo* $m \in M$.

Observación 1.

1. *Los espacios vectoriales sobre* F*, donde* F *es un cuerpo, es lo mismo que definir un módulo sobre el mismo cuerpo* F*. De esta forma podemos decir que los espacios vectoriales son una particularidad de las estructuras de módulos.*

2. *Luego, como tenemos definida la estructura de módulo, también podremos definir la estructura de submódulo.*

Definición 2.

Sea R *un anillo y* M *un* R*-módulo. Un* R*-submódulo de* M *es un subgrupo* N *de* M *el cual es cerrado bajo la acción de los elementos del anillo, es decir,* $rn \in N$*, para todo* $r \in R$*,* $n \in N$*.*

Observación 2.

Ya que mencionamos que los espacios vectoriales son casos particulares de módulos, y así como los espacios vectoriales poseen subespacios, los módulos también poseen submódulos los cuales son subconjuntos de un módulo M *que cumplen las operaciones restringidas. De esta forma, podemos decir que también, al igual que los espacios vectoriales, cada* R*-módulo posee submódulos triviales.*

Ejemplo 1.

F[x]-módulo

Aplicación a Operadores Lineales

Este es basado principalmente en [3].

¿Cómo podríamos definir la acción de un polinomio?

Sea $f = \sum_{i=0}^{n} a_i x^i \in F[x]$, entonces el elemento $a_0 i + a_1 T + \cdots + a_n T^n$ lo que denotamos como $f(T)$ y V un espacio vectorial. Su efecto sobre un elemento arbitrario $v \in V$, viene dado por:

$$f(\alpha)(v) = a_0 v + a_1 T(v) + \cdots + a_n T^n(v),$$

donde $T^n(v) = T(T(\dots(T(v))\dots))$ con n veces T.
Ahora sea T una Transformación lineal fija. Obtenemos un mapa $F[x] \times V \to V$ definiendo

$$fv = f(T)(v)$$

donde $f \in F[x], v \in V$, lo que nos muestra que este mapa convierte a V en un $F[x]$-módulo.
Verificaremos esto en detalle para mejor entendimiento del lector y para ello haremos un cálculo directo para mostrar que se cumplen los axiomas de módulo.

(a) Sea $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{n} b_i x^i$ ambos elementos de $F[x]$ y $v \in V$. Entonces $f + g = \sum_{i=0}^{n} (a_i + b_i) x^i$, y así:

$$\begin{aligned}(f+g)(v) &= \sum_{i=0}^{n} (a_i + b_i) T^i(v) \\ &= \sum_{i=0}^{n} a_i T^i(v) + \sum_{i=0}^{n} b_i T^i(v) \\ &= fv + gv \qquad \text{(por definición).}\end{aligned}$$

(b) Con la notación anterior tenemos $fg = \sum_{k=0}^{2n} (\sum_{i+j=k} a_i b_i) x^k$, y por lo tanto:

$$\begin{aligned}(fg)v &= \sum_{k=0}^{2n} (\sum_{i+j=k} a_i b_j) T^k(v) \qquad \text{(por definición)} \\ &= (\sum_{i=0}^{n} a_i T^i)(\sum_{j=0}^{n} b_j T^j(v)) \\ &= f(T)(g(T)(v)) \\ &= f(gv).\end{aligned}$$

(c)

$$\begin{aligned}f(v_1 + v_2) &= f(T)(v_1 + v_2) && \text{(por definición)} \\ &= f(T)(v_1) + f(T)(v_2) && \text{(cuando } f(T) \text{ es lineal)} \\ &= fv_1 + fv_2 && \text{(por definición).}\end{aligned}$$

(d) Es inmediato.

Para continuar, veremos otro ejemplo mas particular.

Ejemplo 2.

Sea V un n-espacio afín F^n y sea T un "operador de desplazamiento":

$$T(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, 0)$$

Diremos que e_i es el i-ésimo vector base $(0, 0, \ldots, 0, 1, 0, \ldots, 0, 0)$, donde el 1 se encuentra en la posición i. Entonces:

$$T^k(e_i) = \begin{cases} e_{i-k} & si\ i > k \\ 0 & si\ i \leq k \end{cases}$$

así, por ejemplo, si $m < n$,

$$(a_m x^n + a_{m-1} x^{x-1} + \ldots + a_0) e_n = (0, \ldots, 0, a_m, a_{m-1}, \ldots, a_0)$$

De aquí podemos determinar la acción de un polinomio sobre un vector cualquiera.

Observación 3. *La construcción de un $F[x]$-módulo a partir de un espacio vectorial V sobre F y una transformación lineal T desde V hasta V, de hecho, se describe de esta forma a todos los $F[x]$-módulos; un $F[x]$-módulo es un espacio vectorial junto con una transformación lineal que especifica la acción de x. Esto se debe a que si V es un $F[x]$-módulo, entonces V es un F-módulo y la acción del elemento x del anillo sobre V, es una transformación lineal desde V hasta V.*

Los axiomas para un módulo aseguran que las acciones de F y x en V determinan de manera única la acción de cualquier elemento de $F[x]$ en V. Por lo tanto, existe una biyección entre la colección de $F[x]$-módulos y la colección de pares V, T.

$$\left\{ \begin{array}{c} V\ es\ un\ F[x]\text{-}módulo \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} V\ es\ un\ espacio\ vectorial\ sobre\ F\ y \\ T : V \to V es\ una\ transformación\ lineal \end{array} \right\}$$

dado por el elemento x que actúa sobre V como la transformación lineal T.

Ahora consideramos los $F[x]$-submódulos de V, donde V es cualquier $F[x]$-módulo y T es la transformación lineal desde V hasta V dada por una acción de x. Un $F[x]$-submódulo W de V primero debe ser un F-submódulo, es decir, W debe ser un subespacio vectorial de V. En segundo lugar, W debe enviarse a sí mismo bajo la acción del elemento x del anillo, es decir, debemos tener $T(w) \in W$ para todo $w \in W$.

Definición 3.

Cualquier subespacio vectorial U de V, tal que $T(U) \subseteq U$ se llama T-estable o T-invariante.

Proposición 1.

Si U es cualquier subespacio T-estable de V, se deduce que $T^n(U) \subseteq U$ para todo $n \in \mathbb{Z}^+$.

($T(U) \subseteq U$ implica $T^2(U) = T(T(U)) \subseteq T(U) \subseteq U$). Además, cualquier combinación lineal de potencias de T envía U a U, de modo que U también es estable por la acción de cualquier polinomio en T. Por lo tanto, U es un $F[x]$-submódulo de V.

Observación 4. *Los $F[x]$-módulos de V son precisamente el subespacio T-estable de V. En términos de la biyección anterior tenemos:*

$$\left\{ \begin{array}{c} W \text{ es un } F[x]\text{-submódulo} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} W \text{ es un subespacio vectorial sobre de } V \text{ y} \\ W \text{ es una } T\text{-estable} \end{array} \right\}$$

Lo que da un diccionario completo entre los $F[x]$-módulos de V y los espacios vectoriales V junto con una transformación lineal T desde V hasta V.

Ejemplo 3.

Si T es el operador de desplazamiento definido sobre un n-espacio afín y k es cualquier número entero entre $0 \leq k \leq n$, entonces el subespacio

$$U_k = (x_1, x_2, \ldots, x_k, 0, \ldots, 0) \mid x_i \in F$$

Es claramente T-estable, por lo que es un $F[x]$-submódulo de V.

A continuación se establecerá un criterio para submódulo análogamente al de los subgrupos de un grupo.

Proposición 2.

*(**Criterio de Submódulo**) Sea R un anillo y M un R-módulo. Un subconjunto N de M es un submódulo de M si y solo si:*

1. $N \neq \emptyset$,

2. $x + ry \in N$ para todo $r \in R$ y para todo $x, y \in N$

Demostración.

1. Si N es un submódulo, entonces $0 \in N$, de esta forma $N \neq \emptyset$. Además, N es cerrado bajo la adición y se envía a sí mismo bajo la acción de elementos de R.

2. Recíprocamente, supongamos que 1. y 2. se mantienen. Sea $r = -1$ y se aplica el criterio de subgrupo (en su forma aditiva) para ver que N es un subgrupo de M. En particular, $0 \in N$. Ahora sea $x = 0$ y aplicamos la hipótesis 2. para ver que N se envía a sí mismo bajo la acción de R. Esto establece la proposición.

□

Finalizaremos esta sección con una definición importante.

Definición 4.
Sea R un anillo conmutativo con identidad.

1. *Un R-álgebra es un anillo A con identidad.*
2. *Contiene un homomorfismo de anillo $f : R \to A$.*
3. *Posee un mapa 1_R hasta 1_A.*
4. *El subanillo f(R) de A está contenida en el centro de A.*

Definición 5.
Si A y B son dos R-álgebras, un homomorfismo de R-álgebra es un homomorfismo de anillo, es decir, $\varphi : A \to B$ mapeo 1_A a 1_B tal que $\varphi(r \cdot a) = r \cdot \varphi(a)$ para todo $r \in R$ y $a \in A$.

1.2 Módulo Cuociente y Homomorfismo de Módulo

Esta sección contiene la teoría básica de los Módulos Cociente y Homomorfismos de Módulos.

Definición 6.

Sea R un anillo y sean dos R-módulos M y N.

Un mapa $\varphi : M \to N$ es un homomorfismo de un R-módulo si respeta las estructuras de los R-módulos M y N, es decir:

1. $\varphi(x+y) = \varphi(x) + \varphi(y)$, *para todo* $x, y \in M$.
2. $\varphi(rx) = r\varphi(x)$, *para todo* $r \in R, x \in M$.

Observación 5.

Si R es un cuerpo, el homomorfismo del R-módulo se llama "Transformación lineal".

Definición 7.

Sea R un anillo y sean dos R-módulos M y N.

Un homomorfismo de un R-módulo es un isomorfismo (de un R-módulo) si es inyectivo y sobreyectivo a la vez. Los módulos M y N se dicen que son isomorfos si existe un isomorfismo de un R-módulo $\varphi : M \to N$, y se denota $M \cong N$.

Definición 8.

Sea R un anillo y sean dos R-módulos M y N.

1. *Si $\varphi : M \to N$ es un homomorfismo de un R-módulo, su núcleo es Nuc $\varphi = \{m \in M | \varphi(m) = 0\}$ y sea $\varphi(M) = \{n \in N | n = \varphi(m)$ para algunos $m \in M\}$(la imagen de φ, como es usual).*
2. *Sea M y N dos R-módulos y se define $Hom_R(M, N)$ como generalización de todos los homomorfismos de un R-módulo de M en N.*

Proposición 3.

Sea M y N dos R-módulos.

Un mapa $\varphi : M \to N$ es un homomorfismo de un R-módulo si y solo si $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ para todo $x, y \in M$ y para todo $r \in R$.

Demostración.

Ciertamente $\varphi(rx+y) = r\varphi(x) + \varphi(y)$ si φ es un homomorfismo de un R-módulo. De manera inversa, si $\varphi(rx+y) = r\varphi(x) + \varphi(y)$, tomar $r = 1$ para ver que φ es aditivo y tomar $y = 0$ para ver que φ conmuta con la acción de R sobre M (es decir, es homogéneo). □

Proposición 4.

Sea M y N dos R-módulos.

Sean φ, ψ elementos de $Hom_R(M,N)$. Se define $\varphi + \psi$ como:

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m).$$

Luego $\varphi+\psi \in Hom_R(M,N)$ y con esta operación tenemos que $Hom_R(M,N)$ es un grupo abeliano. Si R es un anillo conmutativo con $r \in R$ se define $r\varphi$ como:

$$(r\varphi)(m) = r(\varphi(m)).$$

Para todo $m \in M$.

Entonces $r\varphi \in Hom_R(M,N)$ y con esta acción del anillo conmutativo R, el grupo abeliano $Hom_R(M,N)$ es un R-módulo.

Demostración.

Observamos que la conmutatividad de R se usa para mostrar que $r\varphi$ satisface el segundo axioma de un homomorfismo de un R-módulo:

$$\begin{aligned}
(r_1\varphi)(r_2 m) &= r_1\varphi(r_2 m) && \text{(por definición de } r_1\varphi) \\
&= r_1 r_2(\varphi(m)) && \text{(ya que } \varphi \text{ es un homomorfismo)} \\
&= r_2 r_1\varphi(m) && \text{(ya que } R \text{ es conmutativo)} \\
&= r_2(r_1\varphi(m)) && \text{(por definición de } r_1\varphi).
\end{aligned}$$

La verificación de los axiomas se basan en la hipótesis que N es un R-módulo. Para esto, el dominio M podría ser cualquier conjunto, no necesariamente tiene que ser un R-módulo ni un grupo abeliano. □

¿Qué estructura tiene $Hom_R(M,N)$?

Proposición 5.

Sea M, N y L tres R-módulos.

1. *Si $\varphi \in Hom_R(L, M)$ y $\psi \in Hom_R(M, N)$ entonces $\psi \circ \varphi \in Hom_R(L, N)$.*

2. *Con la adición y multiplicación definida como composición de funciones, $Hom_R(M, M)$ es un anillo con 1. Cuando R es conmutativo $Hom_R(M, M)$ es un R-álgebra.*

Demostración.

1. Dado φ y ψ como se indican, $r \in R$, y $x, y \in L$. Luego

$$\begin{aligned}(\psi \circ \varphi)(rx + y) &= \psi(\varphi(rx + y)) \\ &= \psi(r\varphi(x) + \varphi(y)) && \text{(por (1) aplicado en } \varphi) \\ &= r\psi(\varphi(x)) + \psi(\varphi(y)) && \text{(por (1) aplicado en } \psi) \\ &= r(\psi \circ \varphi)(x) + (\psi \circ \varphi)(y)\end{aligned}$$

   Entonces, por proposición 3, $\psi \circ \varphi$ es un homomorfismo de un R-módulo.

2. Al tomar en cuenta que el dominio y codominio de los elementos de $Hom_R(M, M)$ son iguales, la función composición está definida. Por (1), es una operación binaria en $Hom_R(M, M)$. Como es usual, la función composición es asociativa. La función identidad, I, (como siempre, $I(x) = x$, para todo $x \in M$) se ve como la identidad multiplicativa de $Hom_R(M, M)$. Si R es conmutativo, en proposición 4 muestra que el anillo $Hom_R(M, M)$ es un R-Módulo izquierdo, definiendo $\varphi r = r\varphi$ para todo $\varphi \in Hom_R(M, M)$ y $r \in R$, lo que hace convertir a $Hom_R(M, M)$ en un R-álgebra.

□

Definición 9.

Anillo de Endomorfismo

El anillo $Hom_R(M, M)$ es llamado endomorfismo del anillo M, generalmente se denota como $End_R(M)$ o simplemente $End(M)$ cuando el anillo R tiene un contexto definido. Los elementos de $End(M)$ son llamados endomorfismos.

Proposición 6.

Sea R un anillo, M es un R-módulo y N un submódulo de M. El grupo cociente M/N puede convertirse en un R-módulo definiendo una acción de los elementos de R mediante:

$$r(x + N) = (rx) + N, \text{ para todo } r \in R, x + N \in M/N.$$

La proyección natural del mapa $\pi : M \to M/N$ definida por $\pi(x) = x + N$ es un homomorfismo de un R-módulo con Núcleo N.

Demostración.

Cuando M es un grupo abeliano bajo + (adición), el grupo cociente M/N se encuentra definido y es un grupo abeliano. Para ver que la acción del elemento r del anillo sobre el coset $x+N$ está bien definida, supongamos $x+N = y+N$, es decir, $x-y \in N$. Cuando N es un R-submódulo, $r(x-y) \in N$. Así $rx-ry \in N$ y $rx + N = ry + N$, como se desea. Ahora cuando la operación en M/N es compatible con las de M, el axioma para un R-módulo son simples de comprobar de la misma forma que se hizo para el grupo cociente. Por ejemplo, el axioma 2(b) se mantiene de la siguiente forma: para todo $r_1, r_2 \in R$ y $x + N \in M/N$, por definición de acción de elementos de anillo en elementos de M/N.

$$\begin{aligned}(r_1r_2)(x + N) &= (r_1r_2x) + N \\ &= r_1(r_2x + N) \\ &= r_1(r_2(x + N)).\end{aligned}$$

El otro axioma podemos probarlo de forma similar. Finalmente, la proyección natural del mapa π descrito anteriormente, particularmente, la proyección natural del grupo abeliano M sobre el grupo abeliano M/N es por lo tanto un homomorfismo de grupo con Núcleo N. El Núcleo de cualquier homomorfismo de módulo es el mismo que el Núcleo cuando vemos un homomorfismo de un grupo abeliano. Sólo queda por mostrar que π es un homomorfismo de módulo, es decir, $\pi(rm) = r\pi(m)$.

$$\begin{aligned}\pi(rm) &= rm + N \\ &= r(m + N)(\text{por definición de accion de R sobre M/N}) \\ &= r\pi(m).\end{aligned}$$

Aquí queda completa la demostración. □

Para establecer el segundo teorema de isomorfismo necesitamos lo siguiente:

Definición 10.

Sea A,B dos submódulos de un R-módulo M. La suma de A y B es el conjunto

$$A + B = \{a + b | a \in A, b \in B\}.$$

No es complicado demostrar que la suma de dos submódulos A y B es un submódulo y es el submódulo mas pequeño que contiene a A y B.

Teorema 1.

Teoremas de Isomorfismos

1. *Sea M y N dos R-módulos y $\varphi : M \to N$ un homomorfismo de un R-módulo. Luego $Nuc\varphi$ es un submódulo de M y $M/Nuc\varphi \cong \varphi(M)$.*

2. *Sea A, B dos submódulos de un R-módulo M. Luego $(A+B)/B \cong A/(A \cap B)$.*

3. *Sea M un R-módulo, donde A y B son submódulos de M con $A \subseteq B$. Luego $(M/A)/(B/A) \cong M/B$.*

4. *Sea N un submódulo de un R-módulo M. Existe una biyección entre los submódulos de M que contienen a N y los submódulos de M/N. La correspondencia está dada por $A \longleftrightarrow A/N$, para todo $A \supseteq N$. Esta correspondencia conmuta con los procesos de sumas e intersecciones. (Es decir, es un isomorfismo entre la red de submódulos de M/N y la red de submódulos de M que contienen a N).*

Demostración: ver [6] teoremas 7.8, 7.9, 7.10, 7.11.

1.3 Generación de Módulos, Sumas Directas y Módulos Libres

¿Cómo Podríamos Construir un Submódulo?

Sea R un anillo con 1 (unitario). Al igual que en la sección antes vista, el término módulo significará módulo izquierdo. Primero extenderemos la noción de la suma de dos submódulos a sumas de cualquier número finito de submódulos y luego definimos el submódulo generado por el subconjunto.

Definición 11.

Sea M un R-módulo y $N_1, \ldots, N_n$ submódulos de M.

1. *La suma de $N_1, \ldots, N_n$ es el conjunto de todas las sumas finitas de los elementos de los conjuntos N_i: $\{a_1 + a_2 + \ldots + a_n | a_i \in N_i$ para todo $i\}$. Esta suma se denota por $N_1 + \ldots + N_n$.*

2. *Para cualquier subconjunto A de M diremos que:*

$$< A >= RA = \{r_1a_1 + r_2a_2 + \ldots + r_ma_m | r_1, \ldots, r_m \in R, a_1, \ldots, a_m \in A, m \in \mathbb{Z}^+\}.$$

(Donde por convención $RA = \{0\}$ si $A = \varnothing$). Si A es el conjunto finito $\{a_1, a_2, \ldots, a_n\}$ debemos escribir $Ra_1 + Ra_2 + \ldots + Ra_n$ para RA. Llamaremos RA al submódulo de M generado por A. Si N es un submódulo de M y $N=RA$, para algunos subconjuntos A de M, llamaremos a A como conjunto de generadores para N, y así podemos decir que N es generado por A.

Definición 12.

Importante.

Un submódulo N de M es finitamente generado si hay un subconjunto finito A de M tal que $N=RA$, es decir, si N es generado por algún subconjunto finito.

Un submódulo N de M es cíclico si es que allí existe un elemento $a \in M$ tal que $N=RA$, es decir, si N es generado por un elemento:

$$N = RA = \{ra | r \in R\}.$$

Ejemplo 4.

Sea F un cuerpo, x una variable o indeterminada, V un espacio vectorial sobre F y T una transformación lineal de V a V. Convertimos a V en un $F[x]$-módulo a través de T. Luego, tenemos que V es un $F[x]$-módulo cíclico (con generador v), si y solo si $V = \{p(x)v \mid p(x) \in F[x]\}$, es decir, si y solo si cada elemento de V puede escribirse como una combinación F-lineal de elementos del conjunto $\{T^n(v) \mid n \geq 0\}$. Esto a su vez equivale a decir $\{v, T(v), T^2(v), \ldots\}$ abarca a V como un espacio vectorial sobre F.

En el caso donde T es la transformación lineal de identidad de V a V, entonces para cada $v \in V$ y cada $p(x) \in F[x]$ tenemos $p(x)v = \alpha v$ para algún $\alpha \in F$. Por lo tanto, si V tiene una dimensión > 1, V no puede ser un $F[x]$-módulo cíclico.

Definición 13.

Sea $M_1, \ldots, M_k$ una colección de R-módulos. La colección de las k-tuplas $(m_1, m_2, \ldots, m_k)$ donde $m_i \in M_i$ con adición y acción de R, es llamada "Producto Directo" de $M_1, \ldots, M_k$, denotado como $M_1 \times \cdots \times M_k$.

Es evidente que el producto directo de una colección de R-módulos es nuevamente un R-módulo. El producto directo de $M_1, \ldots, M_k$ también se conoce como la suma directa (externa) de $M_1, \ldots, M_k$ y es denotada como $M_1 \oplus \cdots \oplus M_k$.

La siguiente proposición indica cuando un módulo es isomorfo al producto directo de algunos de sus submódulos y es el análogo de los módulos del teorema que determina cuándo un grupo es el producto directo de dos de sus subgrupos.

Proposición 7.

Sea $N_1, N_2, \ldots, N_k$ submódulos de un R-módulo M. Entonces se cumplen las siguientes equivalencias:

1. *El mapa $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ definido por*

$$\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$$

   es un isomorfismo (de un R-módulo):

   $N_1 + N_2 + \cdots + N_k \cong N_1 \times N_2 \times \cdots \times N_k$.

2. $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ *para todo* $j \in \{1, 2, \cdots, k\}$.

3. *Cada $x \in N_1 + \cdots + N_k$ puede escribirse de manera única de la forma $a_1 + a_2 + \cdots + a_k$ con $a_i \in N_i$.*

Demostración.

Para probar la condición 1. implica que se cumpla 2., supongamos que para algunos j la condición 2. falla y $a_j \in (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) \cap N_j$ con $a_j \neq 0$. Luego

$$a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k$$

para algunos $a_i \in N_i$, y $(a_1, \ldots, a_{j-1}, -a_j, a_{j+1} + \ldots + a_k)$ sería un elemento de Nuc π distinto de cero, entonces tenemos una contradicción.

Supongamos ahora que la condición 2. si se cumple. Si para algunos elementos del módulo $a_i, b_i \in N_i$ tenemos

$$a_1 + a_2 + \cdots + a_k = b_1 + b_2 + \cdots + b_k$$

luego, para cada j tenemos que:

$$a_j - b_j = (b_1 - a_1) + \cdots + (b_{j-1} - a_{j-1}) + (b_{j+1} - a_{j+1}) + \cdots + (b_k - a_k).$$

El lado izquierdo de la ecuación se encuentra en N_j y el lado derecho está en $N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k$.

Por lo tanto

$$a_j - b_j \in N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0.$$

Esto muestra que $a_j = b_j$ para todo j, y así se cumple la condición 2. y esta implica que se cumpla 3.

Finalmente, podemos ver que 3. implica a 1., ya que si observamos primero, el mapa π es claramente un homomorfismo de un R-módulo sobreyectivo. Entonces 3. simplemente implica que π es inyectivo, por lo tanto es un isomorfismo completando así la demostración. □

Si un R-módulo $M = N_1 + N_2 + \cdots + N_k$ es la suma de los submódulos $N_1, N_2, \ldots, N_k$ de M que satisfacen las condiciones equivalentes de la proposición anterior, entonces se dice que M es la suma directa (interna) de $N_1, N_2, \ldots, N_k$, y se escribe como:

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

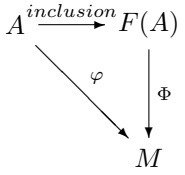
Por la proposición, es equivalente decir que cada elemento m de M puede escribirse únicamente como una suma de elementos $m = n_1 + n_2 + \cdots + n_k$ con $n_i \in N_i$.

Definición 14.

Se dice que un R-módulo F está libre en el subconjunto A de F si para cada elemento x de F distinto de cero, existen elementos únicos distintos de cero $r_1, r_2, \ldots, r_n$ de R y únicos $a_1, a_2, \ldots, a_n$ en A tal que $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$ para algunos $n \in \mathbb{Z}^+$. En esta situación, diremos que A es una base o conjunto de generadores libres para F. Si R es un anillo conmutativo, la cardinalidad de A se denomina como el rango de F.

Teorema 2.

Para cualquier conjunto A hay un R-módulo libre $F(A)$ en el conjunto A y $F(A)$ cumple la siguiente propiedad universal: si M es cualquier R-módulo y $\varphi : A \longrightarrow M$ es cualquier mapa de conjuntos, entonces hay un homomorfismo de módulo R único $\Phi : F(A) \longrightarrow M$ tal que $\Phi(a) = \varphi(a)$, para todo $a \in A$, es decir, el siguiente diagrama conmuta



Cuando A es el conjunto finito $a_1, a_2, \ldots, a_n$,

$$F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R_n.$$

Demostración.

Si $A \neq \emptyset$ entonces $F(A) = 0$.

Sea $F(A) = \{f : A \to R / f(a) = 0$ para todo a menos un número finito $\}$.

En $F(A)$ se define las siguientes operaciones:

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

Sea $r \in R$, $f \in F(A)$

$(rf)(a) = rf(a)$.

Afirmación: $F(a)$ es un R-módulo. (ejercicio al lector).

Para $a \in A$ considere $f : A \to R$ definida por: $f_a(x) = \begin{cases} 1 & \text{si } x = a, \\ 0 & \text{si } x \neq a. \end{cases}$

Entonces podemos inyectar A en $F(A)$ $A \hookrightarrow F(A)$ de la siguiente manera $a \to f_a$.

Si $f \in F(A)$, entonces se puede escribir

$$\begin{aligned} f &= r_1 f_{a_1} + r_2 f_{a_2} + \ldots + r_n f_{a_n} \\ &= r_1 a_1 + r_2 a_2 + \ldots + r_n a_n. \end{aligned}$$

Identificando f_{a_i} con a_i y donde $r_i = f(a_i)$.

Existencia de Φ

$$\begin{aligned} \Phi : & F(A) \to M \\ & \sum_{i=1}^{n} r_i a_i \to \sum_{i=1}^{n} \phi(a_i). \end{aligned}$$

Afirmación: Φ es un homomorfismo de R-módulos. (ejercicio al lector).

Unicidad de Φ

A es una base de $F(A)$ por lo que ϕ es única. □

Corolario 1.

1. *Si F_1 y F_2 son módulos libres en el mismo conjunto A, existe un isomorfismo único entre F_1 y F_2, que es el mapa de identidad en A.*
2. *Si F es cualquier R-módulo libre de base A, entonces $F \cong F(A)$. En particular, F posee la misma propiedad universal con respecto a A que $F(A)$ tiene en el teorema visto anteriormente.*

CAPÍTULO 2

Módulos sobre Dominios de Ideales Principales

Este capítulo es basado principalmente en [2].

2.1 Teoría básica

Primero definiremos condiciones generales de finitud. Sea R un anillo y M un R-módulo izquierdo.

Definición 15.

1. *El R-módulo izquierdo M se dice que es un R-módulo Noetheriano o que satisface la condición de cadena ascendente en submódulos solo si no hay cadenas de submódulos crecientes infinitas, es decir, siempre que*

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

es una cadena creciente de submódulos de M, entonces hay un número entero positivo m tal que para todos $k \geq m, M_k = M_m$ (por lo que la cadena se vuelve estacionaria en la etapa $m : M_m = M_{m+1} = M_{m+2} = \ldots$).

2. *El anillo R, se dice que es Noetheriano si es Noetheriano como un módulo izquierdo sobre sí mismo, es decir, si no hay cadenas infinitas crecientes de ideales izquierdos en R.*

Se pueden formular nociones de A.C.C. en ideales derechos y en dos lados de un anillo R. Para anillos no conmutativos, estas propiedades necesitan estar relacionadas.

Teorema 3.

Sea R un anillo y M un R-módulo izquierdo. Entonces tendremos las siguientes equivalencias:

1. *M es un R-módulo Noetheriano.*
2. *Cada conjunto no vacío de submódulos de M contiene un elemento máximo bajo inclusión.*
3. *Cada submódulo de M es finitamente generado.*

Demostración.

[1. implica 2.] Asumiremos que M es Noetheriano y la $\sum$ de la colección de submódulos de M no es vacía. Se elige cualquier $M_1 \in \sum$. Si M_1 es el elemento máximo de $\sum$, 2. se mantiene, así se asume que M_1 no es maximal. Luego hay algún $M_2 \in \sum$ tal que $M_1 \subset M_2$. Si M_2 es máximo en $\sum$, 2. se mantiene, entonces podemos suponer que hay un $M_3 \in \sum$ que contiene a M_2 correctamente. Procediendo de esta manera, se ve que si 2. falla, podemos producir mediante el Axioma de Elección una cadena infinita de elementos estrictamente crecientes de $\sum$, donde se contradice 1.

[2. implica 3.] Asumir que 2. se cumple y N es un submódulo de M. Sea $\sum$ la colección de todos los submódulos finitamente generados de N. Como $\{0\} \in \sum$, esta colección no es vacía. Por 2. tenemos que $\sum$ contiene un elemento máximo N'. Si $N' \neq N$, tenemos $x \in N - N'$. Ya que $N' \in \sum$, el submódulo N' se genera finitamente por suposición, por lo tanto, también se genera finitamente el submódulo generado por N' y x es finitamente generado. Esto contradice la maximalidad de N', por lo que $N = N'$ generado finitamente.

[3. implica 1.] Se asume que se cumple 3. y $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$ es una cadena de submódulos de M. Sea

$$N = \bigcup_{i=1}^{\infty} M_i$$

y notar que N es un submódulo. Por 3. N es finitamente generado por $a_1, a_2, \ldots, a_n$. Ya que $a_i \in N$ para todo i, cada a_i se encuentra en uno de los submódulos de la cadena, es decir M_{j_i}. Sea $m = max\{j_1, j_2, \ldots, j_n\}$. Entonces $a_i \in M_m$ para todo i, de modo que el módulo que generan se encuentra contenido en M_m, es decir, $N \subset M_m$. Esto implica que $M_m = N = M_k$ para todo $k \geq m$, de esta forma queda 1 probado. $\square$

Corolario 2.

Si R es un P.I.D. entonces cada conjunto de ideales no vacíos de R tiene un elemento máximo y R es un anillo Noetheriano.

Demostración.

El P.I.D. R satisface la condición 3. en el teorema con $M = R$. Hay que recordar que incluso si M es un R-módulo finitamente generado, los submódulos de M no necesitan ser generados finitamente, por lo que la condición de que M sea un R-módulo Noetheriano es en general más fuerte que la condición de que M sea un R-módulo finitamente generado. □

¿Cómo saber si los elementos son linealmente dependientes?

Proposición 8.

Sea R un dominio integral y M un R-módulo libre de rango $n < \infty$. Entonces cualquier elemento $n+1$ de M es R-linealmente dependiente, es decir, para cualquier $y_1, y_2, \ldots, y_{n+1} \in M$ hay elementos $r_1, r_2, \ldots, y_{n+1} \in R$, donde no todos son cero, de modo que

$$r_1 y_1 + r_2 y_2 + \ldots + r_{n+1} y_{n+1} = 0.$$

Demostración.

La forma más rápida de demostrar esto, es colocar a R en el cuociente del cuerpo F (ya que R es un dominio integral) y observamos que desde $M \cong R \oplus R \oplus \cdots \oplus R$ (n veces) obtendremos $M \subseteq F \oplus \cdots \oplus F$. Este último es un espacio vectorial n-dimensional sobre F, por lo que cualquier elemento $n+1$ de M es F-linealmente dependiente. Al borrar los denominadores de los escalares (multiplicando por el producto de todos los denominadores, por ejemplo), obtenemos una relación de dependencia R-lineal entre los elementos de $n+1$ de M.

Alternativamente diremos que $e_1, \ldots, e_n$ es una base del R-módulo libre M y $y_1, \ldots, y_{n+1}$ son cualesquiera $n+1$ elementos de M. Para $1 \leq i \leq n+1$ escribimos $y_i = a_{1i}e_i + a_{2i}e_2 + \ldots + a_{ni}e_i$ en terminos de la base $e_1, e_2, \ldots, e_n$. Sea A la matriz $(n+1)\times(n+1)$ cuya entrada es a_{ij} donde $1 \leq i \leq n, 1 \leq j \leq n+1$ y cuya última fila es cero, entonces ciertamente $detA = 0$. Cualquier relación de dependencia en las columnas de A da una relación de dependencia en los y_i's, completando la demostración. □

Definición 16.

Si R es cualquier dominio integral y M es cualquier R-módulo,

$$Tor(M) = \{x \in M | rx = 0 \text{ para algunos } r \text{ distintos de cero y } r \in R\}$$

es un submódulo de M, llamado submódulo de torsión de M. Si $Tor(M) = 0$, se dice que el módulo está libre de torsión.

Definición 17.

Para cualquier submódulo N de M, el anulador de N es el ideal de R, definido por

$$Ann(N) = \{r \in R | rn = 0, \text{ para todo } n \in N\}.$$

Definición 18.

Para cualquier dominio integral R, el rango de un R-módulo M es el número máximo de elementos R-linealmente independientes de M.

Teorema 4.

Sea R un dominio de ideales principales, donde M es un R-módulo libre con un rango finito n y N un submódulo de M. Luego:

1. *N es libre con rango m, $m \leq n$.*
2. *Existe una base $y_1, y_2, \ldots, y_n$ de M de modo que $a_1y_1, a_2y_2, \ldots, a_my_m$ es una base de N, donde $a_1, a_2, \ldots, a_m$ son elementos distintos de cero de R con las relaciones de divisibilidad siguiente:*

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

Demostración.

El teorema se cumple para $N = \{0\}$, así que supondremos que $N \neq \{0\}$. Para cada homomorfismo del R-módulo $\varphi : M \to R$, la imagen de $\varphi(N)$ de N

es un submódulo de R, es decir, un ideal en R. Ya que R es un P.I.D. este ideal debe ser principal, digamos $\varphi(N) = (a_\varphi)$, para algunos $a_\varphi \in R$. Luego

$$\sum = \{(a_\varphi) \mid \varphi \in Hom_R(M, R)\}$$

es la colección de los ideales principales en R obtenidos de esta manera de los homomorfismos del R-módulo de M en R. La colección $\sum$ ciertamente no es vacía ya que tomar φ como el homomorfismo trivial muestra que $(0) \in \sum$.
Según el corolario anterior, $\sum$ tiene al menos un elemento máximo, es decir, hay al menos un homomorfismo v de M a R, de modo que el ideal principal $v(N) = (a_v)$ no está contenido adecuadamente en ningún otro elemento de $\sum$. Sea $a_1 = a_v$ el elemento máximo y $y \in N$ un mapeo de elementos para el generador a_1 bajo el homomorfismo $v : v(y) = a_1$.
Ahora mostramos que el elemento a_1 no es cero. Sea $x_1, x_2, \ldots, x_n$ cualquier base del módulo libre M y donde $\pi_i \in Hom_r(M, R)$ que es el homomorfismo de proyección natural en la cordenada i-ésima con respecto a esta base. Como $N \neq \{0\}$, existe un i tal que $\pi_i(N) \neq 0$, que en particular muestra que $\sum$ contiene mas que solo el ideal trivial (0). Como (a_1) es un elemento máximo de $\sum$, se deduce que $a_1 \neq 0$.
A continuación mostramos que el elemento a_1 divide a $\varphi(y)$ para cada $\varphi \in Hom_R(M, R)$. Para esto diremos que d es un generador del ideal principal generado por a_1 y $\varphi(y)$. Luego d es un divisor de a_1 y $\varphi(y)$ en R y $d = r_1a_1 + r_2\varphi(y)$ para algunos $r_1, r_2 \in R$. Considerar el homomorfismo $\psi = r_1v + r_2\varphi$ desde M a R. Luego $\psi(y) = (r_1v + r_2\varphi)(y) = r_1a_1 + r_2\varphi(y) = d$ así entonces $d \in \psi(N)$, por lo tanto también $(d) \subset \psi(N)$. Pero d es un divisor de a_1, entonces también tenemos $(a_1) \subset (d)$. Luego $(a_1) \subset (d) \subset \psi(N)$ y por la maximalidad de (a_1) obtenemos la siguiente igualdad: $(a_1) = (d) = \psi(N)$. En particular $(a_1) = (d)$ muestra que $a_1 \mid \varphi(y)$ ya que d divide a $\varphi(y)$.

Si aplicamos esto a la proyección del homomorfismo π_i veremos que a_1 divide a $\pi_i(y)$ para todo i. Escribimos $\pi_i(y) = a_1b_i$ para algunos $b_i \in R, 1 \leq i \leq n$ y definimos

$$y_1 = \sum_{i=1}^{n} b_i x_i.$$

Notar que $a_1y_1 = y$. Ya que $a_1 = v(y) = v(a_1y_1) = a_1v(y_1)$ y a_1 es un elemento distinto de cero del dominio integral R, vemos que

$$v(y_1) = 1.$$

Ahora verificamos que el elemento y_1 puede tomarse como un elemento en una base para M y que a_1y_1 puede tomarse como un elemento en una base para N,

ahora tenemos:
Afirmación

(a) $M = Ry_1 \oplus Nuc\ v$, y

(b) $N = Ra_1y_1 \oplus (N \cap Nuc\ v)$.

1. Ahora probaremos la parte (1) del teorema por inducción del rango m de N. Si $m = 0$, entonces N es un módulo de torsión, por lo tanto $N = 0$ ya que un módulo libre es libre de torsión, entonces (1) se mantiene trivial. Supongamos entonces que $m > 0$. Como la suma anterior en (b) es directa se puede ver que $N \cap Nuc\ v$ tiene rango $m - 1$. Por inducción $N \cap Nuc\ v$ es un R-módulo libre de rango $m - 1$. Nuevamente por la suma directa en (b) podemos ver que adjuntando a_1y_1 a cualquier base de $N \cap Nuc\ v$ nos da nuevamente una base de N, por lo que N también es libre y de rango m, así queda demostrado (1).

2. Finalmente probaremos (2) por inducción en n el rango de M. Aplicando (1) al submódulo $Nuc\ v$ veremos que este submódulo es libre y por la suma en (a) es directo y libre con rango $n-1$. Por el supuesto de inducción aplicado al módulo $Nuc\ v$ (que cumple el rol de M) y su submódulo $Nuc\ v \cap N$ (que cumple el rol de N), vemos que hay una base $y_2, y_3, \ldots, y_n$ de $Nuc\ v$ tal que $a_2y_2, a_3y_3, \ldots, a_my_m$ es una base de $N \cap Nuc\ v$ para algunos elementos $a_2, a_3, \ldots, a_m$ de R con $a_2 \mid a_3 \mid \cdots \mid a_m$. Como la suma (a) y (b) son directas, $y_1, y_2, \ldots, y_n$ es una base de M y $a_1y_1, a_2y_2, \ldots, a_my_m$ es una base de N. Para completar la inducción queda por demostrar que a_1 divide a a_2. Se define un homomorfismo φ desde M hasta R definiendo $\varphi(y_1) = \varphi(y_2) = 1$ y $\varphi(y_i) = 0$, para todo $i > 2$, sobre la base de M. Entonces para este homomorfismo φ tenemos $a_1 = \varphi(a_1y_1)$, entonces $a_1 \in \varphi(N)$, por lo tanto también $(a_1) \subset \varphi(N)$. Por la maximalidad de (a_1) en $\sum$ resulta que $(a_1) = \varphi(N)$. Ya que $a_2 = \varphi(a_2y_2) \in \varphi(N)$, entonces tenemos que $a_2 \in (a_1)$, es decir, $a_1 \mid a_2$. Con esto se completa la demostración del teorema.

Demostración afirmación

(a) Tomamos un elemento arbitrario x en M y lo escribimos como

$$x = v(x)y_1 + (x - v(x)y_1).$$

Ya que:

$$\begin{aligned} v(x - v(x)y_1) &= v(x) - v(x)v(y_1) \\ &= v(x) - v(x),1 \\ &= 0 \end{aligned}$$

vemos que $x - v(x)y_1$ es un elemento en el núcleo de v. Esto muestra que x puede ser escrito como la suma de un elemento en Ry_1 y un elemento en el núcleo de v, entonces $M = Ry_1 + Nuc\ v$. Luego $0 = v(ry_1) = rv(y_1) = r$ y esto muestra que el elemento es 0.

Para (b) observamos que $v(x')$ es divisible por a_1 para algún $x' \in N$ por la definición de a_1 es un generador para $v(N)$. Si nosotros escribimos $v(x') = ba_1$ donde $b \in R$, entonces la descomposición que usamos en (a) es $x' = v(x')y_1 + (x' - v(x')y_1) = ba_1y_1 + (x' - ba_1y_1)$ donde el segundo sumando se encuentra en el núcleo de v y es un elemento de N. Esto muestra que $N = Ra_1y_1 + (N \cap Nuc\ v)$.

(b) El hecho de que la suma en (b) sea directa es un caso especial de la suma directa en (a).

□

Recordemos que el R-módulo izquierdo C es un R-módulo cíclico (para cualquier anillo R no necesariamente conmutativo ni con 1) si hay un elemento $x \in C$ tal que $C = Rx$. Podemos definir un homomorfismo de un R-módulo

$$\pi : R \to C$$

por $\pi(r) = rx$, será sobreyectivo por el supuesto $C = Rx$. El primer teorema de isomorfismo da un isomorfismo del R-módulo

$$R/Nuc\ \pi \cong C.$$

Si R es un P.I.D., $Nuc\ \pi$ es un ideal principal, (a), entonces vemos que los R-módulos cíclicos C son de la forma $R/(a)$ donde $(a) = Ann(C)$. Los módulos cíclicos son los módulos más simples, ya que requieren solo un generador. La parte de existencia del Teorema Fundamental establece que cualquier módulo finitamente generado sobre un P.I.D. es isomorfo a la suma directa de muchos módulos cíclicos finitos.

Teorema 5.

Teorema Fundamental, Existencia: Forma del Factor Invariante

Sea R un P.I.D. y M un R-módulo finitamente generado.

1. *Entonces M es isomorfo a la suma de muchos módulos cíclicos finitos, mas precisamente,*

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

para algún entero $r \geq 0$ y elementos no nulos $a_1, a_2, \ldots, a_m$ de R que no son unidades en R y satisfacen la relación de divisibilidad

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

2. *M es libre de torsión, si y solo si M es libre.*

3. *En la descomposición en (1),*

$$Tor(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

En particular M es un módulo de torsión si y solo si $r = 0$ y en este caso el anulador de M es el ideal (a_m).

Demostración.

El módulo M puede ser generado por un conjunto de elementos finitos. Por suposición diremos que $x_1, x_2, \ldots, x_n$ es un conjunto generador de M de cardinalidad mínima. Sea R^n un R-módulo libre de rango n con base $b_1, b_2, \ldots, b_n$ y define al homomorfismo $\pi : R^n \to M$ definiendo $\pi(b_i) = x_i$ para todo i, que es automaticamente sobreyectivo ya que $x_1, \ldots, x_n$ genera a M. Por el Primer Teorema de Isomorfismo para módulos tenemos $R^n/Nuc\ \pi \cong M$. Ahora, por teorema 4 aplicado a R^n y el submódulo $Nuc\ \pi$ podemos elegir otra base que será $y_1, y_2, \ldots, y_n$ de R para que $a_1y_1, a_2y_2, \ldots, a_my_m$ sea una base de $Nuc\ \pi$ y para algunos elementos $a_1, a_2, \ldots, a_m$ de R con $a_1 \mid a_2 \mid \cdots \mid a_m$. Esto implica

$$M \cong R^n/Nuc\ \pi = (Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n)/((Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m).$$

Para identificar el cociente en el lado derecho, utilizamos la sobreyectividad natural del homomorfismo del R-módulo

$$Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n \to R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

El mapa desde $(\alpha_1 y_1, \ldots, \alpha_n y_n)$ a $(\alpha mod(a_1), \ldots, \alpha_m mod(a_m), \alpha_{m+1}, \ldots, \alpha_n)$. El núcleo de este mapa es claramente el conjunto de elementos donde a_i divide a $\alpha_i, i = 1, 2, \ldots, m$, es decir, $Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m$, de ahí obtenemos

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

Si a es unidad en R, entonces $R/(a) = 0$, en esta suma directa podemos eliminar cualquiera de las a_i iniciales que sean unidades. Esto da la descomposición en (1)(con $r = n - m$).

Como $R/(a)$ es un R-módulo de torsión para cualquier elemento a distinto de cero en R, (1) inmediatamente implica que M es un módulo libre de torsión si y solo si $M \cong R^r$, que es (2). La parte (3) es inmediata a partir de las definiciones del anulador de $R/(a)$ es evidente que (a) es un ideal.

Prontamente se demostrará la unicidad en el teorema 5, es decir, si tenemos

$$M \cong R^{r'} \oplus R/(b_1) \oplus R/(b_2) \oplus \cdots \oplus R/b_{m'}$$

para algunos $r' \geq 0$ y elementos $b_1, b_2, \ldots, b_{m'}$ distintos de cero en R y que no son unidades con

$$b_1 \mid b_2 \mid \cdots \mid b_{m'},$$

entonces $r = r'$, $m = m'$ y $(a_i) = (b_i)$ para todo i. Es precisamente la condición de divisibilidad $a_1 \mid a_2 \mid \cdots \mid a_m$ que le da esta singularidad. □

Definición 19.

El número entero r es llamado rango libre o el número de Betti de M y los elementos $a_1, a_2, \ldots, a_m \in R$ se llaman factores invariantes de M.

Observación 6.

Debemos tener en cuenta que hasta que se demuestre que los factores invariantes de M son únicos, deberíamos referirnos adecuadamente al conjunto a de factores invariantes para M (y de manera similar para el rango libre), con lo que nos referimos a cualquier elemento que dé una descomposición para M como en (1) del teorema anterior.

Teorema 6.

Teorema Fundamental, Existencia: Forma de Divisor Elemental

Sea R un P.I.D. y M un R-módulo finitamente generado. Entonces M es la suma directa de un número finito de módulos cíclicos cuyos anuladores son 0 o

son generados por potencias de primos en R, es decir,

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t}).$$

Donde r es un numero entero positivo mayor o igual que 0 y $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ *son potencias positivas de primos en R, no necesariamente distintas.*

Definición 20.

Sea R un P.I.D. y M un R-módulo finitamente generado como en el teorema anterior. Las potencias principales $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ *(incluyendo la multiplicación por unidades en R) son llamadas "Divisores Elementales de M".*

Teorema 7.

Teorema de Descomposición Primaria

Sea R un P.I.D. y M es una torsión distinta de cero de un R-módulo (no necesariamente finitamente generado) con anulador "a" distinto de cero. Supongamos la fatorización de a en distintas potencias primarias de R es:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

y $N_i = \{x \in M \mid p_i^{\alpha_i} x = 0\}, 1 \leq i \leq n$. *Entonces* N_i *es un submódulo de M con anulador* $p_i^{\alpha_i}$ *y es el submódulo de M de todos los elementos anulados por alguna potencia de* p_i. *Luego tenemos:*

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_n.$$

Si M es finitamente generado entonces cada N_i *es la suma directa de muchos módulos cíclicos cuyos anuladores son divisores de* $p_i^{\alpha_i}$.

Demostración.

Ya hemos demostrado estos resultados en el caso en que M es finitamente generado sobre R. En el caso general, está claro que N_i es un submódulo de M con un anulador que divide a $p_i^{\alpha_i}$. Como R es un P.I.D. los ideales $(p_i^{\alpha_i})$ y $(p_j^{\alpha_j})$ son comaximales para $i \neq j$, por lo que la descomposición de la suma directa de M se puede prever fácilmente modificando el argumento en la demostración del Teorema Chino del Resto para aplicarlo a los módulos. Utilizando esta descomposición de suma directa, es fácil ver que el anulador de N_i es precisamente $p_i^{\alpha_i}$. □

Definición 21.

El submódulo N_i en el teorema anterior es llamado el p_i-principal componente de M.

Lema 1.

Sea R un P.I.D. y p un primo en R. Sea F un cuerpo denotado como $R/(p)$.

1. *Sea $M = R^r$. Entonces $M/pM \cong F^r$.*
2. *Sea $M = R/(a)$ donde a es un elemento distinto de cero en R. Entonces:*

$$M/pM = \begin{cases} F & \text{si } p \text{ divide a en } R, \\ 0 & \text{si } p \text{ no divide a en } R. \end{cases}$$

3. *Sea $M = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k)$ donde cada a_i es divisible por p. Entonces $M/pM \cong F^k$.*

Demostración.

Este es un mapa natural de R^r a $(R/(p))^r$ definido mediante el mapeo de $(\alpha_1, \ldots, \alpha_r)$ a (α_1 mód $(p), \ldots, \alpha_r$ mód (p)). Esto es claramente un homomorfismo de un R-módulo sobreyectivo con núcleo que son las r-tuplas cuyas coordenadas son divisibles por p, es decir, pR^r, entonces $R^r/pR^r \cong (R/(p))^r$, que es 1. Luego 2 se desprende de los teoremas de isomorfismos que hemos visto. Debemos primero notar que $p(R/(a))$ es la imagen del ideal (p) en el cociente $R/(a)$, por lo tanto es $(p) + (a)/(a)$. El ideal $(p) + (a)$ es generado por un máximo común divisor de p y a, por lo tanto es (p) si p divide a a y en caso contrario $R = (1)$. Por lo tanto $pM = (p)/(a)$ si p divide a a y en caso contrario $R/(a) = M$. Si p divide a a, entonces $M/pM = (R(a))/((p)/(a)) \cong R/(p)$, y si p no divide a a entonces $M/pM = M/M = 0$, lo que prueba 2. El tercer punto del Lema se deduce del punto demostrado anteriormente como en la demostración de la parte 1 del teorema 5. □

Teorema 8.

Teorema Fundamental de Unicidad

Sea R un P.I.D.

1. *Dos R-módulos M_1 y M_2 generados finitamente son isomorfos si y solo si tienen el mismo rango libre y la misma lista de factores invariantes.*

2. *Dos R-módulos M_1 y M_2 generados finitamente son isomorfos si y solo si tienen el mismo rango libre y la misma lista de divisores elementales.*

Demostración. 2. Supongamos que $M_1 \cong M_2$. Por lo tanto $Tor(M_1) \cong Tor(M_2)$. Entonces

$$R_1^{r_1} \cong M_1/Tor(M_1) \cong M_2/Tor(M_2) \cong R_2^{r_2}$$

Usando parte 1 del lema anterior $F^{r_1} \cong F^{r_2}$ donde $F = R/pR$ y p es cualquier primo de R. Luego $r_1 = r_2$.

Afirmación: Si dos módulos M_1 y M_2 son anulados por la misma potencia p^e de p son isomorfos, entonces tienen los mismos divisores elementales. (Ejercicio al lector).

Inducción: Si $e = 0$ entonces $M_1 = \{0\}$ y $M_2 = \{0\}$ $e > 0$. Supongamos que M_1 tiene la siguiente lista de divisores elementales:

$$\underbrace{p, \ldots, p}_{m-veces}, p^{\alpha_1}, \ldots, p^{\alpha_s}, \text{donde } 2 \leq \alpha_1 \leq \ldots \leq \alpha_s.$$

M_1 es la suma directa de módulos cíclicos con generadores $x_1, x_2, \ldots, x_m, x_{m+1}, \ldots, x_{m+s}$ cuyos anuladores son$(p), (p), \ldots, (p), (p_{\alpha_1}), \ldots, (p_{\alpha_s})$, respectivamente.

El submódulo pM_1 tiene los siguientes divisores elementales:

$$p^{\alpha_1 - 1}, \ldots, p^{\alpha_s - 1}.$$

Similarmente M_2 tiene la siguiente lista de divisores elementales:

$$\underbrace{p, \ldots, p}_{n-veces}, p^{\beta_1}, \ldots, p^{\beta_t}, \text{donde } 2 \leq \beta_1 \leq \ldots \leq \beta_t.$$

El submódulo pM_2 tiene los siguientes divisores elementales:

$$p^{\beta_1 - 1}, \ldots, p^{\beta_t - 1}.$$

Supongamos que $M_1 \cong M_2$. Por lo tanto $pM_1 \cong pM_2$.

Aplicamos hipótesis de inducción por lo que pM_1 y pM_2 tienen los mismos divisores elementale. Así $s = t$ y

$$\alpha_i - 1 = \beta_i - 1, \text{ para } i = 1, \ldots, s.$$

Entonces

$$\alpha_i = \beta_i, \text{ para } i = 1, \ldots, s.$$

Finalmente desde $M_1/pM_1 \cong M_2/pM_2$ tenemos que $F^{m+s} \cong F^{n+t}$. Así $m+s = n+s$ entonces $m = n$.

1. Usando la lista de divisores elementales desde (2) construimos factores invariantes. Las otras impedancias son directas.
$\Leftarrow$) M_1 y M_2 tienen la misma lista de factores invariantes y el mismo rango entonces son isomorfos o la misma lista de divisores elementales y el mismo rango son isomorfos claramente. □

Corolario 3.

Sea R un P.I.D. y M un R-módulo finitamente generado.

1. *Los divisores elementales de M son los factores de potencias de primos de los factores invariantes de M.*
2. *El factor invariante más grande de M es el producto de la mayor de las potencias primas distinta entre los divisores elementales de M, el siguiente factor invariante más grande es el producto de la mayor de las potencias primas distintas entre los divisores elementales restantes de M, y así sucesivamente.*

Demostración.

El procedimiento en 1. da a conjuntos de divisores elementales y dado que los divisores elementales para M son únicos por el teorema, se deduce que el procedimiento en 1. da el conjunto de divisores elementales. Análogamente se procede de la misma forma para 2. □

2.2 Forma Canónica Racional

Existen diversos métodos para hallar reducciones de matrices cuando no es posible. Cuando el polinomio mínimo no puede factorizarse como producto de factores lineales podemos buscar la forma canónica racional.

Definición 22.

1. *Un elemento λ de F es llamado valor propio de la transformación lineal T si existe un vector v de V que es distinto de cero tal que $T(v) = \lambda v$. En esta situación v es llamado vector propio de T con el correspondiente valor propio λ.*

2. *Si A es una matriz de $n \times n$ con coeficientes en F, un elemento λ es llamado valor propio de A con su correspondiente vector propio v si v es un vector columna $n \times 1$ distinto de cero tal que $Av = \lambda v$.*

3. *Si λ es un valor propio de la transformación lineal T, el conjunto $\{v \in V \mid T(v) = \lambda V\}$ es llamado espacio propio de T correspondiente al valor propio λ. Similarmente, si λ es un valor propio de la matriz A $n \times n$, el conjunto de matrices $n \times 1$ v con $Av = \lambda v$ es llamado espacio propio de A correspondiente al valor propio λ.*

Definición 23.

El determinante de una transformación lineal de V a V es el determinante de cualquier matriz que represente la transformación lineal, debemos tener en cuenta que esto no depende de la elección de la base utilizada.

Proposición 9.

Los siguientes puntos son equivalentes:

1. *λ es un valor propio de T.*

2. *$\lambda I - T$ es una transformación lineal singular de V.*

3. *$det(\lambda I - T) = 0$.*

Demostración.

Dado que λ es un valor propio de T con el vector propio correspondiente v, si y solo si v es un vector distinto de cero en el núcleo de $\lambda I - T$, se deduce que 1 y 2 son equivalentes. Luego 2 y 3 son equivalentes por resultados en determinantes. □

Definición 24.

Sea x una indeterminada sobre F. El polinomio $det(xI - T)$ es llamado "polinomio característico" de T y será denotado como $c_T(x)$. Si A es una matriz $n \times n$ con coeficientes en F, $det(xI - A)$ es llamado "polinomio característico" de A y se denota como $c_A(x)$.

Definición 25.

El único polinomio mónico que genera el ideal $Ann(V)$ en $F[x]$ es llamado "polinomio mínimo" de T y es denotado como $m_T(x)$. El único polinomio mónico de menor grado que cuando se evalua en la matriz A da la matriz cero o matriz nula se llama "polinomio mínimo" de A.

Proposición 10.

El polinomio mínimo $m_T(x)$ es el factor invariante más grande de V. Todo factor invariante de V divide a $m_T(x)$.

Los elementos $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{k-1}$ forman una base para el espacio vectorial $F[x]/(a(x))$ donde $a(x) = x^k + b_{k-1}X^{k-1} + \ldots + b_1x + b_0$ es cualquier polinomio mónico en F [x] $\overline{x} = x$ mód $(a(x))$. Con respecto a esta base, la transformación lineal de la multiplicación por x actúa de la siguiente manera:

$$\begin{aligned} 1 &\mapsto \overline{x} \\ \overline{x} &\mapsto \overline{x}^2 \\ &\vdots \\ \overline{x}^{k-2} &\mapsto \overline{x}^{k-1} \\ \overline{x}^{k-1} &\mapsto \overline{x}^k = -b_{k-1}x^{k-1} - \ldots - b_1x - b_0 \end{aligned}$$

Con respecto a esta base, la matriz para la multiplicación por x es por lo tanto

$$\begin{pmatrix} 0 & 0 & \ldots & \ldots & \ldots & -b_0 \\ 1 & 0 & \ldots & \ldots & \ldots & -b_1 \\ 0 & 1 & \ldots & \ldots & \ldots & -b_2 \\ 0 & 0 & \ddots & & & \\ & & & \ddots & & \\ 0 & 0 & \ldots & \ldots & 1 & -b_{k-1} \end{pmatrix}$$

Definición 26.

Sea $a(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1x + b_0$ cualquier polinomio mónico en $F[x]$. La matriz compañera de $a(x)$ es la matriz $k \times k$ con 1's por la subdiagonal inferior, $-b_0, -b_1, \ldots, -b_{k-1}$ hacia abajo la última columna y ceros en otra parte. La matriz compañera de $a(x)$ está denotada por $C_{a(x)}$.

Definición 27.

1. *Se dice que una matriz está en la forma "canónica racional" si es la suma directa de matrices compañeras que forman los polinomios mónicos $a_1(x), \ldots, a_m(x)$ de grado uno al menos, con $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$. Los polinomios $a_i(x)$ se denominan factores invariantes de la matriz. Dicha matriz también se dice que es una matriz diagonal de bloque con bloques de las matrices compañerass para $a_i(x)$.*

2. *Una forma canónica racional para una transformación lineal T es una matriz que representa a T que está en la forma canónica racional.*

Teorema 9.

Forma Canonica Racional para Transformación Lineal

Sea V un espacio vectorial de dimensión finita sobre el cuerpo F y T una transformación lineal de V.

1. *Hay una base para V con respecto a la cual la matriz para T está en forma canónica racional, es decir, es una matriz diagonal en bloque cuyos bloques diagonales son las matrices compañeras para polinomios mónicos $a_1(x), a_2(x), \ldots, a_m(x)$ de grado al menos uno con $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$.*

2. *La forma canónica racional de T es única.*

Demostración. Ver [2] teorema 14, capítulo 12. □

Teorema 10.

Sea S y T dos transformaciones lineales de V. Entonces se dan las siguientes equivalencias:

1. *S y T son transformaciones lineales similares.*

2. *Los F[x]-módulos obtenidos de V por S y T son F[x]-módulos isomorfos.*

3. *S y T tienen la misma forma canónica racional.*

Teorema 11.

Forma Canónica Racional para Matrices

Sea A una matriz $n \times n$ sobre el cuerpo F.

1. *La matriz A es similar a una matriz en su forma canonica racional, es decir hay una matriz $n \times n$ P sobre F tal que $P^{-1}AP$ es una matriz diagonal en bloque cuyos bloques diagonales son las matrices compañeras para polinomios mónicos $a_1(x), a_2(x), \ldots, a_m(x)$ de grado al menos uno con $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$.*

2. *La forma canónica racional es única.*

Demostración. Es consecuencia del diccionario entre matrices y transformaciones lineales. □

Definición 28.

Los factores invariantes de una matriz $n \times n$ sobre el cuerpo F son los factores invariantes de su forma canónica racional.

Teorema 12.

Sea A y B dos matrices $n \times n$ sobre el cuerpo F. Entonces A y B son similares si y solo si A y B tienen la misma forma canónica racional.

Demostración. Es consecuencia del diccionario entre matrices y transformaciones lineales. □

Corolario 4.

Sea A y B dos matrices $n \times n$ sobre un cuerpo F y suponga que es un subcuerpo del cuerpo K.

1. *La forma canónica racional de A es la misma ya sea que se calcule sobre K o sobre F. Los polinomios mínimos y característicos y los factores invariantes de A son los mismos si A se considera como una matriz sobre F o como una matriz sobre K.*

2. *Las matrices A y B son similares sobre K si y solo si son similares sobre F, es decir, existe una matriz $n \times n$ P con entradas de K tal que $B = P^{-1}AP$ si y solo si existe una matriz $n \times n$ Q con entradas de F tal que $B = Q^{-1}AQ$.*

Demostración. Ver [2] corolario 18 capítulo 12. □

Lema 2.

Sea $a(x) \in F[x]$ un polinomio mónico cualquiera.

1. *El polinomio caracteristico de la matriz compañera de $a(x)$ es $a(x)$.*

2. *Si M es la matriz diagonal de bloque*

$$M = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix},$$

dada por la suma directa de las matrices $A_1, A_2, \ldots, A_k$, entonces el polinomio característico de M es el producto de los polinomios característicos de $A_1, A_2, \ldots, A_k$.

Proposición 11.

Sea A una matriz $n \times n$ sobre el cuerpo F.

1. *El polinomio característico de A es el producto de todos los factores invariantes de A.*

2. *(**Teorema de Cayley - Hamilton**). El polinomio mínimo de A divide al polinomio característico de A.*

3. *El polinomio característico de A divide parte de la potencia del polinomio mínimo de A. En particular, estos polinomios tienen las mismas raíces, no multiplicidades.*

Demostración: ver [2] proposición 20, capítulo 12.

Teorema 13.

Forma Normal de Smith

Sea A una matriz $n \times n$ sobre el cuerpo F. Usando las tres operaciones elementales de fila y columna, la matriz $xI - A$ $n \times n$ con entradas $F[x]$ puede salir a la forma diagonal, esta es llamada "Forma Normal de Smith para A".

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & a_1(x) & & & & \\ & & & a_2(x) & & & \\ & & & & \ddots & & \\ & & & & & a_m(x) & \end{pmatrix}$$

Con los elementos mónicos distintos de cero $a_1(x), a_2(x), \ldots, a_m(x)$ de $F[x]$ con grados de al menos uno y que satisfacen $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$. Los elementos $a_1(x), a_2(x), \ldots, a_m(x)$ son los factores invariantes de A.

Demostración: ver [6] teorema 9.58.

2.2.1 Descomposición Algoritmica de Factor Invariante

Sea V un $F[x]$-módulo con base de espacio vectorial $[e_1, e_2, \ldots, e_n]$. Sea T la transformación lineal de V a sí misma definida por x y sea A la matriz $n \times n$ asociada a T y esta elección de base para V, es decir,

$$T(e_j) = xe_j = \sum_{i=1}^{n} a_{ij} e_i \quad \textit{donde} \quad A = (a_{ij})$$

1. Por medio de las tres operaciones elementales para filas y columnas debe diagonalizar la matriz $xI - A$ sobre $F[x]$, manteniendo registro de las operaciones utilizadas:

   a) Intercambie dos filas o columnas.

   b) Sumar un múltiplo (en $F[x]$) de una fila o columna a otra.

   c) Multiplicar una fila o columna por un valor en $F[x]$, es decir, por un elemento distinto a cero en F.

2. Comenzando con los generadores del $F[x]$-módulo $[e_1, e_2, \ldots, e_n]$, para cada operación de fila utilizada en (1), cambie el conjunto de generadores por las siguientes reglas:

   a) Si la i-ésima fila se intercambia con la fila j-ésima, entonces intercambie los generadores i-ésimo y j-ésimo.

   b) Si la fila j-ésima se agrega $p(x)$ veces a la fila i-ésima, entonces sustraiga $p(x)$ veces el generador i-ésimo desde el generador j-ésimo.

c) Si la fila i-ésima es multiplicada por $u \in F$ entonces divida el generador i-ésimo por u.

3. Cuando $xI - A$ se ha diagonalizado a la forma Normal de Smith, los generadores $[e_1, e_2, \ldots, e_n]$ para V estarán en forma de $F[x]$-combinaciones lineales de $e_1, e_2, \ldots, e_n$. Use $xe_j = T(e_j) = \sum_{i=1}^{n} a_{ij}e_i$ para usar estos elementos como F-combinaciones lineales de $e_1, e_2, \ldots, e_n$. Cuando $xI - A$ se ha diagonalizado, los primeros $n-m$ de estas combinaciones lineales son 0 y las combinaciones lineales m restantes son distintas de cero, es decir, los generadores para V están en la forma $[0, \ldots, 0, f_1, \ldots, f_m]$ correspondiente precisamente a los elementos diagonales en la forma Normal de Smith. Los elementos $f_1, \ldots, f_m$ son un conjunto de generadores de $F[x]$-módulos para los factores cíclicos en la descomposición de factores invariantes de V (con anuladores $a_1(x), \ldots, (a_m(x))$ respectivamente):

$$V = F[x]f_1 \oplus F[x]f_2 \oplus \ldots \oplus F[x]f_m$$

$$F[x]f_1 \cong F[x]/(a_i(x)), \quad i = 1, 2, \ldots, m$$

dando la descomposición del factor invariante del $F[x]$-módulo V.

4. La base del espacio vectorial correspondiente para cada factor cíclico de V viene dada por elementos $f_i, Tf_i, T^2f_i, \ldots, T^{dega_i(x)-1}f_i$.

5. Escriba el elemento k-ésimo de la base del espacio vectorial calculado en (4) en términos de la base del espacio vectorial original $[e_1, e_2, \ldots, e_n]$ y use las coordenadas para la columna k-ésima de una matriz $n \times n$ P. Entonces $P^{-1}AP$ está en forma canónica racional. Esta es la matriz para la transformación lineal T con respecto a la base del espacio vectorial en (4).

Ejemplo 5.

A continuación se mostrará un ejemplo donde encontraremos la forma canónica racional de una matriz en particular de las tres siguientes:

$$A = \begin{pmatrix} 1 & -2 & 6 \\ 0 & 5 & -3 \\ 0 & 0 & 1 \end{pmatrix}; \; B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}; \; C = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

Primero debemos calcular el polinomio característico para estas matrices, en este caso hemos tomado tres matrices con el mismo polinomio característico. Tenemos:

$$C_A = C_B = C_C = (x-1)^2 (x-5)$$

Luego, para continuar debemos encontrar el polinomio mínimo para cada una de estas matrices donde tenemos que pueden ser las siguientes dos opciones para cada una:

$$M = (x-1)(x-5) \quad o \quad M = (x-1)^2 (x-5).$$

Para encontrar cual es el polinomio mínimo para cada matriz, debemos evaluar el posible polinomio mínimo en la matriz con la que deseamos trabajar y el término que acompaña multiplicado por la matriz identidad , en este caso trabajaremos con la matriz B, para saber si es el polinomio mínimo, al realizar esta operatoria debemos llegar como resultado final a la matriz nula:

$$M(B) = (B-I)^2 (B-5I) = 0$$

Como podemos apreciar, al resolver eso, nos da como resultado la matriz nula, por lo tanto el polinomio mínimo para la matriz B es

$$M = (x-1)^2 (x-5)$$

coincidentemente es el mismo polinomio para la matriz A, B y C.

Ejemplo 6.

1. *A continuación, para proseguir en nuestra búsqueda de la forma canónica racional para la matriz B, debemos diagonalizar la siguiente matriz:*

$$IX - B = \begin{pmatrix} x-1 & -1 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & x-5 \end{pmatrix}$$

Para diagonalizar y llegar a la forma de Smith con dicha matriz debemos utilizar las operaciones elementales e ir tomando nota clara de ellas ya

que serán utilizadas posteriormente.

$$IX - B = \begin{pmatrix} x-1 & -1 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & x-5 \end{pmatrix} \; F_1 \; - \; F_2 \to F_1$$

$$\begin{pmatrix} x-1 & -x & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & x-5 \end{pmatrix} C_1 + C_2 \to C_1$$

$$\begin{pmatrix} -1 & -x & 0 \\ x-1 & x-1 & 0 \\ 0 & 0 & x-5 \end{pmatrix} F_2 + F_1\,(X-1) \to F_2$$

$$\begin{pmatrix} -1 & -x & 0 \\ 0 & -x^2+2x-1 & 0 \\ 0 & 0 & x-5 \end{pmatrix} C_2 + C_1\,(-x) \to C_2$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -\,x^2+2x-1 & 0 \\ 0 & 0 & x-5 \end{pmatrix} F_1 * (-1)$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -x^2+2x-1 & 0 \\ 0 & 0 & x-5 \end{pmatrix} F_2 + F_3 \to F_2$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -x^2+2x-1 & x-5 \\ 0 & 0 & x-5 \end{pmatrix} C_2 + C_3(x+3) \to C_2$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -16 & x-5 \\ 0 & (x+3)(x-5) & x-5 \end{pmatrix} F_2\left(-\tfrac{1}{16}\right)$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{x-5}{16} \\ 0 & (x+3)(x-5) & x-5 \end{pmatrix} F_3 - (x+3)\,(x-5)F_2 \to F_3$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{x-5}{16} \\ 0 & 0 & \frac{(x-5)}{16}(x+3)(x-5)+x-5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{x-5}{16} \\ 0 & 0 & \frac{(x-5)}{16}(x^2-2x+1) \end{pmatrix} C_3 + C_2\left(\tfrac{x-5}{16}\right) \to C_3$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{(x-5)}{16}(x^2-2x+1) \end{pmatrix} F_3(16)$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x-5)(x^2-2x+1) \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x-5)(x-1)^2 \end{pmatrix}$$

De esta forma logramos determinar el factor invariante de nuestra matriz B.

2. *Ahora diremos que V es un espacio vectorial 3-dimensional sobre Q con base e_1, e_2, e_3 y sea T la transformación lineal correspondiente, es decir:*

$$\begin{aligned} xe_1 &= T(e_1) &&= 1e_1 \\ xe_2 &= T(e_2) &&= 1e_1 + 1e_2 \\ xe_3 &= T(e_3) &&= 5e_3 \end{aligned}$$

Ya teniendo nuestra matriz en la forma de Smith, podemos hacer un recuento de operaciones de filas utilizadas para la diagonalización y escribirlas ordenadamente:

a) $F_2 - F_1 \ \rightarrow F_1$

b) $F_2 + F_1(x-1) \ \rightarrow F_2$

c) $F_1(-1)$

d) $F_2 + F_3 \rightarrow F_2$

e) $F_2\left(-\frac{1}{16}\right)$

f) $F_3 - F_2(x+3)(x-5) \rightarrow F_3$

g) $F_3(16)$

Luego, comenzando con la base de V $[e_1, e_2, e_3]$ y cambiando de acuerdo a las reglas mencionadas anteriormente, obtenemos lo siguiente:

$[e_1, e_2, e_3] \rightarrow [e_1, e_2 + e_1, e_3]$
$\rightarrow [e_1 - (x-1)(e_2 + e_1), e_2 + e_1, e_3]$
$\rightarrow [(x-1)(e_2 + e_1) - e_1, e_2 + e_1, e_3]$
$\rightarrow [(x-1)(e_2 + e_1) - e_1, e_2 + e_1, e_3 \ - \ e_2 \ - \ e1]$
$\rightarrow [(x-1)(e_2 + e_1) - e_1, -16e_2 \ - \ 16e_1, e_3 \ - \ e_2 \ - \ e1]$

$\rightarrow [(x-1)(e_2+e_1)-e_1, -16e_2 - 16e_1 + (x+3)(x-5)(e_3 - e_2 - e1), e_3 - e_2 - e1]$
$\rightarrow [(x-1)(e_2+e_1)-e_1, -16e_2 - 16e_1 + (x+3)(x-5)(e_3 - e_2 - e_1), \frac{e_3 - e_2 - e1}{16}]$

3. *Desarrollando y utilizando las fórmulas de acción de x, vemos que estos últimos elementos son los elementos $[0, 0, \frac{e_3-e_2-e_1}{16}]$ de V correspondiente a los elementos $1, 1, (x-1)^2(x-5)$ en la diagonalización de $xI - B$, respectivamente.*

4. *Los elementos correspondientes a las columnas de la matriz P son los siguientes $f_1 = \frac{e_3-e_2-e_1}{16}$, $xf_1 = T(f_1) = \frac{5e_3}{16} - \frac{e_2}{16} - \frac{e_1}{8}$ y por último $x(xf_1) = T(T(f_1) = \frac{25e_3}{16} - \frac{e_2}{16} - \frac{3e_1}{16}$,*

5. *lo que nos forma la siguiente matriz:*

$$P = \begin{pmatrix} -\frac{1}{16} & -\frac{1}{8} & -\frac{3}{16} \\ -\frac{1}{16} & -\frac{1}{16} & -\frac{1}{16} \\ \frac{1}{16} & \frac{5}{16} & \frac{25}{16} \end{pmatrix}$$

Luego podemos calcular la forma canónica racional de la siguiente forma según el algoritmo:

$$P^{-1}BP = \begin{pmatrix} 0 & 0 & 5 \\ 1 & 0 & -11 \\ 0 & 1 & 7 \end{pmatrix}.$$

2.2.2 Convertir una Matriz $n \times n$ a Forma Canónica Racional

Sea A una matriz $n \times n$ con entradas en el cuerpo F.

1. Por medio de las tres operaciones elementales para filas y columnas debe diagonalizar la matriz $xI - A$ sobre $F[x]$, manteniendo registro de las operaciones utilizadas:

   a) Intercambie dos filas o columnas.

   b) Sumar un múltiplo (en $F[x]$) de una fila o columna a otra.

   c) Multiplicar una fila o columna por un valor en $F[x]$, es decir, por un elemento distinto a cero en F.

Defina $d_1, d_2, \ldots, d_m$ como los grados de los polinomios mónicos no constantes $a_1(x), \ldots, a_m(x)$ que aparecen en la diagonal, respectivamente.

2. Comenzando con la matriz identidad $n \times n$ P', para cada operación de fila utilizada en (1) cambie la matriz P' por las siguientes reglas:

   a) Si $F_i \leftrightarrow F_j$ entonces intercambiamos la i-ésima y j-ésima columna de P'.

   b) Si $F_i + p(x)F_j \to F_i$ entonces debemos sustraer $p(A)$ veces la i-ésima columna de P' de la j-ésima columna de P'.

   c) Si uF_i entonces dividimos los elementos de la i-ésima columna de P' por u.

3. Cuando $xI - A$ se ha diagonalizado a la forma Normal de Smith, las primeras columnas $n-m$ de la matriz P' son 0 y las m columnas restantes de P' son distintas de cero. Para cada $i = 1, 2, \ldots, m$ multiplique la i-ésima columna distinta de cero de P' sucesivamente por $A^0 = 1, A^1, A^2, \ldots, A^{d_i - 1}$, donde d_i es el número entero en (1) anterior, y use los vectores de columna resultantes como las siguientes d_i columnas de una matriz $n \times n$ P. Luego $P^{-1}AP$ está en forma canónica racional (cuyos bloques diagonales son las matrices compañeras para los polinomios $a_1(x), \ldots, a_m(x)$ en (1)).

Ejemplo 7.

1. Los primeros pasos son los del algortimo de descomposición.

2. $$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{C_2 + C_1 \to C_2}{\longrightarrow} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{C_1 - (A-I)C_2 \to C_1}{\longrightarrow} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
   $$\overset{-C_1}{\longrightarrow} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{C_3 - C_2 \to C_3}{\longrightarrow} \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \overset{-16C_2}{\longrightarrow} \begin{pmatrix} 0 & -16 & -1 \\ 0 & -16 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$
   $$\overset{C_2 - (A+3I)(A-5I)C_3 \to C_2}{\longrightarrow} \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 0 & 0 & 1 \end{pmatrix} \overset{1/16C_3}{\longrightarrow} \begin{pmatrix} 0 & 0 & -1/16 \\ 0 & 0 & -1/16 \\ 0 & 0 & 1/16 \end{pmatrix}$$

3. Luego utilizamos las columnas no nulas de la matriz para encontrar nuestra matriz de cambio P según el algoritmo.

Así

$$A\begin{pmatrix}-1/16\\-1/16\\1/16\end{pmatrix} = \begin{pmatrix}-1/8\\-1/16\\5/16\end{pmatrix}$$
$$A^2\begin{pmatrix}-1/16\\-1/16\\1/16\end{pmatrix} = \begin{pmatrix}-3/16\\-1/16\\25/16\end{pmatrix}$$

Luego $P = \begin{pmatrix}-\frac{1}{16} & -\frac{1}{8} & -\frac{3}{16}\\ -\frac{1}{16} & -\frac{1}{16} & -\frac{1}{16}\\ \frac{1}{16} & \frac{5}{16} & \frac{25}{16}\end{pmatrix}$

2.3 Forma Canónica de Jordan

Sabemos que la diagonalización de matrices dentro del álgebra lineal se puede interpretar como la búsqueda de una base respecto a la cual la matriz asociada a la aplicación lineal al endomorfismo tiene la forma mas sencilla posible (matriz diagonal), pero no siempre es posible encontrar una forma diagonal para algunas matrices, para esto es que utilizamos la forma canónica de Jordan, ya que es la siguiente forma más sencilla de la matriz y en este caso, para todas las matrices tendremos una solución.

Para lograr encontrar esta forma de la matriz necesitaremos una matriz de paso, la cual en esta sección se muestran los algoritmos para lograr conseguir dicha matriz y así lograr encontrar la forma canónica de Jordan.

Considere los elementos

$$(\overline{x}-\lambda)^{k-1}, (\overline{x}-\lambda)^{k-2}, \cdots, \overline{x}-\lambda, 1,$$

en el cociente $F[x]/(x-A)^k$. Los elementos anteriores son una base F para $F[x]/(x-\lambda)^k$. Con respecto a esta base, la transformación lineal de la multiplicación por x actúa de la siguiente manera.
Notar que $x = \lambda + (x-\lambda)$ y que $(\overline{x}-\lambda)^k = 0$ en el cociente:

$$\begin{aligned}(\overline{x}-\lambda)^{k-1} &\mapsto \lambda(\overline{x}-\lambda)^{k-1} - (\overline{x}-\lambda)^k = \lambda(\overline{x}-\lambda)^{k-1}\\ (\overline{x}-\lambda)^{k-2} &\mapsto \lambda(\overline{x}-\lambda)^{k-2} - (\overline{x}-\lambda)^{k-1}\\ &\vdots\\ \overline{x}-\lambda &\mapsto \lambda(\overline{x}-\lambda) - (\overline{x}-\lambda)^2\\ 1 &\mapsto \lambda\cdot 1 - (\overline{x}-\lambda)\end{aligned}$$

Con respecto a esta base, la matriz para la multiplicación por x es por lo tanto

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \ddots & & \\ & & \ddots & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}.$$

Definición 29. *La matriz $k \times k$ con λ a lo largo de la diagonal principal y 1 a lo largo de la primera superdiagonal se llama matriz de Jordan Elemental $k \times k$ con valor propio λ o el Bloque de Jordan de tamaño k con valor propio λ.*

Definición 30.

1. *Se dice que una matriz está en forma canónica de Jordan si es una matriz diagonal de bloque con bloques de Jordan a lo largo de la diagonal.*
2. *Una forma canónica de Jordan para una transformación lineal T es una matriz que representa T que está en forma canónica de Jordan.*

Teorema 14.

Forma Canonica de Jordan para Transformación Lineal

Sea V un espacio vectorial de dimensión finita sobre el cuerpo F y T es una transformación de V. Asumiremos que F contiene a todos los valores propios de T.

1. *Hay una base para V con respecto a la cual la matriz para T está en forma canónica de Jordan, es decir, es una matriz diagonal de bloque cuyos bloques diagonales son los bloques de Jordan para los divisores elementales de V.*
2. *La forma canónica de Jordan para T es única hasta una permutación de los bloques de Jordan a lo largo de la diagonal.*

Demostración. Es consecuencia de la unicidad de los divisores elementales. □

Teorema 15.

Forma Canónica de Jordan para Matrices

Sea A una matriz $n \times n$ sobre el cuerpo F y asumiremos que F contiene todos los valores propios de A.

1. *La matriz A es similar a una matriz en forma canónica de Jordan, es decir, hay una matriz P $n \times n$ invertible sobre F, de modo que $P^{-1}AP$ es una matriz diagonal en bloque cuyos bloques diagonales son los bloques de Jordan para los divisores elementales de A.*

2. *La forma canónica de Jordan para A es única hasta una permutación de los bloques de Jordan a lo largo de la diagonal.*

Corolario 5.

1. *Si una matriz A es similar a una matriz diagonal D, entonces D es la forma canónica de Jordan de A.*

2. *Dos matrices diagonales son similares si y solo si sus entradas diagonales son la misma hasta una permutación.*

Demostración. Ver [2] corolario 24, capítulo 12.- □

Corolario 6.

Si A es una matriz $n \times n$ con entradas desde F y F contiene todos los valores propios de A, entonces A es similar a una matriz diagonal sobre F si y solo si el polinomio mínimo de A no tiene raices repetidas.

Demostración. [2] corolario 25, capítulo 12.- □

2.3.1 Cambiar de una forma canónica a otra

Continuamos asumiendo que el cuerpo F contiene todos los valores propios de T (o de A), por lo que tanto las formas canónicas racionales como las de Jordan existen sobre F.

En resumen, recuerde que los divisores elementales son los principales divisores de potencia de los factores invariantes. Se obtienen de los factores invariantes escribiendo cada factor invariante como un producto de distintos factores lineales a las potencias; el conjunto resultante de potencias de polinomios lineales es el conjunto de divisores elementales.

Ejemplo 8.

Si los factores invariantes de T son:

$$(x+2)(x-7)^3, \quad (x+2)(x+3)(x-7)^3, \quad (x+2)(x+3)^2(x-7)^3$$

luego los divisores elementales son:

$$(x+2), (x-7)^3, \quad (x+2), (x+3), (x-7)^3, \quad (x+2), (x+3)^2, (x-7)^3.$$

El factor invariante más grande es el producto de la mayor de las potencias primarias distintas entre los divisores elementales, el siguiente factor invariante más grande es el producto de la mayor de las potencias primarias distintas entre los divisores elementales restantes, y así sucesivamente. Dada una lista de divisores elementales, podemos encontrar la lista de factores invariantes organizando primero los divisores elementales en n listas separadas, una para cada valor propio. En cada una de estas listas n, organice los polinomios en grado creciente (es decir, no decreciente). Luego organice para que todas las listas n tengan la misma longitud agregando un número apropiado del polinomio constante 1. Ahora forme el i-ésimo factor invariante tomando el producto del i-ésimo polinomio en cada una de estas listas.

Ejemplo 9.

Si los divisores elementales de T son:

$$(x+2)^2, (x-3)^2, (x+2), (x-7)^3, (x+2)^4, (x-3)^2, (x-7)^5, (x+2)^7, (x-3)^4$$

Entonces las listas intermedias son:

$$\begin{array}{llllll} (1) & (x+2), & (x+2)^2, & (x+2)^4, & (x+2)^7 \\ (2) & 1, & (x-3)^2, & (x-3)^2, & (x-3)^4 \\ (3) & 1, & 1, & (x-7)^3, & (x-7)^5 \end{array}$$

Entonces la lista de factores invariantes es:

$$(x+2), \quad (x+2)^2(x-3)^2, \quad (x+2)^4(x-3)^2(x-7)^3, \quad (x+2)^7(x-3)^4(x-7)^5.$$

2.3.2 Algoritmo de Descomposición de Divisor Elemental: Conversión a la Forma Canónica de Jordan

El teorema 13 indica un procedimiento computacional para determinar los factores invariantes de cualquier matriz A. La factorización de estos factores

invariantes produce los divisores elementales de A, por lo tanto, determina la forma canónica de Jordan para A como se indicó anteriormente. El algoritmo de descomposición factorial invariante que sigue el Teorema 13 se basa en una base $e_1, \ldots, e_n$ para V y produce un conjunto $f_1, \ldots, f_m$ de elementos de V que son generadores de $F[x]$-módulos para los factores cíclicos en la descomposición factorial invariante de V (con anuladores $(a_1(x)), \ldots, (am(x))$, respectivamente). Dado que la descomposición de los divisores elementales se obtiene de la descomposición del factor invariante aplicando el Teorema Chino del Resto a los módulos cíclicos $F[x]/(a_i(x))$, esto proporciona un conjunto de generadores de $F[x]$-módulos para los factores cíclicos en la descomposición de los divisores elementales de V. Estos elementos dan lugar a una base explícita de espacio vectorial para V con respecto a la cual la transformación lineal correspondiente a A está en forma canónica de Jordan. En cuanto al algoritmo de descomposición de factor invariante, establecemos el resultado en el contexto general de descomposición de un espacio vectorial y luego describimos el algoritmo para convertir una matriz $n \times n$ A dada a la forma canónica de Jordan. Ejemplo numérico explícito de este algoritmo se da más adelante en el ejemplo 11.

2.3.3 Algoritmos de Descomposición de Divisor Elemental

(1) -(3) Los primeros tres pasos en el algoritmo son los del algoritmo de descomposición de factor invariante que sigue al Teorema 13.

(4) Para cada factor invariante $a(x)$ calculado para A escribe:

$$a(x) = (x - \lambda_1)^{\alpha_1}(x - \lambda_2)^{\alpha_2} \ldots (x - \lambda_s)^{\alpha_s}$$

donde $\lambda_1, \ldots, \lambda_s \in F$ son distintos. Sea $f \in V$ el generador de $F[x]$-módulos para el factor cíclico correspondiente al factor invariante $a(x)$ calculado en (3). Entonces los elementos

$$\frac{a(x)}{(x - \lambda_1)^{\alpha_1}} f, \quad \frac{a(x)}{(x - \lambda_2)^{\alpha_2}} f, \quad \ldots, \quad \frac{a(x)}{(x - \lambda_s)^{\alpha_s}} f.$$

Debemos tener en cuenta que $\dfrac{a(x)}{(x - \lambda_i)^{\alpha_i}} \in F[x]$, es decir, son polinomios. Estos son generadores de $F[x]$-módulos para los factores cíclicos de V correspondientes a los divisores elementales

$$(x - \lambda_1)^{\alpha_1}, \quad (x - \lambda_2)^{\alpha_2}, \quad \ldots, \quad (x - \lambda_s)^{\alpha_s}$$

respectivamente.

(5) Si $g_i = \dfrac{a(x)}{(x-\lambda_i)^{\alpha_i}} f$ es el generador de un $F[x]$-módulo para el factor cíclico de V correspondiente al divisor elemental $(x-\lambda_i)^{\alpha_i}$, entonces la base del espacio vectorial correspondiente para este factor cíclico de V viene dada por los elementos siguientes:

$$(T-\lambda_i)^{\alpha_i-1} g_i, \quad (T-\lambda_i)^{\alpha_i-2} g_i, \quad \ldots, \quad (T-\lambda_i) g_i, \quad g_i.$$

(6) Escriba el elemento k-ésimo de la base del espacio vectorial calculada en (5) en los términos de la base del espacio vectorial original $[e_1, e_2, \ldots, e_n]$ para V y vea las coordenadas para la columna k-ésima de una matriz P $n \times n$. Entonces $P^{-1}AP$ está en Forma Canónica de Jordan (con bloques de Jordan que aparecen en el orden utilizado en (5) para los factores cíclicos de V).

Ejemplo 10.

Para desarrollar este ejemplo utilizaremos las matrices utilizadas en el ejemplo 5 para encontrar la Forma Canónica de Jordan de la matriz B que se muestra a continuación.

$$A = \begin{pmatrix} 1 & -2 & 6 \\ 0 & 5 & -3 \\ 0 & 0 & 1 \end{pmatrix}; \; B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}; \; C = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

Para encontrar la Forma Canónica de Jordan debemos realizar los primeros dos pasos que utilizamos en la sección anterior donde buscabamos encontrar la Forma Canónica Racional, por lo cual omitiremos sus desarrollos.

(1)-(3) Una vez que tenemos nuestra matriz en la Forma Normal de Smith, desarrollando y utilizando las fórmulas de acción de x, vemos que estos últimos elementos son los elementos $[0, 0, \frac{e_3 - e_2 - e_1}{16}]$ de V correspondiente a los elementos $1, 1, x^3 - 7x^2 + 11x - 5$ en la diagonalización de $xI - B$, respectivamente.

(4) Primero factorizamos $x^3 - 7x^2 + 11x - 5 = (x-1)^2(x-5)$ Entonces los elementos

$$\frac{x^3 - 7x^2 + 11x - 5}{(x-1)^2} f = (x-5)f, \frac{x^3 - 7x^2 + 11x - 5}{(x-5)} f = (x-1)^2 f$$

son los generadores

(5) $g_1 = (x-5)f$
$(x-1)g_1 = (x-1)(x-5)f = \dfrac{1}{4} e_1$

$$g_1 = (x-5)f = \frac{3}{16}e_1 + \frac{1}{4}e_2$$
$$g_2 = (x-1)^2 f = e_3$$

(6) $$P = \begin{pmatrix} 1/4 & 3/16 & 0 \\ 0 & 1/4 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Luego la Forma Canónica de Jordan sería la siguiente matriz:

$$P^{-1}BP = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

Notar que esta matriz ya estaba en forma de Jordan por lo que quedo igual al aplicar el algoritmo.

2.3.4 Convertir una matrix $n \times n$ a la Forma Canónica de Jordan

(1)-(2) , estos primeros dos pasos son los del algoritmo que utilizamos para convertir una matriz $n \times n$ a la forma canónica racional siguiendo el Teorema de la Forma Normal de Smith.

(3) Cuando $XI - A$ se ha diagonalizado a la Forma Normal de Smith, las primeras $n - m$ columnas de la matriz P' son cero y las m columnas restantes de P' son distintas de cero, para cada $i = 1, 2, \ldots, m$:

a) Factorice el i-ésimo elemento diagonal no constante que es de grado d_i:

$$a(x) = (x - \lambda_1)^{\alpha_1}(x - \lambda_2)^{\alpha_2} \ldots (x - \lambda_s)^{\alpha_s}$$

donde $\lambda_1, \lambda_2, \ldots, \lambda_s \in F$ son distintos (aquí $a(x) = a_i(x)$ es el i-ésimo elemento diagonal no constante y s depende de i).

b) Multiplique la i-ésima columna de P' sucesivamente por las matrices

d_i:

$$\begin{array}{ccc}
(A-\lambda_1 I)^{\alpha_1-1} & (A-\lambda_2 I)^{\alpha_2} & \dots (A-\lambda_s I)^{\alpha_s} \\
(A-\lambda_1 I)^{\alpha_1-2} & (A-\lambda_2 I)^{\alpha_2} & \dots (A-\lambda_s I)^{\alpha_s} \\
 & \vdots & \\
(A-\lambda_1 I)^{0} & (A-\lambda_2 I)^{\alpha_2} & \dots (A-\lambda_s I)^{\alpha_s} \\
(A-\lambda_1 I)^{\alpha_1} & (A-\lambda_2 I)^{\alpha_2-1} & \dots (A-\lambda_s I)^{\alpha_s} \\
(A-\lambda_1 I)^{\alpha_1} & (A-\lambda_2 I)^{\alpha_2-2} & \dots (A-\lambda_s I)^{\alpha_s} \\
 & \vdots & \\
(A-\lambda_1 I)^{\alpha_1} & (A-\lambda_2 I)^{0} & \dots (A-\lambda_s I)^{\alpha_s} \\
 & \vdots & \\
(A-\lambda_1 I)^{\alpha_1} & (A-\lambda_2 I)^{\alpha_2} & \dots (A-\lambda_s I)^{\alpha_s-1} \\
(A-\lambda_1 I)^{\alpha_1} & (A-\lambda_2 I)^{\alpha_2} & \dots (A-\lambda_s I)^{\alpha_s-2} \\
 & \vdots & \\
(A-\lambda_1 I)^{\alpha_1} & (A-\lambda_2 I)^{\alpha_2} & \dots (A-\lambda_s I)^{0}
\end{array}$$

c) Use los vectores de columna de (b) (en ese respectivo orden) como las siguientes columnas d_i de una matriz $n \times n$ P.

Entonces $P^{-1}AP$ está en forma canónica de Jordan, donde los bloques de Jordan corresponden al orden de los factores en (a).

Ejemplo 11.

(1)-(2) Una vez que tenemos nuestra matriz en la Forma Normal de Smith, desarrollando y utilizando las fórmulas de acción de x, vemos que estos últimos elementos son los elementos $[0, 0, \frac{e_3-e_2-e_1}{16}]$ de V correspondiente a los elementos $1, 1, x^3 - 7x^2 + 11x - 5$ en la diagonalización de $xI - B$, respectivamente.

(3) *a*) Primero factorizamos $x^3 - 7x^2 + 11x - 5 = (x-1)^2(x-5)$

b) Utilizando la matriz $P' = \begin{pmatrix} 0 & 0 & -1/16 \\ 0 & 0 & -1/16 \\ 0 & 0 & 1/16 \end{pmatrix}$

Luego utilizamos las columnas no nulas de la matriz P' para encontrar nuestra matriz de cambio P según el algoritmo.

Así

$$\begin{aligned}(A-I)(A-5I)\begin{pmatrix}-1/16\\-1/16\\1/16\end{pmatrix} &= \begin{pmatrix}1/4\\0\\0\end{pmatrix}\\ (A-5I)\begin{pmatrix}-1/16\\-1/16\\1/16\end{pmatrix} &= \begin{pmatrix}3/16\\1/4\\0\end{pmatrix}\\ (A-I)^2\begin{pmatrix}-1/16\\-1/16\\1/16\end{pmatrix} &= \begin{pmatrix}0\\0\\1\end{pmatrix}\end{aligned}$$

c) De aquí entonces obtenemos la matriz P siguiente:

$$P = \begin{pmatrix}1/4 & 3/16 & 0\\ 0 & 1/4 & 0\\ 0 & 0 & 1\end{pmatrix}$$

Luego la Forma Canónica de Jordan sería la siguiente matriz:

$$P^{-1}BP = \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 5\end{pmatrix}.$$

CAPÍTULO 3

Magma y Álgebra lineal

Magma es un sistema de álgebra computacional diseñado para realizar cálculos en distintas ramas del álgebra, como lo son la teoría de números, geometría algebraica y combinatoria algebraica. En esta sección, nos concentraremos en el uso de algunos comandos de Magma en Álgebra Lineal y Teoría de Números elemental específicamente en Espacios Vectoriales, Teoría de Módulos, Forma Canónica Racional y Forma Canónica de Jordan.

Para la realización de los ejemplos de uso, en este caso utilizaremos una versión disponible online de magma en http: //magma.maths.usyd.edu.au/calc/. También existe una versión de escritorio la cual posee un costo de licencia.

1. Ideas básicas para usar Magma:

   a) Tipear un comando o expresión después del prompt(>).

   b) No olvidar colocar una semicolon (;) al final de la línea.

   c) Luego, presione la tecla enter o submit en el caso de la versión online.

   Por ejemplo, para la multiplicación:

   ```
   > 5*6;
   30
   ```

2. Ayuda en Magma:

   Es posible obtener información acerca de las funciones. Hay que tipear ? seguido por el comando que se desea conocer.

   ```
   > ?load
   5 matches:
    1 0 /system/database
   ```

```
 2 O /system/library
 3 O /system/load
 4 S /language/IO/load
 5 I /language/IO/load/load
To view an entry, type ? followed by the number next to it
```

3. Álgebra Lineal:

   a) Para introducir una matriz debemos definir un nombre luego dos puntos (:) y el signo igual (=) y luego introducir el comando de matriz, posteriormente abrir paréntesis y escribir el cuerpo en el cual se desea trabajar los elementos de dicha matriz, prosigue una coma (,) para señalar el orden de dicha matriz y luego abrir paréntesis cuadrado para escribir los elementos de dicha matriz separados por comas, al terminar con los elementos cerramos los paréntesis correspondientes (generalmente, es necesario escribir la inicial de cada palabra o comando siempre en mayúscula). Por ejemplo, escribiremos la matriz de nombre A con elementos en los racionales y de orden 3:

   ```
   > A:=Matrix(RationalField(),3,[4,0,0,1,0,3,0,0,4]);
   [4 0 0]
   [1 0 3]
   [0 0 4]
   ```

   b) Para realizar operaciones elementales con las filas de una matriz, necesitamos aplicar distintos comandos según la operación que se desee realizar.

      1) Para realizar un intercambio de filas en una matriz A ya definida debemos ingresar el siguiente comando:

      ```
      > SwapRows(A,1,2);
      [1 0 3]
      [4 0 0]
      [0 0 4]
      ```

      Donde A es la matriz ya definida, 1 es la primera fila y 2 es la segunda fila.

      2) En una matriz A ya definida, para multiplicar una fila por un valor "n" escalar debemos introducir el siguiente comando:

      ```
      > MultiplyRow(A,2,1);
      ```

```
[8 0 0]
[1 0 3]
[0 0 4]
```

Donde A es la matriz ya definida, 2 es el escalar por el cual se desea multiplicar la fila y 1 la fila que se multiplica.

3) Para agregar "n" veces la fila i a la fila j en una matriz A ya definida debemos introducir el siguiente comando:

```
> AddRow(A,3,1,2);
[ 4 0 0]
[13 0 3]
[ 0 0 4]
```

Donde A es la matriz ya definida, 3 es el número de veces que queremos agregar la primera fila a la segunda.

c) Para realizar operaciones con dicha matriz y algún escalar u otra matriz, basta tener definida las matrices y operar de igual forma que la operación mostrada anteriormente:

```
> A*5;
[20 0 0]
[ 5 0 15]
[ 0 0 20]

> A*A;
[16 0 0]
[ 4 0 12]
[ 0 0 16]
```

d) Podemos encontrar el polinomio característico de cualquier matriz con el comando CharacteristicPolynomial. Encontraremos el polinomio característico de la matriz A:

```
> CharacteristicPolynomial(A);
```

$\$.1\hat{}3 - 8 * \$.\hat{}2 + 16 * \$.1$

e) Para realizar la factorización de dicho polinomio o cualquier otro necesitamos definirlo, en este caso llamaremos B al polinomio caracteristico de A de la siguiente forma:

> B:=CharacteristicPolynomial(A);

f) Así al escribir B nos arrojará el polinomio caracteristico A:

> B;

$\$.1\hat{}3 - 8 * \$.\hat{}2 + 16 * \$.1$

g) A continuación para realizar la factorización de dicho polinomio debemos ingresar el comando:

> Factorization(B);

[

$< \$.1 - 4, 2 >$,

$< \$.1, 1 >$

]

h) Esto nos dice que tenemos un factor que es $(x-4)^2$ y el otro es x. (el primer término antes de la coma es el factor y el termino luego de la coma nos indica el grado de dicho factor).

4. Forma Canónica Racional y de Jordan.

a) Para poder encontrar la Forma Canónica Racional simplemente debemos ingresar el comando junto con el elemento al cual le deseamos encontrar esta forma:

> RationalForm(A);

[4 0 0]

[0 0 1]

[0 0 4]

b) Similarmente podemos encontrar la Forma Canónica de Jordan:

> JordanForm(A);

[4 0 0]

[0 4 0]

[0 0 0]

Bibliografía

[1] Cannon John J., Playoust Catherine *First Steps in Magma*. 1996.

[2] Dummit, D. y Foote, R., Abstract Algebra Third Edition, University of Vermont, John Wiley and Sons, Inc., 2004.

[3] Hartley B., Hawkes T.O., Rings, Modules and Linear Algebra.

[4] Luis-Puebla E. , Álgebra Homológica, Cohomología de Grupos K-Teoría Algebraica Clásica

[5] Roman Steven , Advanced Linear Algebra, Springer Verlag, 1992.

[6] Rotman Joseph J., Advanced Modern Algebra, 2nd printing (2003).