Notas del curso de Algebra Moderna III

Luis Valero Elizondo

01 de Marzo del 2005

Índice general

Introducción.

Estas son las notas del curso de Algebra Moderna III impartido por Luis Valero Elizondo en la licenciatura de la Facultad de Ciencias Físico-Matemáticas de la Universidad Michoacana de San Nicolás de Hidalgo, Morelia, Michoacán, México. Se pueden bajar por internet de la página del autor, que es

`http://www.fismat.umich.mx/~valero`

Escribí estas notas para que ustedes (mis alumnos) no tengan que perder tiempo en clase escribiendo. Si se ponen a hacer cuentas, notarán que pasan la mayor parte del tiempo de una clase típica escribiendo, y muy poco tiempo pensando o haciendo activamente matemáticas.

Para que ustedes puedan aprovechar al máximo este curso, es indispensable que le dediquen muchas horas de esfuerzo dentro y fuera del salón de clases. Antes de cada clase es muy importante que lean con cuidado el material que vamos a cubrir, que usualmente consistirá de una o dos secciones de estas notas (pues son secciones muy cortas).

También antes de clase deben intentar hacer todos los ejercicios de las secciones que lean. En cualquier caso, incluso si no les sale uno o varios ejercicios, ya habrán pasado un tiempo razonable pensando en ellos, y eso nos será de utilidad cuando cubramos ese material en la clase. Los ejercicios son computacionales (para repasar los conceptos aprendidos) y las *demostraciones*, muy importantes para desarrollar el pensamiento analítico propio de los científicos.

Dentro de la clase vamos a hablar acerca del material que prepararon, y nos vamos a ir con bastante rapidez. Si no prepararon la lección, entonces la clase será tan aburrida como oír gente hablando de una película que no han visto. Si no leyeron las definiciones, no van a saber ni siquiera de lo que estamos hablando; y si leyeron las notas sin haber hecho los ejercicios, no van a poder entender lo que hagamos porque les faltará familiaridad con el tema. No tiene nada de vergorzoso haber intentado los ejercicios y estar atorado en uno o varios; de hecho yo estaré en la mejor disposición de ayudarlos y aclararles sus dudas. Pero es muy importante que ustedes hagan un esfuerzo por aprenderse las definiciones, y que le dediquen al menos 10 minutos a cada ejercicio antes de darse por vencidos. Noten que esto involucra un compromiso de parte de ustedes de al menos unas 4 o 5 horas por semana fuera del salón de clases para dedicarle a mi materia.

Al final de estas notas hay un índice analítico, para facilitarles la vida si necesitan encontrar una definición o notación. Las palabras que aparecen en el índice analítico están en **negritas** en el texto. Casi siempre cerca de una definición hay ejercicios que tienen que ver con ella, y que les pueden servir de inspiración cuando estén resolviendo otros ejercicios.

Espero que estas notas les ayuden a entender mejor la teoría de módulos, y que aprendamos y nos divirtamos mucho en nuestro curso.

Capítulo 1

Anillos.

1.1. Anillos.

Definición 1. Un **semigrupo** es un conjunto junto con una operación binaria asociativa. Un **monoide** es un semigrupo $(M,*)$ en el que existe un elemento 1 tal que $1m = m = m1$ para todo $m \in M$. Usualmente denotamos al monoide $(M,*)$ por M, y escrimos mb en lugar de $m * b$.

Definición 2. Un **anillo** es una tercia ordenada $(A, +, \cdot)$, donde A es un conjunto no vacío y $+$, $\cdot$ son operaciones binarias asociativas en A que cumplen lo siguiente:

(1) $(A, +)$ es un grupo abeliano, cuyo elemento identidad se suele denotar 0, y comúnmente se llama el **cero** del anillo A. A veces lo escribiremos como 0_A para enfatizar el hecho de que es el cero del anillo A.

(2) $(A, \cdot)$ es un monoide, cuyo elemento identidad se suele denotar 1, y comúnmente se llama el **uno** del anillo A. A veces lo escribiremos como 1_A para enfatizar el hecho de que es el uno del anillo A.

(3) (Leyes distributivas) Para cualesquiera a, b, $c \in A$ se tiene que $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ y $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Usualmente denotamos un anillo $(A, +, \cdot)$ simplemente por A. La operación $+$ se llama **suma**, y la operación $\cdot$ el **producto** del anillo A. Siguiendo la convención para grupos abelianos, el inverso aditivo de a se denota $-a$. Usualmente escribimos ab en lugar de $a \cdot b$. Para algunos autores, nuestra definición de anillo es lo que ellos llaman un **anillo con uno**.

Notación 3. Al interpretar una expresión que involucre sumas y productos en un anillo, el producto lleva prioridad sobre la suma. Es decir, la expresión $a + bc$ se debe interpretar como $a + (bc)$.

Ejemplo 4. Los enteros, los racionales, los reales y los complejos con las operaciones usuales de suma y producto son anillos. Las matrices cuadradas con coeficientes en un anillo son a su vez un anillo con la suma y el producto usual de matrices.

Ejemplo 5. Sea A un conjunto con un sólo elemento. Entonces existe una única operación binaria en A, y A con esa operación binaria como suma y producto es un anillo conmutativo. A este tipo de anillo se le llama **anillo cero**.

Observación 6. Sea A un anillo. Entonces A es el anillo cero si y sólo si $0 = 1$.

Ejemplo 7. Sean A y B anillos. Tenemos que el producto cartesiano $A \times B$ es un anillo con suma y producto **coordenada a coordenada**, es decir, $(a, b) + (c, d) = (a + c, b + d)$ y $(a, b) \cdot (c, d) = (ac, bd)$. A este anillo se le llama el **producto directo externo** de A y B.

Ejemplo 8. Sea n un entero positivo. Demuestre que el conjunto de las n clases de equivalencias de los números enteros módulo n forma un anillo con la operación usual de suma y producto módulo n. Este anillo se llama el **anillo de los enteros módulo n** , y se denota $\mathbb{Z}/n\mathbb{Z}$.

Definición 9. Un anillo A es **conmutativo** si el producto de A es conmutativo, es decir, si para cualesquiera $a, b \in A$ se tiene que $ab = ba$.

Observación 10. En estas notas nos vamos a interesar principalmente en los anillos conmutativos. Sin embargo, muchos resultados valen en general para anillos no conmutativos.

Proposición 11. *Sea D un anillo conmutativo no cero. Son equivalentes las siguientes condiciones:*

(1) Para cualesquiera $a, b \in D$, si $a \neq 0$ y $b \neq 0$, entonces $ab \neq 0$.

(2) Para cualesquiera $a, b \in D$, si $ab = 0$, entonces $a = 0$ o $b = 0$.

(3) (Ley de la cancelación) Para cualesquiera $a, b, c \in D$, si $ab = ac$ y $a \neq 0$, entonces $b = c$.

*Un anillo conmutativo que satisfaga cualquiera de estas condiciones se llama un **dominio**, o también un **dominio entero**.*

Demostración: La segunda condición es la contrapositiva de la primera. La tercera condición es equivalente a la segunda a través de $a(b-c)=0$. □

Ejemplo 12. El anillo $\mathbb{Z}$ de los números enteros es un dominio entero. Las matrices cuadradas no forman un dominio entero, pues no son un anillo conmutativo.

Ejemplo 13. Sea $\mathbb{G}=\{n+mi \mid n,m\in\mathbb{Z}\}$, donde i denota una de las raíces cuadradas complejas de -1. Demuestre que $\mathbb{G}$ es un dominio entero con las operaciones usuales de suma y producto de números complejos. A este anillo se le conoce como el anillo de los **enteros Gaussianos**.

Ejemplo 14. Sea $A=\{n+m\sqrt{5} \mid n,m\in\mathbb{Z}\}$, donde $\sqrt{5}$ denota una de las raíces cuadradas reales de 5. Demuestre que A es un dominio entero con las operaciones usuales de suma y producto de números reales.

Proposición 15. *Sea A un anillo conmutativo no cero. Son equivalentes las siguientes condiciones:*

(1) Para cualquier $a\in A$, si $a\neq 0$, entonces existe $b\in A$ tal que $ab=1$.

(2) El conjunto $\{a\in A \mid a\neq 0\}$ forma un grupo con el producto de A.

*Un anillo que cumpla cualquiera de las condiciones anteriores se llama un **campo**. Algunos autores usan la palabra **cuerpo** en lugar de campo.*

Demostración: La primera parte se sigue de la segunda. La segunda se tiene porque el producto de A ya es asociativo y tiene un neutro (y por la primera parte hay inversos). □

Ejemplo 16. Tenemos que $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son campos, pero $\mathbb{Z}$ no.

Observación 17. Todo campo es un dominio entero. Los enteros son un dominio entero que no son campo.

Lema 18. *Sea A un anillo. Para cualquier $a\in A$ se tiene que $-(-a)=a$, es decir, el inverso aditivo del inverso aditivo de a es a.*

Demostración: Se sigue de que este resultado vale para grupos, y A forma un grupo con la suma. □

Definición 19. Sean A un anillo, $a\in A$ y n un entero positivo. Definimos $0a=0$ (donde el 0 de la izquierda está en $\mathbb{Z}$, y el 0 de la derecha está en A), $1a=a$, y $a^1=a$ (donde ambos 1's están en $\mathbb{Z}$). Inductivamente también

definimos $(n+1)a = na + a$ y $a^{n+1} = a^n a$. Además, definimos $(-n)a = -(na)$, donde -b denota al inverso aditivo de b en $(A, +)$. Los elementos de la forma na y (-n)a se llaman **múltiplos enteros** de a, y los elementos de la forma a^n se llaman **potencias** de a.

Observación 20. Sean A un anillo, $a \in A$, n, m enteros. Entonces:

- $(-1)a = -a$, donde -1 denota un elemento de $\mathbb{Z}$, y $-a$ denota el inverso aditivo de a en A.
- $(nm)a = n(ma)$, y $(n + m)a = na + ma$.
- si n, m son enteros positivos, entonces $(a^n)^m = a^{nm} = (a^m)^n$.

Definición 21. Sea A un anillo, y sea $a \in A$. Decimos que a es una **unidad** de A si existe un elemento $b \in A$ tal que $ab = 1 = ba$. Al conjunto de todas las unidades del anillo A lo denotamos A^*.

Observación 22. Sea A un anillo. Tenemos que el producto de dos unidades es una unidad. Así, A^* es un grupo con el producto de A. A este grupo se le llama el **grupo de unidades** del anillo A.

Ejemplo 23. El grupo de unidades de $\mathbb{Z}$ es cíclico de orden dos, y el grupo de unidades de $\mathbb{Z} \times \mathbb{Z}$ es isomorfo al grupo cuatro de Klein.

Definición 24. Sea A un anillo, y sean C y D subconjuntos de A. Definimos su **suma**, denotada C+D, como el conjunto $\{a+b \mid a \in C, b \in D\}$. Si $C = \{a\}$, usualmente escribimos $a + D$ en lugar de $\{a\} + D$.

Observación 25. Sean A un anillo y C, D, E subconjuntos de A. Tenemos que $(C + D) + E = C + (D + E)$. Por esta razón, este conjunto se denota $C + D + E$.

Ejemplo 26. En los enteros tenemos que $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.

Definición 27. Sean A un anillo, C un subconjunto de A y a un elemento de A. Definimos aC como el conjunto $\{ab \mid b \in C\}$. Análogamente se define Ca como el conjunto $\{ba \mid b \in C\}$.

Observación 28. Puede también definirse un producto para algunos subconjuntos de A, pero la definición no es la "obvia".

Definición 29. Sea A un anillo. Un **subanillo** de A es un subconjunto no vacío S que es cerrado bajo sumas, inversos aditivos y productos, y tal que existe un elemento $e \in S$ con la propiedad de que $ea = a = ae$ para todo $a \in S$. Note que e no necesariamente es igual al uno de A.

1.2. Ideales.

Definición 30. Sea A un anillo. Un **ideal izquierdo** de A es un subconjunto no vacío I que es cerrado bajo sumas e inversos aditivos, y tal que para todo $a \in A$ se tiene $aI \subseteq I$, es decir, para todo $i \in I$ tenemos que $ai \in I$. Análogamente se define un **ideal derecho** de A como un subconjunto no vacío I que es cerrado bajo sumas e inversos aditivos, y tal que para todo $a \in A$ se tiene $Ia \subseteq I$, es decir, para todo $i \in I$ tenemos que $ia \in I$.

Definición 31. Sea A un anillo. Un **ideal bilateral** de A (también llamado simplemente **ideal** de A) es un subconjunto no vacío I que es cerrado bajo sumas e inversos aditivos, y tal que para todo $a \in A$ se tiene $aI \subseteq I$ y $Ia \subseteq I$, es decir, para todo $i \in I$ tenemos que $ai \in I$ y $ia \in I$.

Observación 32. Si A es un anillo conmutativo, entonces los conceptos de ideal izquierdo, ideal derecho, e ideal bilateral coinciden.

Ejemplo 33. Sea A un anillo. Se tiene que A es un ideal bilateral de A, llamado el **ideal total** de A.

Definición 34. Sea A un anillo y sea I un ideal de A. Decimos que I es un ideal **propio** de A si $I \neq A$.

Ejemplo 35. Sea A un anillo. El conjunto $\{0\}$ es un ideal bilateral de A, llamado el **ideal cero** de A, y denotado usualmente 0.

Ejemplo 36. Sea n un entero positivo. El conjunto $n\mathbb{Z}$ que consta de los múltiplos enteros de n es un ideal de $\mathbb{Z}$. Más aún,todos los ideales no cero de $\mathbb{Z}$ son de esta forma.

1.3. Homomorfismos.

Definición 37. Sean A y B anillos, y sea $f\colon A \longrightarrow B$ una función. Decimos que f es un **homomorfismo de anillos** si cumple lo siguiente:

(1) $f(a+b) = f(a) + f(b)$ para cualesquiera $a, b \in A$;
(2) $f(ab) = f(a)f(b)$ para cualesquiera $a, b \in A$;
(3) $f(1_A) = 1_B$.

Algunos autores le llaman a esto un **homomorfismo de anillos con uno**, y reservan el nombre de homomorfismo de anillos a algo que cumpla

(1) y (2), aunque no mande al uno de A en el uno de B. Un **isomorfismo** es un homomorfismo biyectivo. Un **endomorfismo** es un homomorfismo de un anillo en sí mismo. Un **automorfismo** es un isomorfismo de un anillo en sí mismo. Dos anillos A y B son **isomorfos**, denotado $A \cong B$, si existe un isomorfismo de A en B.

Ejemplo 38. Sea A un anillo arbitrario. Demuestre que existe un único homomorfismo de $\mathbb{Z}$ en A, el cuál está dado por la fórmula $f(n) = n1_A$.

Ejemplo 39. No existen homomorfismos de anillos de $\mathbb{Z}/2\mathbb{Z}$ en $\mathbb{Z}/3\mathbb{Z}$, ni tampoco de $\mathbb{Z}/3\mathbb{Z}$ en $\mathbb{Z}/2\mathbb{Z}$.

Observación 40. La composición de dos homomorfismos de anillos es un homomorfismo de anillos.

Observación 41. Sea $f\colon A \longrightarrow B$ un homomorfismo de anillos. Entonces f es un homomorfismo entre sus grupos aditivos, y por lo tanto $f(0_A) = 0_B$.

Observación 42. Sean A y B anillos, $f\colon A \longrightarrow B$ un homomorfismo, y sea $a \in A$ una unidad. Entonces $f(a)$ es una unidad, y de hecho f se restringe a un homomorfismo de grupos de A^* a B^*. Se sigue que $f(a^{-1}) = f(a)^{-1}$.

Observación 43. Sean A y B anillos, $f : A \longrightarrow B$ un homomorfismo, y sea $a \in A$. Entonces f preserva múltiplos enteros y potencias, es decir, para cualquier entero n se tiene que $f(na) = nf(a)$, y si n es positivo, también se tiene $f(a^n) = f(a)^n$.

Ejemplo 44. Sea A un anillo. Tenemos que la **función identidad** de A, es decir, $id_A : A \longrightarrow A$ dada por $id_A(a) = a$ para toda a en A, es un automorfismo del anillo A.

Definición 45. Sean A y B anillos, y $f : A \longrightarrow B$ un homomorfismo. El **núcleo** de f, denotado $\mathrm{Ker}(f)$, es el conjunto $\{a \in A \mid f(a) = 0_B\}$. La **imagen** de f, denotada $\mathrm{Im}(f)$, es el conjunto $\{f(a) \mid a \in A\}$.

1.4. Ejercicios.

Ejercicio 46. Sea M un monoide. Demuestre que existe un único elemento 1 tal que $1\ m = m$ para todo $m \in M$. Al elemento 1 se le llama el **elemento identidad** del monoide M.

Ejercicio 47. Sea A un anillo. Demuestre que para cualquier $a \in A$ se tiene que $0a = 0a + 0a$. Concluya que $0a = 0$.

Ejercicio 48. Sea A un anillo. Demuestre que para cualquier $a \in A$ se tiene que $(-1)a = -a$, donde -1 denota al inverso aditivo de 1 en A, y $-a$ denota al inverso aditivo de a. Demuestre también que $a(-1) = -a$. Compare este ejercicio con la Proposición 20.

Ejercicio 49. Sea A un anillo. Demuestre que $(-1)(-1) = 1$.

Ejercicio 50. Sea A un anillo. Demuestre que para cualesquiera $a, b \in A$ se tiene que $(-a)b = -(ab) = a(-b)$.

Ejercicio 51. Sea A un anillo. Demuestre que para cualesquiera $a, b \in A$ se tiene que $(-a)(-b) = ab$.

Ejercicio 52. Sea A un anillo y sea $a \in A$ tal que existen $b, c \in A$ con $ab = 1 = ca$. Simplifique la expresión cab de dos maneras para demostrar que $b = c$. Concluya que a es una unidad. Al elemento b se le denota a^{-1}, y se le llama el **inverso multiplicativo** de la unidad a, o simplemente el **inverso** de la unidad a. Note que solamente las unidades tienen inversos multiplicativos.

Ejercicio 53. Sea $A = \mathbb{Z} \times \mathbb{Z}$. Demuestre que $S = \{(n, 0) \mid n \in \mathbb{Z}\}$ es un subanillo de A, y que el uno de A no pertenece a S.

Ejercicio 54. Sea A un anillo, y sea $a \in A$. Demuestre que el conjunto $Aa = \{ba \mid b \in A\}$ es un ideal izquierdo de A. Enuncie y demuestre un resultado análogo para ideales derechos.

Ejercicio 55. Sea A un dominio entero.

(a) Demuestre que para toda $a \in A$, la función $\mu_a : A \longrightarrow A$ dada por $\mu_a(b) = ab$ es inyectiva.

(b) Demuestre que todo dominio entero finito es un campo.

Ejercicio 56. Sea A un dominio entero. Demuestre que todo subanillo de A es un dominio entero.

Ejercicio 57. Sea A un anillo conmutativo no cero. Demuestre que A es un campo si y sólo si los únicos ideales de A son el cero y el total.

Ejercicio 58. Demuestre que la intersección arbitraria de ideales de un anillo es un ideal. Muestre con un ejemplo que la unión de dos ideales no necesariamente es un ideal.

Ejercicio 59. Sea A un anillo y sea C un subconjunto de A. Demuestre que existe un único ideal I con las siguientes propiedades:

(1) $C \subseteq I$;

(2) Para todo ideal J de A, si $C \subseteq J$ entonces $I \subseteq J$.

Al ideal I se le llama el **ideal generado** por el conjunto C, y se le denota $< C >$. Si $C = \{a_1, \ldots, a_n\}$, uno escribe $<a_1, \ldots, a_n>$ en lugar de $< C >$.

Ejercicio 60. Sea A un anillo conmutativo, y sea $a \in A$. Demuestre que $< a >= aA$. Muestre con un ejemplo que este resultado no es válido para anillos no conmutativos.

Ejercicio 61. Sean A un anillo, I y J ideales de A. Demuestre que $I + J$ es un ideal de A. Más aún, demuestre que $I + J$ está contenido en cualquier ideal que contenga tanto a I como a J. En otras palabras, $I + J$ es el ideal generado por $I \cup J$.

Ejercicio 62. Demuestre que el inverso de un isomorfismo es un isomorfismo.

Ejercicio 63. Sean A y B anillos, y $f : A \longrightarrow B$ un homomorfismo. Demuestre que $\mathrm{Ker}(f)$ es un ideal de A.

Ejercicio 64. Sean A y B anillos, y $f : A \longrightarrow B$ un homomorfismo. Demuestre que f es inyectivo si y sólo si $\mathrm{Ker}(f)$ es el ideal cero.

Ejercicio 65. Sean K un campo, A un anillo no cero y $f : K \longrightarrow A$ un homomorfismo de anillos. Demuestre que f es inyectiva.

Ejercicio 66. Sean A y B anillos, y $f : A \longrightarrow B$ un homomorfismo. Demuestre que $\mathrm{Im}(f)$ es un subanillo de B. Dé un ejemplo en el que $\mathrm{Im}(f)$ no sea un ideal de H.

Capítulo 2

Dominios de ideales principales.

2.1. Divisibilidad.

Definición 67. Sea A un anillo conmutativo, y sean $a, b \in A$. Decimos que a **divide** a b, denotado $a \mid b$, si existe $c \in A$ tal que $ac = b$. También decimos que a es un **divisor** de b, o que b es un **múltiplo** de a.

Definición 68. Sea A un anillo conmutativo, y sean $a, b \in A$. Decimos que a es **asociado** a b en A si existe una unidad u de A tal que $a =u\ b$. La relación "ser asociado a" es una relación de equivalencia en A. Si a es asociado a b en A, también decimos que a y b son **asociados** en A. Si no hay riesgo de confusión, decimos simplemente que a y b son asociados.

Ejemplo 69. Los números 2 y 3 no son asociados en los enteros, pero que sí son asociados en los racionales.

2.2. Máximo común divisor.

Definición 70. Sea D un dominio entero, y sean $d, c, b \in D$. Decimos que b es un **máximo común divisor** de d y c si se cumple lo siguiente:

(a) b es un divisor de d y de c

(b) para cualquier $a \in D$, si a es un divisor de d y de c, se tiene que a es un divisor de b.

Si los elementos d, c y b pertenecen a varios dominios enteros y hay riesgo de confusión, nos referiremos a b como a un máximo común divisor de d y c en D.

Ejemplo 71. Se tiene que 2 no es un máximo común divisor de 2 y 3 en los enteros, pero 2 sí es un máximo común divisor de 2 y 3 en los racionales.

Lema 72. *Sea D un dominio entero, y sean $d, c \in D$. Cualesquiera dos máximos comunes divisores de d y c son asociados. Cualquier asociado a un máximo común divisor de d y c es un máximo común divisor de d y c.*

Demostración: Para establecer el primer enunciado, basta notar que d y c se dividen mutuamente. El segundo se sigue de que los asociados mantienen las mismas relaciones de divisibilidad. □

2.3. Elementos irreducibles y elementos primos.

Definición 73. Sea D un dominio entero, y sea d un elemento en D. Decimos que d es un elemento **irreducible** en D si cumple lo siguiente:

(a) d es diferente de 0

(b) d no es una unidad de D

(c) los únicos divisores de d son las unidades de D y los asociados de d

Definición 74. Sea D un dominio entero, y sea d un elemento de D. Decimos que d es un elemento **primo** de D si cumple lo siguiente:

(a) d es diferente de 0

(b) d no es una unidad de D

(c) para cualesquiera c, b en D, si d divide a c b, entonces d divide a c o d divide a b.

2.4. Dominios de factorización única.

Definición 75. Sea D un dominio entero. Decimos que D es un **dominio de factorización única** si ocurre lo siguiente:

(1) Para todo elemento distinto de 0 y que no sea unidad de D, existe una factorización en elementos irreducibles.

(2) Cualesquiera dos factorizaciones del mismo elemento en irreducibles son iguales salvo asociados, es decir, existe una biyección entre el conjunto de irreducibles de una factorización y el conjunto de irreducibles de la otra factorización de tal manera que elementos correspondientes son asociados.

Ejemplo 76. Todo campo es un dominio de factorización única.

Definición 77. Sea D un dominio entero. Sean d y c elementos de D. Decimos que d es un **factor propio** de c si d divide a c pero c no divide a d. Decimos que D satisface la **condición de cadena de divisores** si D no contiene una sucesión infinita de elementos $d_1, d_2, \ldots$ tales que cada d_{i+1} es un factor propio de d_i.

Definición 78. Sea D un dominio entero. Decimos que D satisface la **condición de primalidad** si todo elemento irreducible en D es primo.

Lema 79. *Sea D un dominio entero que satisface las condiciones de cadena de divisores y de primalidad. Entonces D es de factorización única.*

Demostración: Se sigue de los Ejercicios 101 y 102 □

Lema 80. *Sean d y c elementos no cero en un dominio de factorización única. Entonces d divide a c si y sólo si todo irreducible en una factorización de d aparece (hasta asociado) en c a una potencia mayor o igual.*

Demostración: Suponga que d divide a c, y considere un irreducible p que divida a a d. Entonces se sigue que p divide a c, y cancelando p obtenemos un d' y un c' tales que d' divide a c' y d' tiene un irreducible menos que d en su factorización. Por inducción en el número de irreducibles en d se tiene el resultado deseado. La otra parte de la demostración es inmediata. □

Proposición 81. *En un dominio de factorización única, cualesquiera dos elementos diferentes de cero tienen al menos un máximo común divisor.*

Demostración: Considere sendas factorizaciones de los dos elementos. Escoja irreducibles comunes (hasta asociados) a las mínimas potencias. □

2.5. Dominios de ideales principales.

Definición 82. Sea D un dominio entero. Decimos que un ideal de D es **principal** si está generado por un sólo elemento. Decimos que D es un **dominio de ideales principales** si todo ideal de D es principal.

Ejemplo 83. Todo campo es un dominio de ideales principales. Los enteros son un dominio de ideales principales.

Teorema 84. *Todo domino de ideales principales es un dominio de factorización única.*

Demostración: Se sigue de los Ejercicios 105 y 79. □

Definición 85. Sea A un anillo conmutativo, y sean a y b elementos de A. Decimos que un elemento c de A es **combinación lineal** de a y b si existen d y e en A tales que $c = ad + be$.

Proposición 86. *Sea D un dominio de ideales principales, y sean d y c elementos diferentes de cero en D. Demuestre que existe un máximo común divisor de d y c. Demuestre que cualquier máximo común divisor de d y c se puede escribir como combinación lineal de d y c.*

Demostración: Sea $I = \{db + ca \mid b, a \in D\}$. Tenemos que I es un ideal de D, y por tanto existe α en D tal que I es el ideal generado por α. Afirmamos que α es un máximo común divisor de d y c. Como d y c son elementos de I, se sigue que α es un divisor común. Por otro lado, cualquier otro divisor común de d y c divide a α pues α es un elemento de I y es por tanto una combinación lineal de d y c. □

2.6. Dominios euclidianos.

Definición 87. Sea D un dominio entero. Una **norma euclidiana** en D es una función $\partial : D - \{0\} \longrightarrow \mathbb{Z}$ con las siguientes propiedades:

(1) La función ∂ nunca toma valores negativos.

(2) Para cualesquiera elementos d, c de D diferentes de 0, existen q y r en D tales que $d = cq + r$, donde $r = 0$ o $\partial(r) < \partial(c)$.

Si D es un dominio entero en el que se puede definir una norma euclidiana, decimos que D es un **dominio euclidiano**.

Ejemplo 88. Todo campo es un dominio euclidiano, con norma euclidiana constante cero (o cualquier otra cantidad no negativa). Los enteros son un dominio euclidiano, con norma euclidiana dada por el valor absoluto.

Observación 89. *(Algoritmo euclidiano)* Sea D un dominio euclidiano con norma euclidiana ∂, y sean d, c elementos diferentes de cero en D. Si c divide a d, entonces c es un máximo común divisor de d y c. Si c no divide a d, y $d = cq + r$ con $r \neq 0$ y $\partial(r) < \partial(c)$, entonces el conjunto de máximos comunes

divisores de d y c coincide con el conjunto de máximos comunes divisores de c y r. Utilizando este argumento recursivamente tenemos un algoritmo que calcula un máximo común divisor de d y c.

2.7. Anillos de polinomios.

Definición 90. Sea A un anillo conmutativo. Un **polinomio** con coeficientes en A es una sucesión infinita $p = (p_0, p_1, p_2, \dots)$ que cumple lo siguiente:

(1) $p_i \in A$ para toda $i = 0, 1, 2, \dots$

(2) Existe un entero N tal que $p_n = 0$ para toda $n \geq N$.

Notación 91. Sea A un anillo conmutativo y sea $p = (p_i)_{i=0}^{\infty}$ un polinomio con coeficientes en A. Usualmente denotamos al polinomio p como $p(x)$, y llamamos a la "x" una "indeterminada". Además, si $p_i = 0$ para toda $i = 0, 1, \dots,$ llamamos a p el **polinomio cero**, y lo denotamos 0. Si $p \neq 0$, entonces existe un único entero no negativo n tal que $p_n \neq 0$ y $p_i = 0$ para toda $i > n$. A tal n la llamamos el **grado** del polinomio $p(x)$, y usualmente en lugar de escribir $p = (p_i)_{i=0}^{\infty}$ escribimos $p(x) = p_0 + p_1x + p_2x^2 + p_3x^3 + \cdots + p_nx^n$. A los elementos p_i los llamamos los **coeficientes** del polinomio $p(x)$. A las expresiones p_ix^i las llamamos los **términos** del polinomio p (x). Si algún p_i es igual a 1, usualmente escribimos x^i en lugar de $1x^i$. Si algún p_i es igual a 0, usualmente omitimos el término $0x^i$ en la descripción del polinomio $p(x)$. Al elemento p_n lo llamamos el **coeficiente principal** del polinomio $p(x)$, y al elemento p_0 lo llamamos el **término constante** del polinomio $p(x)$. Si el coeficiente principal de $p(x)$ es 1, decimos que $p(x)$ es un polinomio **mónico**. Si el grado de $p(x)$ es cero, decimos que $p(x)$ es un polinomio **constante**. El polinomio cero también es un polinomio constante, pero no se le asigna un grado. Los polinomios constantes usualmente se identifican con los elementos del anillo conmutativo A. Al anillo de polinomios con coeficientes en A se le denota como $A[x]$.

Definición 92. Sean $p_0 + p_1x + \cdots + p_nx^n$y $q_0 + q_1x + \cdots + q_mx^m$polinomios con coeficientes en un anillo conmutativo A. Definimos su suma $p_0 + p_1x + \cdots + p_nx^n + q_0 + q_1x + \cdots + q_mx^m$como el polinomio $(p_i + q_i)_{i=0}^{\infty}$, y su producto como el polinomio cuya entrada i-ésima es $\sum_{j=0}^{i} p_j q_{i-j}$.

Observación 93. La suma de polinomios es asociativa, conmutativa, y tiene al polinomio constante 0 como elemento neutro. Además tiene inversos. El

producto de polinomios es asociativo, conmutativo, y tiene al polinomio constante 1 como elemento neutro. Los únicos polinomios que tienen inverso multiplicativo son los polinomios constantes representados por unidades en el anillo A.

Definición 94. Sea D un anillo conmutativo, sea A un anillo conmutativo que contiene a D, y sea $a \in A$. La **función evaluación** en a de $D[x]$ a A es el homomorfismo de anillos $f_a : D[x] \longrightarrow A$ definido en los escalares como la inclusión de D en A, y que manda a x en a. Denotamos usualmente a la imagen del polinomio p bajo la función evaluación en a por $p\ (a)$. Si $p\ (a)$=0 decimos que a es una **raíz** del polinomio p.

Notación 95. Por convención, en $k[x]$ se pide que el máximo común divisor de dos polinomios sea un polinomio mónico, y por lo tanto, es único.

2.8. Ejercicios.

Ejercicio 96. Sea A un anillo conmutativo. Demuestre que $a \mid 0$ y $a \mid a$ para cualquier $a \in A$. Demuestre que $0 \mid a$ si y sólo si a =0. Demuestre que a es una unidad de A si y sólo si $a \mid 1$.

Ejercicio 97. Demuestre que la divisibilidad es una propiedad reflexiva y transitiva.

Ejercicio 98. Sea A un anillo conmutativo, y sean $a, b, c \in A$. Demeustre que si a divide a b y c, entonces a divide a $bd+ce$ para cualesquiera $d, e \in A$.

Ejercicio 99. Sea D un dominio entero y sean $d, c \in D$. Demuestre que $d \mid c$ y $c \mid d$ si y sólo si d y c son asociados en D.

Ejercicio 100. Sea D un dominio entero, y sean $d, c, b, a \in D$ tales que $d = cb + a$. Demuestre que el conjunto de los máximos comunes divisores de d y c coincide con el conjunto de los máximos comunes divisores de c y a.

Ejercicio 101. Sea D un dominio entero, y sea d un elemento de D que no sea cero ni unidad. Demuestre que si d no es irreducible, entonces tiene un factor propio que no es unidad. Demuestre que si además D satisface la condición de cadena de divisores, entonces d tiene un factor irreducible. Demuestre que en un dominio entero que satisfaga la condición de cadena de divisores, todo elemento (que no sea unidad ni cero) tiene al menos una

factorización en irreducibles (aunque no necesariamente dicha factorización es única).

Ejercicio 102. Sea D un dominio entero que satisface la condición de primalidad. Demuestre que si un elemento de D tiene dos factorizaciones en irreducibles, entonces existe una biyección entre los irreducibles donde irreducibles correspondientes son asociados (es decir, la factorización es única).

Ejercicio 103. Demuestre que todo elemento primo es irreducible.

Ejercicio 104. Demuestre que en un dominio de factorización única, un elemento es irreducible si y sólo si es primo.

Ejercicio 105. Sea D un dominio de ideales principales. Demuestre que D satisface las condiciones de cadena de divisores y de primalidad.

Ejercicio 106. Demuestre que todo dominio euclidiano es un dominio de ideales principales (y por lo tanto también es un dominio de factorización única).

Ejercicio 107. Calcule un máximo común divisor de 314880 y 97102350 en los enteros.

Ejercicio 108. Sea D un anillo conmutativo. Demuestre que D es un dominio entero si y sólo si D [x] es un dominio entero.

Ejercicio 109. Demuestre que el ideal de $\mathbb{Z}[x]$ generado por x y 2 no es un ideal principal. Concluya que aunque D sea un dominio de ideales principales, D [x] no necesariamente es dominio de ideales principales.

Ejercicio 110. Sea k un campo, y sean $f(x)$, $g(x)$ y $h(x)$ polinomios en $k[x]$ tales que el máximo común divisor de $f(x)$ y $g(x)$ en $k[x]$ es 1. Demuestre que si $f(x)$ divide a $g(x)h(x)$, entonces $f(x)$ divide a $h(x)$.

Ejercicio 111. Sea k un campo, y sean $f(x)$ y $g(x)$ polinomios en $k[x]$. Sea F un campo que contiene a k. Demuestre que el máximo común divisor de $f(x)$ y $g(x)$ en $k[x]$ es también el máximo común divisor de $f(x)$ y $g(x)$ en $F[x]$.

Ejercicio 112. Sea $f \in k[x]$ un polinomio de grado 2 o 3. Demuestre que f es irreducible en $k[x]$ si y sólo si f no tiene raíces en k. (Comentario: este criterio falla en grado 4: el polinomio $(x^2+1)^2$ no tiene raíces en los reales y no es irreducible en $\mathbb{R}[x]$.)

Ejercicio 113. Sean $p_0 + p_1 x + \cdots + p_n x^n$y $q_0 + q_1 x + \cdots + q_m x^m$polinomios distintos de cero con coeficientes en un dominio entero D. Demuestre que el grado del producto $p\ q$ es la suma de sus grados. (Comentario: este resultado no es cierto si se reemplaza el dominio entero D con un anillo conmutativo. Tome por ejemplo dos divisores de cero d y c, y multiplique los polinomios dx y $cx^2 + x$.)

Ejercicio 114. Sea D un dominio entero y sea p un polinomio con coeficientes en D. Demuestre que el número de factores en cualquier descomposición de p como producto de polinomios irreducibles (no necesariamente distintos) es menor o igual al grado de p. Concluya que el número de raíces de p (contando raíces múltiples tantas veces como su multiplicidad) es menor o igual a su grado.

Ejercicio 115. Sea k un campo. Demuestre que $k[x]$ es un dominio euclidiano con norma euclidiana dada por el grado. (Comentario: así, $k[x]$ también es un dominio de ideales principales, y por lo tanto $k[x]$ también es un dominio de factorización única. Se sigue que los elementos irreducibles de $k[x]$ coinciden con los elementos primos en $k[x]$, y que dos elementos no cero cualesquiera siempre tienen máximos comunes divisores en $k[x]$.)

Capítulo 3

Módulos.

3.1. Módulos, submódulos y módulos cociente.

Definición 116. Sean A un anillo y M un grupo abeliano. Decimos que M es un **módulo izquierdo** sobre A, o también que es un A-módulo izquierdo (denotado ${}_AM$) si existe una **acción** del anillo A en el grupo abeliano M, es decir, una función $\cdot : A \times M \longrightarrow M$ (denotada am en lugar de $\cdot(a, m)$ para $a \in A, m \in M$) que cumple lo siguiente para todos $a, b \in A$, para todos $m, n \in M$::

- $(a + b)m = am + bm$
- $a(m + n) = am + an$
- $(ab)m = a(bm)$
- $1m = m$

Ejemplo 117. Sea A un anillo cualquiera, y sea M un grupo abeliano trivial. Entonces M tiene una única acción de A. A este módulo se le llama **módulo cero**, y se le denota 0.

Ejemplo 118. Sea A un anillo cualquiera. El anillo A es un módulo con acción dada por su multiplicación. A este módulo se le llama **módulo regular**.

Ejemplo 119. Todo grupo abeliano es un módulo izquierdo sobre el anillo de los enteros, con acción $0g = 0,\ (n + 1)g = ng + g,\ (-n)g = -(ng)$.

Ejemplo 120. Sean k un campo, M un grupo abeliano. Entonces M es un k-módulo izquierdo si y sólo si M es un espacio vectorial sobre k.

Ejemplo 121. Sean k un campo, $A = k[x]$, V un espacio vectorial sobre k, $T\colon V \longrightarrow V$ una transformación lineal. Podemos darle a V una estructura de A-módulo izquierdo definiendo la acción $f(x) \cdot v = f(T)(v)$, donde $f(T)$ denota a la transformación lineal de V en V que se obtiene de evaluar al polinomio $f(x)$ en T. Este $k[x]$-módulo se denota $V\,(T)$

Definición 122. Sean A un anillo y M un grupo abeliano. Decimos que M es un **módulo derecho** sobre A, o también que es un A-módulo derecho (denotado M_A) si existe una **acción derecha** del anillo A en el grupo abeliano M, es decir, una función $\cdot : M \times A \longrightarrow M$ (denotada ma en lugar de $\cdot(m, a)$ para $a \in A, m \in M$) que cumple lo siguiente para todos $a, b \in A$, para todos $m, n \in M$::

- $m(a + b) = ma + mb$
- $(m + n)a = ma + na$
- $m(ab) = (ma)b$
- $m1 = m$

Ejemplo 123. Sean A un anillo y M un A-módulo izquierdo. Sea B el anillo opuesto de A (es decir, el conjunto subyacente de B es A y la suma también es la de A, pero el producto de a y b en B es ba en lugar de ab). Entonces M es un B-módulo derecho, con acción $*$ dada por $m * a = am$. Note que en particular si A es un anillo conmutativo, entonces $A = B$, y todo A-módulo izquierdo es un A-módulo derecho.

Definición 124. Sean A, B anillos y M un grupo abeliano. Decimos que M es un **bimódulo** sobre A y B, o también que es un A-B-bimódulo (denotado ${}_AM_B$), si es posible definir en M una acción izquierda de A y una acción derecha de B de tal forma que se tenga $(am)b = a(mb)$ para todos $a \in A, b \in B, m \in M$.

Ejemplo 125. Sean A el anillo de los enteros, B un anillo, y M un B-módulo derecho. Note que M es un A-módulo izquierdo por lo visto en el Ejemplo 119. Más aún, M es un A-B-bimódulo.

Notación 126. De aquí en adelante, la palabra "módulo" significará "módulo izquierdo".

Definición 127. Sean A un anillo y M un módulo sobre A. Sea N un subconjunto de M. Decimos que N es un **submódulo** de M si N es un subgrupo abeliano de M y si para todo $a \in A$ y todo $n \in N$ se tiene $an \in N$.

Ejemplo 128. Sea M un A-módulo. Entonces 0 y M son submódulos de M.

Ejemplo 129. Sea A un anillo, y sea M el módulo regular. Los submódulos de M son exactamente los ideales izquierdos de A.

Ejemplo 130. Sea M un grupo abeliano, es decir, un $\mathbb{Z}$-módulo. Todo subgrupo de M es un submódulo de M.

Ejemplo 131. Sea *V (T)* un módulo (es decir, hay un un campo k, un k-espacio vectorial V, y una transformación lineal $T\colon V \longrightarrow V$). Un submódulo de *V (T)* es un subespacio vectorial W de V que es **invariante** bajo T, es decir, tal que $T(v) \in W$ para todo $v \in W$.

Definición 132. Sean A un anillo, M un módulo sobre A y N un submódulo de N. Sea M/N el grupo cociente de clases laterales de N en M. Podemos definir una acción de A en M/N por medio de $a(m+N) = am+N$. Esta acción está bien definida (es decir, no depende del representante de la clase lateral), e induce una estructura de módulo en M/N, llamado **módulo cociente**. La función que va de M a N que asigna a cada elemento m en M su clase lateral $m + N$ es un homomorfismo de módulos, y se le llama la **aplicación cociente**.

Ejemplo 133. Sea M un $\mathbb{Z}$-módulo, y sea N un submódulo de M. El módulo cociente M/N es el grupo cociente usual.

3.2. Homomorfismos.

Definición 134. Sean A un anillo, M y N módulos sobre A, y $f\colon M \longrightarrow N$ una función. Decimos que f es un **homomorfismo de módulos** si para todos $m, n \in M$ y para todo $a \in A$ se tiene $f(am + n) = af(m) + f(n)$. El conjunto de todos los homomorfismos de A-módulos de M a N se denota $Hom_A(M, N)$. Un **isomorfismo** es un homomorfismo biyectivo. Si existe un isomorfismo de M a N, decimos que M y N son **isomorfos**, y lo denotamos $M \cong b$.

Ejemplo 135. Sean M y N $\mathbb{Z}$-módulos. Entonces los homomorfismos de $\mathbb{Z}$-módulos de M a N coinciden con los homomorfismos de grupos de M a N.

Ejemplo 136. Sean k un campo, V y W k-espacios vectoriales, $T: V \longrightarrow V$ y $U: W \longrightarrow W$ transformaciones lineales, V *(T)* y W *(U)* los respectivos módulos sobre $k[x]$. Un homomorfismo de V *(T)* a W *(U)* es una transformación lineal $F: V \longrightarrow W$ tal que $F \circ T = U \circ F$.

Teorema 137. ***(Primer teorema de isomorfismo)*** *Sean M y N A-módulos, y sea $f: M \longrightarrow N$ un homomorfismo con núcleo K. Entonces K es un submódulo de M y M/K es isomorfo a la imagen de f. Más aún, la función $\bar{f}: M/K \longrightarrow Im(f)$ dada por $\bar{f}(m+K) = f(m)$ es un isomorfismo.*

Demostración: La primera parte es un ejercicio. La función $\bar{f}$ es un isomorfismo de grupos por el Primer teorema de isomorfismo para grupos. Esta función también preserva la acción del anillo, y es por tanto un isomorfismo de A-módulos. □

Teorema 138. ***(Segundo teorema de isomorfismo)*** *Sean M un A-módulo, N un submódulo cualquiera de M y K otro submódulo de M. Entonces $N \cap K$ es un submódulo de N y $N/(N \cap K)$ es isomorfo a $(N+K)/K$.*

Demostración: El isomorfismo del Segundo teorema de isomorfismo para grupos es también un isomorfismo de módulos. □

Teorema 139. ***(Tercer teorema de isomorfismo)*** *Sea M un módulo, y sean N y K submódulos de M con $N \leq K$. Entonces K/N es un submódulo de M/N y $(M/N)/(K/N)$ es isomorfo a M/K.*

Demostración: El isomorfismo del Tercer teorema de isomorfismo para grupos es también un isomorfismo de módulos. □

3.3. Módulos finitamente generados, módulos noetherianos, y sucesiones exactas.

Definición 140. Sean A un anillo, M un módulo y C un subconjunto de M. Decimos que C **genera** a M si para todo $m \in M$ existen $m_1, \ldots, m_t \in C$ y $a_1, \ldots, a_t \in A$ tales que $m = a_1 m_1 + \cdots + a_t m_t$. Decimos que el módulo M es un A-módulo **finitamente generado** si existe un subconjunto finito de M que lo genera.

Ejemplo 141. Sea A un anillo arbitrario. El módulo regular está finitamente generado (por el uno del anillo).

Definición 142. Sean A un anillo y M un módulo sobre A. Decimos que M es un módulo **noetheriano** si todo submódulo de M está finitamente generado. Decimos que el anillo A es noetheriano si el A-módulo regular es noetheriano.

Ejemplo 143. Sea A un dominio de ideales principales. Entonces el módulo regular es noetheriano, pues sus submódulos son los ideales de A, que por ser principales, están finitamente generados. Por lo tanto, A es un anillo noetheriano. En particular $\mathbb{Z}$ y $k[x]$ son anillos noetherianos.

Definición 144. Sea A un anillo. Una **sucesión exacta** de A-módulos es una sucesión $M_1, \ldots, M_t$ de módulos sobre A junto con una sucesión $f_i : M_i \longrightarrow M_{i+1}$ de homomorfismos de módulos tales que el núcleo de f_{i+1} es igual a la imagen de f_i.

Ejemplo 145. Sean M un módulo, N un submódulo, $f : N \longrightarrow M$ la inclusión y $g : M \longrightarrow M/N$ la aplicación cociente. Entonces la sucesión

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} M/N \longrightarrow 0$$

es una sucesión exacta de módulos. A este tipo de sucesión se le llama **sucesión exacta corta**.

3.4. Ejercicios.

Ejercicio 146. Sea M un A-módulo. Demuestre que el homomorfismo de M en M que manda a todos los elementos de M al elemento neutro 0 es un homomorfismo de A-módulos, llamado **homomorfismo cero**. Demuestre también que la función identidad de M en M es un isomorfismo de A-módulos.

Ejercicio 147. Sea M un A-módulo tal que para cualquier A-módulo N existe un único homomorfismo $f : M \longrightarrow N$. Demuestre que $M = 0$.

Ejercicio 148. Sea M un A-módulo tal que para cualquier A-módulo N existe un único homomorfismo $f : N \longrightarrow M$. Demuestre que $M = 0$.

Ejercicio 149. Sea A un anillo cualquiera (no necesariamente conmutativo), y sea M el A-módulo regular. Sea $a \in M$ arbitrario, y sea $f : M \longrightarrow M$ dada por $f(x) = xa$. Demuestre que f es un homomorfismo de A-módulos izquierdos.

Ejercicio 150. Demuestre que la composición de dos homomorfismos de módulos es un homomorfismo de módulos.

Ejercicio 151. Demuestre que el inverso de un isomorfismo de módulos es un isomorfismo de módulos. Concluya que si $M \cong N$ entonces $N \cong M$.

Ejercicio 152. Demuestre que si $M \cong N$ y $N \cong K$ entonces $M \cong K$.

Ejercicio 153. Dé un ejemplo de un anillo A y dos A-módulos M y N distintos de cero tales que el único homomorfismo de M en N sea el homomorfismo cero, y el único homomorfismo de N en M sea también cero.

Ejercicio 154. Sea $f : M \longrightarrow N$ un homomorfismo de módulos. El **núcleo** de f, denotado $Ker(f)$, es el conjunto $Ker(f) = \{m \in M \mid f(m) = 0\}$. Demuestre que $Ker(f)$ es un submódulo de M.

Ejercicio 155. Sea $f : M \longrightarrow N$ un homomorfismo de módulos. La **imagen** de f, denotada $Im(f)$, es el conjunto $Im(f) = \{f(m) \mid m \in M\}$. Demuestre que $Im(f)$ es un submódulo de N.

Ejercicio 156. Demuestre que $\mathbb{Q}$ no es un $\mathbb{Z}$-módulo finitamente generado. Explique por qué esto no contradice la noetherianidad de $\mathbb{Z}$.

Ejercicio 157. Sea

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} K \longrightarrow 0$$

una sucesión exacta de módulos. Demuestre que $K \cong (M/N)$.

Capítulo 4

Sumas directas y productos de módulos.

4.1. Definiciones.

Definición 158. Sean A un anillos, $\{M_i\}_{i\in I}$ una familia de A-módulos. El **producto** de los A-modulos $\{M_i\}_{i\in I}$, denotado $\prod_{i\in I} M_i$, es el producto cartesiano de los M_i como conjuntos, donde la suma y la multiplicación por escalares se realizan coordenada a coordenada. La **suma directa externa** de los A-modulos $\{M_i\}_{i\in I}$, denotada $\oplus_{i\in I} M_i$, es el submódulo del producto que consta de los elementos (m_i) que son cero **para casi toda** i, es decir, todas salvo un número finito.

Observación 159. Si el conjunto de índices I es finito, entonces el producto $\prod_{i\in I} M_i$ es igual a la suma directa externa $\oplus_{i\in I} M_i$. Si el conjunto I es infinito, en general el producto y la suma directa son diferentes, e incluso pueden no ser isomorfos.

Definición 160. Sean A un anillo, M un A-módulo, y $\{M_i\}_{i\in I}$ una familia de submódulos de M. Decimos que M es la **suma directa interna** de los $\{M_i\}_{i\in I}$, y lo denotamos $M = \oplus_{i\in I} M_i$, si todo elemento de M se puede escribir de manera única como una suma de elementos de los M_i. En este caso decimos que cada M_i es un **sumando directo** de M, y lo denotamos $M_i \mid M$.

Ejemplo 161. Todo módulo M tiene como sumandos directos a M mismo y al submódulo cero.

Definición 162. Sea A un anillo. Un A-módulo M es **libre** si M es isomorfo a una suma directa externa de copias del módulo regular A.

Ejemplo 163. Si A es un campo, entonces todo A-módulo es libre, pues tiene una base indexada por un conjunto I, y es por tanto isomorfo a la suma directa externa de I copias del campo A.

4.2. Propiedades universales.

Teorema 164. *(Propiedad universal del producto de módulos) Sean A un anillo y $\{M_i\}_{i\in I}$ una familia de A-módulos. Denote por P el producto de dicha familia de módulos. Para cada $j \in I$, la función $\pi_j : P \longrightarrow M_j$ dada por $\pi_j((m_i)) = m_j$ es un homorfismo de A-módulos, y se le llama la **proyección** a M_j. Si X es otro A-módulo junto con una familia de homorfismos de A-módulos $p_j : X \longrightarrow M_j$, entonces existe un único homomorfismo de A-módulos $p : X \longrightarrow P$ tal que $\pi_j \circ p = p_j$ para toda $j \in I$.*

Demostración: La única función que cumple la última condición está dada por $p(x) = (p_i(x))$. Es inmediato verificar que esta función es de hecho un homomorfismo de A-módulos. Si X es otro A-módulo junto con una familia de homorfismos de A-módulos $p_j : X \longrightarrow M_j$, entonces existe un único homomorfismo de A-módulos $p : X \longrightarrow P$ tal que $\pi_j \circ p = p_j$ para toda $j \in I$. □

Corolario 165. *Sean A un anillo y $\{M_i\}_{i\in I}$ una familia de A-módulos. Sea Y otro A-módulo junto con una familia de homomorfismos $q_j : Y \longrightarrow M_j$. Suponga que para cualquier otro A-módulo X junto con una familia de homorfismos de A-módulos $p_j : X \longrightarrow M_j$, existe un único homomorfismo de A-módulos $q : X \longrightarrow Y$ tal que $q_j \circ q = p_j$ para toda $j \in I$. Entonces Y es isomorfo al producto de dicha familia de módulos.*

Demostración: Basta hacer competir al producto P y al módulo Y para encontrar funciones $p : Y \longrightarrow P$ y $q : P \longrightarrow Y$ que cumplan $\pi_j \circ p = q_j$ y $q_j \circ q = \pi_j$ para toda $j \in I$. Luego se pone a competir P consigo mismo para demostrar que $p \circ q$ es la identidad en P, y Y consigo mismo para demostrar que $q \circ p$ es la identidad en Y, por lo que p y q son isomorfismos. □

Teorema 166. *(Propiedad universal de la suma directa externa de módulos) Sean A un anillo y $\{M_i\}_{i\in I}$ una familia de A-módulos. Denote por S la suma*

directa externa de dicha familia de módulos. Para cada $j \in I$, la función $\lambda_j : M_j \longrightarrow S$ dada por $\lambda_j(m) = (m_i)$ con $m_i = 0$ para $i \neq j$ y $m_j = m$, es un homorfismo de A-módulos, y se le llama la ***inclusión*** *de M_j. Si X es otro A-módulo junto con una familia de homorfismos de A-módulos $l_j : M_j \longrightarrow X$, entonces existe un único homomorfismo de A-módulos $q : S \longrightarrow X$ tal que $q \circ \lambda_j = l_j$ para toda $j \in I$.*

Demostración: La única función que cumple la última condición es $q(x_i) = \sum l_i(x_i)$, donde la suma se toma únicamente sobre el conjunto finito de las x_i distintas de cero. Es inmediato verificar que esta función es de hecho un homomorfismo de A-módulos. □

Corolario 167. *Sean A un anillo y $\{M_i\}_{i \in I}$ una familia de A-módulos. Sea Y otro A-módulo junto con una familia de homomorfismos $q_j : M_j \longrightarrow Y$. Suponga que para cualquier otro A-módulo X junto con una familia de homorfismos de A-módulos $p_j : M_j \longrightarrow X$, existe un único homomorfismo de A-módulos $p : Y \longrightarrow X$ tal que $p \circ q_j = p_j$ para toda $j \in I$. Entonces Y es isomorfo a la suma directa externa de dicha familia de módulos.*

Demostración: Basta hacer competir a la suma directa externa S y al módulo Y para encontrar funciones $q : S \longrightarrow Y$ y $p : Y \longrightarrow S$ que cumplan $p \circ q_j = \lambda_j$ y $q \circ \lambda_j = q_j$ para toda $j \in I$. Luego se pone a competir S consigo mismo para demostrar que $p \circ q$ es la identidad en S, y Y consigo mismo para demostrar que $q \circ p$ es la identidad en Y, por lo que p y q son isomorfismos. □

4.3. Ejercicios.

Ejercicio 168. Sea M un grupo cíclico de orden primo. Demuestre que, visto como $\mathbb{Z}$-módulo, M no puede escribirse como suma directa de submódulos no cero. Muestre que este ejercicio no es cierto para el grupo cíclico de orden seis.

Ejercicio 169. Demuestre que si M es un grupo abeliano finito no trivial, entonces M no es libre como $\mathbb{Z}$-módulo.

Ejercicio 170. Sea A el campo de los números reales. Demuestre que el único A-módulo libre numerable es el módulo cero.

Ejercicio 171. Sea A el anillo de los enteros, sea I un conjunto infinito numerable, y sea $\{M_i\}$ una familia de copias del módulo regular indexada por I. Demuestre que el producto de dicha familia es no numerable, pero que su suma directa es numerable. Concluya que este producto no es isomorfo a esta suma directa.

Capítulo 5

Representaciones matriciales de módulos finitamente generados sobre un dominio de ideales principales.

5.1. Módulos finitamente generados como cocientes de módulos libres.

Definición 172. Sean A un anillo conmutativo, r un entero positivo y M un módulo isomorfo a la suma directa de r copias del módulo regular. Decimos que M es un A-módulo libre de **rango** r. Para cada copia de A, sea e_i la respectiva copia del 1 de A, con $i = 1, \ldots, r$. A los elementos $e_1, \ldots, e_r$ se les llama la **base canónica** de M.

Lema 173. *Sea A un anillo conmutativo con un ideal maximal J. Sea M un A-módulo libre de rango r. Sea JM es submódulo de M generado por el conjunto $\{jm \mid j \in J,\ m \in M\}$. Tenemos que A/J es un campo, y M/JM es un espacio vectorial sobre A/J de dimensión r.*

Demostración: El anillo conmutativo A/J es un campo, pues para todo $a \in A$ con $a \notin J$ el ideal generado por a y J es todo A. La acción de A/J en M/JM es $(a + J) \cdot (m + JM) = am + JM$, que está bien definida. Las imágenes de la base canónica de M forman una base de M/JM. □

Corolario 174. *El rango de un módulo libre sobre un anillo conmutativo está determinado de manera única.*

Demostración: Todo anillo conmutativo con uno tiene al menos un ideal maximal por el Lema de Zorn. El resto se sigue del Lema 173. □

Teorema 175. *(Propiedad universal de los módulos libres) Sean A un anillo, M un A-módulo libre de rango r con base canónica e_i, N un A-módulo arbitrario y $n_1, \ldots, n_r$ elementos arbitrarios de N. Entonces existe un único homomorfismo de A-módulos $f : M \longrightarrow N$ tal que $f(e_i) = n_i$.*

Demostración: Note primero que el resultado es válido para el módulo regular (es decir, libre de rango uno). El resto se sigue de la Propiedad universal de la suma directa (Teorema 166). □

Corolario 176. *Sean A un anillo y M un A-módulo finitamente generado. Entonces A es isomorfo a un cociente de un A-módulo libre de rango finito.*

Demostración: Sean $m_1, \ldots, m_r$ generadores de M. Sea L un módulo libre de rango r con base canónica $e_1, \ldots, e_r$. Sea $f : L \longrightarrow M$ el único homomorfismo tal que $f(e_i) = m_i$. Como la imagen de f es un submódulo de M que contiene a los generadores de M, tenemos que f es suprayectiva. Por el Primer Teorema de Isomorfismo (Teorema 137), tenemos que M es isomorfo a un cociente de L. □

Lema 177. *Sea A un anillo arbitrario, sea M un A-módulo, y sea N un submódulo de M tal que N y M/N están finitamente generados. Entonces M está finitamente generado.*

Demostración: Sean $w_1, \ldots, w_t$ representantes tales que el conjunto $w_1 + N, \ldots, w_t + N$ genera a M/N. Sean $n_1, \ldots, n_s$ generadores de N. Entonces el conjunto $n_1, \ldots, n_s, w_1, \ldots, w_t$ genera a M, pues para todo m en M, la clase $m + N$ se genera con los $w_i + N$, por lo que m está generado por los w_i salvo por un elemento de N, que se genera con los n_j. □

Lema 178. *Sea A un anillo noetheriano, y sea M un módulo libre de rango finito. Entonces M es noetheriano.*

Demostración: Usaremos inducción sobre el rango de M. Si M es de rango uno, entonces M es isomorfo al módulo regular, que por hipótesis es noetheriano. Supongamos que el resultado es válido para módulos libres de rango r, y

sea M un módulo libre de rango $r+1$. Sea N un submódulo de M. Debemos demostrar que N está finitamente generado. Sea W el sumando directo de M isomorfo al último módulo regular en la expresión de M como suma directa de módulos regulares. Note que M/W es un módulo libre de rango r. Por el Segundo Teorema de Isomorfismo (Teorema 138), se tiene que $N/(N \cap W)$ es isomorfo a $(N+W)/W$. Este último módulo es un submódulo de M/W, y por hipótesis de inducción, $(N+W)/W$ está finitamente generado. Tenemos entonces que $N/(N \cap W)$. Además, $N \cap W$ es un submódulo de W, que es libre de rango uno, y por la base de la inducción, se sigue que $N \cap W$ está finitamente generado. El resto se sigue del Lema 177. □

Corolario 179. *Sean A un anillo noetheriano y M un A-módulo finitamente generado. Entonces A es isomorfo a un cociente de un A-módulo libre de rango finito entre un submódulo finitamente generado.*

Demostración: Se sigue del Corolario 176 y del Lema 178. □

5.2. Representación matricial.

Definición 180. Sean A un anillo noetheriano y M un A-módulo libre de rango r con base canónica $e_1, \ldots, e_r$. Sea m un elemento arbitrario de M. Entonces m puede escribirse como combinación lineal de los e_i con coeficientes en A, digamos $m = b_1e_1 + \cdots + b_re_r$. Al vector $(b_1, \ldots, b_r)$ se le llama el **vector de coordenadas** de m con respecto a la base $e_1, \ldots, e_r$. Sean $m_1, \ldots, m_t$ elementos de M, y sea N el submódulo generado por ellos. Para cada m_i, sea $(b_{i1}, \ldots, b_{ir})$ el vector de coordenadas de m_i. La matriz (b_{ij}) de t renglones y r columnas es la **representación matricial** del submódulo N.

5.3. Ejercicios.

Ejercicio 181. Sean A un anillo, M un A-módulo libre de rango r con base canónica e_i, N un A-módulo arbitrario y $n_1, \ldots, n_r$ elementos arbitrarios de N. Sea $f : M \longrightarrow N$ el único homomorfismo de A-módulos tal que $f(e_i) = n_i$. Demuestre que f está dado en los elementos de M por $f(a_1e_1 + \cdots + a_re_r) = a_1n_1 + \cdots + a_rn_r$.

Ejercicio 182. Sea M el $\mathbb{Z}$-módulo libre de rango dos (es decir, $M = \mathbb{Z} \oplus \mathbb{Z}$. Sea G un grupo abeliano de orden 10. Calcule todos los homomorfismos de $\mathbb{Z}$-módulos de M en G.

Ejercicio 183. Sea M el $\mathbb{Z}$-módulo libre de rango dos (es decir, $M = \mathbb{Z} \oplus \mathbb{Z}$. Sea N el submódulo de M generado por los vectores (2,2), (4,6) y (2,-4). Demuestre que N se puede generar con dos vectores.

Ejercicio 184. Sean M y N como en el Ejercicio 183. Demuestre que N no se puede generar con únicamente un vector.

Capítulo 6

Teorema fundamental de los módulos finitamente generados sobre un dominio de ideales principales.

6.1. Operaciones elementales de matrices.

Definición 185. Sea A un anillo conmutativo, y sea n un entero positivo. La **matriz identidad** de tamanño n, denotada I_n o simplemente I (cuando es claro en el contexto que todas las matrices son de n renglones y n columnas), es la matriz con n renglones y n columnas cuyas entradas son (a_{ij}) donde $a_{ij} = 1$ si $i = j$, y 0 si $i \neq j$. La **matriz canónica** de n renglones y n columnas de coordenadas (a, b), denotada $E^n_{a,b}$ o simplemente E_{ab}, es la matriz cuyas entradas son (a_{ij}) con $a_{ij} = 1$ si el par ordenado (i, j) es igual al par ordenado (a, b), y 0 en cualquier otro caso. Una **matriz elemental** es una matriz cuadrada que tenga alguna de las siguientes formas:

Tipo I: $I + aE_{ij}$ con algún $a \in A$;

Tipo II: $I - E_{ii} - E_{jj} + E_{ij} + E_{ji}$, con $i \neq j$;

Tipo III: $I - E_{ii} + aE_{ii}$ para alguna unidad $a \in A$.

Observación 186. Sean B una matriz con p renglones y C una matriz con p columnas. Sean X_1, X_2, X_3 matrices elementales cuadradas de tamanño p

por p, dadas por

$$\begin{aligned} X_1 &= I + aE_{ij} \\ X_2 &= I - E_{ii} - E_{jj} + E_{ij} + E_{ji} \\ X_3 &= I - E_{ii} + aE_{ii}. \end{aligned}$$

Tenemos entonces que:

- X_1B es la matriz que se obtiene de B sumándole a veces el renglón j-ésimo al renglón i-ésimo;
- X_2B es la matriz que se obtiene de B intercambiando los renglones i y j;
- X_3B es la matriz que se obtiene de la matriz B multiplicando el renglón i-ésimo por la unidad a.

Análogamente, se tiene que:

- CX_1 es la matriz que se obtiene de C sumándole a veces la columna i-ésima a la columna j-ésima;
- CX_2 es la matriz que se obtiene de C intercambiando las columnas i y j;
- CX_3 es la matriz que se obtiene de la matriz C multiplicando la columna i-ésima por la unidad a.

Las operaciones arriba mencionadas se llaman **operaciones elementales** (respectivamente de renglones y de columnas).

6.2. Forma normal de Schmidt.

Definición 187. Sea $B = (b_{ij})$ una matriz con p renglones y q columnas. Decimos que B es una matriz **diagonal** si $b_{ij} = 0$ para toda $i \neq j$.

Proposición 188. *Sean A un anillo conmutativo, M un A-módulo libre de rango r, y N un submódulo de M tal que su representación matricial es una matriz diagonal $B = (b_{ij})$. Entonces M/N es isomorfo a*

$$(A/b_{11}A) \oplus (A/b_{22}A) \oplus \ldots (A/b_{rr}A),$$

donde las b_{ii} que no existan en B se definen como cero.

Demostración: Sea W el módulo arriba mencionado. Sea $f : M \longrightarrow W$ el homomorfismo que manda a $(m_1, \ldots, m_r)$ en la r-ada de sus respectivos cocientes $(m_1 + A/b_{11}A, \ldots, m_r + A/b_{rr}A)$. Este homomorfismo es suprayectivo y su núcleo es N. Por el Primer teorema de isomorfismo (Teorema 137) se tiene que W es isomorfo a M/N. □

Definición 189. Sea B una matriz de rango r, y sea $i \leq r$. Un **menor** de i renglones de B es el determinante de una submatriz cuadrada de B que se obtiene al escoger i renglones e i columnas de B.

Definición 190. Sea $B = (b_{ij})$ una matriz no cero con p renglones y q columnas, cuyas entradas están en un dominio entero, y sea r un entero positivo. Decimos que B tiene **rango** r si existe un menor de r renglones diferente de cero, pero todo menor de $r + 1$ renglones de B es cero.

Teorema y definición 191. *Sea B una matriz con entradas en un dominio de ideales principales. Realizando operaciones elementales tanto de renglones como de columnas, es posible llevar a B a una matriz diagonal $D = (d_{ij})$ con la propiedad de que d_{ii} divide a $d_{i+1,i+1}$ para todo posible valor de i. Una tal matriz diagonal se llama una* ***forma normal de Schmidt*** *de B. A los d_{ii} diferentes de cero se les llama los* ***factores invariantes*** *de B. El número de factores invariantes es el rango de la matriz original B.*

Demostración: El último enunciado se sigue de que las operaciones elementales no cambian el rango de la matriz. Proporcionaremos un algoritmo para obtener dicha matriz diagonal.

1. Si la matriz es la matriz cero, ya terminamos. De lo contrario, sea d el máximo común divisor de todas las entradas distintas de cero. Como las entradas están en un dominio de ideales principales, d se puede escribir como una combinación lineal de las entradas de B.

2. Realizando operaciones elementales, haga que una de las entradas de la matriz sea d, y permutando renglones y columnas haga que la entrada (1,1) sea d.

3. Note que el máximo común divisor de todas las entradas de la matriz no cambia al realizar operaciones elementales, por lo que d divide a todas las entradas de la matriz. Use a la entrada (1,1) como pivote para hacer ceros en el primer renglón y la primera columna.

4. Observe que ha llegado a una matriz que tiene a d en la entrada (1,1), ceros en el resto del primer renglón y de la primera columna, y una submatriz con un renglón y una columna menos, cuyas entradas son todas múltiplos de d. Repita el procedimiento con esta submatriz.

□

Teorema 192. *Sea B una matriz de rango r con entradas en un dominio de ideales principales. Para cada $i \leq r$, sea Δ_i el máximo común divisor de los menores de i renglones de B. Sean $d_1, d-2, \ldots, d_r$ dados por $d_1 = \Delta_1$, $d_2 = \Delta_2/\Delta_1, \ldots, d_i = \Delta_i/\Delta_{i-1}, \ldots, d_r = \Delta_r/\Delta_{r-1}$. Entonces cualquier conjunto de factores invariantes de B difiere por unidades de los elementos $d_1, \ldots, d-r$.*

Demostración: Se sigue del hecho de que las operaciones elementales no cambian el determinante (salvo multiplicar por una unidad). □

Corolario 193. *Sea B una matriz con entradas en un dominio de ideales principales. Los factores invariantes de B son únicos hasta asociados. La forma normal de Schmidt de B también es única hasta asociados de los elementos de su diagonal.*

Demostración: Se sigue del Teorema 192. □

6.3. Teorema fundamental de los módulos finitamente generados sobre un dominio de ideales principales.

Proposición 194. *Sean A un anillo noetheriano, r un entero positivo, M el A-módulo libre de rango r, N un submódulo de M, y B una representación matricial de N. Sea B' una matriz obtenida a partir de B realizando un número finito de operaciones elementales de renglón. Entonces B' también es una representación matricial de N.*

Demostración: Analicemos cada tipo de operación elemental. Supongamos que los renglones de la matriz B son los vectores coordenadas de $m_1, \ldots, m_t$, los cuales son por tanto generadores de N.

Tipo I: Sumar a veces el renglón j-ésimo al renglón i-ésimo; los vectores representados por dicha matriz son $m_1, \ldots, m_{i-1}, m_i + am_j, m_{i+1}, \ldots, m_t$, los cuales generan también a N.

Tipo II: Intercambiar los renglones i y j; los generadores son los mismos, sólo que están permutados.

Tipo III: Multiplicar el renglón i-ésimo por la unidad a; los vectores representados por dicha matriz son $m_1, \ldots, m_{i-1}, am_i, m_{i+1}, \ldots, m_t$, los cuales generan también a N.

□

Lema 195. *Sean A un anillo conmutativo, r un entero positivo, M el A-módulo libre de rango r, y X una matriz con r renglones. Sea $f : M \longrightarrow M$ la función que a cada $(m_1, \ldots, m_r)$ en M lo manda al producto $(m_1, \ldots, m_r)X$. Entonces f es un homomorfismo de A-módulos. Más aún, si X es invertible, entonces f es un isomorfismo.*

Demostración: Los vectores en M se pueden ver como matrices con un renglón y r columnas. Como el producto de matrices distribuye a la suma, se tiene que f abre sumas. Además, f saca escalares porque la multiplicación por escalares conmuta con el producto de matrices, es decir, $(aY)X = a(YX)$ para a escalar y Y, X matrices. Si X es invertible, la función inversa de f se obtiene multiplicando por la izquierda por la matriz inversa de X. □

Teorema 196. *Sean A un anillo noetheriano, r un entero positivo, M el A-módulo libre de rango r, N un submódulo de M, y B una representación matricial de N. Sea B' una matriz obtenida a partir de B realizando un número finito de operaciones elementales de renglón y/o de columna, y sea N' el módulo generado por los renglones de B'. Entonces M/N es isomorfo a M/N'.*

Demostración: Por la Proposición 194, basta considerar el caso cuando se realiza una operación elemental de columna, digamos que la representada por la matriz elemental X, que es invertible. Por el Lema 195, se tiene un isomorfismo $f : M \longrightarrow M$ dado por multiplicación izquierda por la matriz elemental X. Como los renglones de B' se obtienen a partir de los renglones de B multiplicando por X por la izquierda, se sigue que $f(N) = N'$. Sea $\pi : M \longrightarrow M/N'$ la proyección al cociente. Tenemos que la composición $\pi \circ f : M \longrightarrow M/N'$ es suprayectiva y su núcleo es N; por el Primer teorema de isomorfismo (Teorema 137), se sigue que M/N es isomorfo a M/N'. □

Notación 197. Sean A un anillo, M un A-módulo y m un entero no negativo. Denotamos por M^m a la suma directa externa de m copias de M. En particular, A^m denota al A-módulo libre de rango r. Por convención, M^0 es el módulo cero.

Teorema 198. *(Teorema fundamental de los módulos finitamente generados sobre un dominio de ideales principales) Sea A un dominio de ideales principales, y sea M un A-módulo finitamente generado. Entonces existen elementos $d_1, \ldots, d_r$ en A y un entero no negativo m tales que d_i divide a d_{i+1} para $i = 1, \ldots, r-1$ y M es isomorfo a*

$$(A/d_1A) \oplus (A/d_2A) \oplus \ldots (A/d_rA) \oplus A^m.$$

Demostración: Por el Corolario 179, existen un A-módulo libre L de rango finito t y un submódulo N de L tales que L/N es isomorfo a M. Sea B la representación matricial de N, sea B' una forma normal de Schmidt de B, y sea N' el submódulo de L representado por B'. Por el Teorema 196, L/N es isomorfo a L/N', por lo que este último módulo es isomorfo a M. El resto se sigue de la Proposición 188. □

6.4. Ejercicios.

Ejercicio 199. Considere la siguiente matriz sobre los enteros:

$$\mathbf{B} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 200. Considere la siguiente matriz sobre los enteros:

$$\mathbf{B} = \begin{pmatrix} -3 & 2 \\ 7 & 12 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 201. Considere la siguiente matriz sobre $\mathbb{R}[x]$:

$$\mathbf{B} = \begin{pmatrix} x-1 & 1 \\ 7 & x-2 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 202. Considere la siguiente matriz sobre $\mathbb{R}[x]$:

$$\mathbf{B} = \begin{pmatrix} x-3 & 2 \\ 9 & x-5 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 203. Considere la siguiente matriz sobre los enteros:

$$\mathbf{B} = \begin{pmatrix} 4 & 0 \\ 0 & 6 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 204. Considere la siguiente matriz sobre los enteros:

$$\mathbf{B} = \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 205. Considere la siguiente matriz sobre los enteros:

$$\mathbf{B} = \begin{pmatrix} 0 & 0 \\ 3 & 4 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 206. Considere la siguiente matriz sobre un dominio de ideales principales arbitrario:

$$\mathbf{B} = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$$

Demuestre que su forma normal de Schmidt es de la forma

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

donde a es el máximo común divisor de x y y, y b es el mínimo común múltiplo de a y b. (Sugerencia: use el hecho de que a se puede escribir como una combinación lineal de x y y, y que $ab = xy$.)

Ejercicio 207. Considere la siguiente matriz sobre los enteros:

$$\mathbf{B} = \begin{pmatrix} 1 & 7 \\ 3 & 2 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 208. Considere la siguiente matriz sobre un dominio de ideales principales arbitrario:

$$\mathbf{B} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

Demuestre que su forma normal de Schmidt es de la forma

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

donde a es el máximo común divisor de las cuatro entradas de B, y b es el determinante de B dividido entre a.

Ejercicio 209. Considere la siguiente matriz sobre $\mathbb{R}[x]$:

$$\mathbf{B} = \begin{pmatrix} x-3 & (x-3)^2(x-5)^3 \\ 0 & x-5 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 210. Considere la siguiente matriz sobre los enteros:

$$\mathbf{B} = \begin{pmatrix} 1 & 7 & 2 \\ 3 & 2 & -4 \\ 0 & 1 & -1 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 211. Considere la siguiente matriz sobre los enteros:

$$\mathbf{B} = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 15 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 212. Considere la siguiente matriz sobre $\mathbb{R}[x]$:

$$\mathbf{B} = \begin{pmatrix} x-1 & 1 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & x-2 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 213. Considere la siguiente matriz sobre $\mathbb{R}[x]$:

$$\mathbf{B} = \begin{pmatrix} x-1 & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & x-2 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 214. Considere la siguiente matriz sobre $\mathbb{R}[x]$:

$$\mathbf{B} = \begin{pmatrix} x-1 & 3 & -2 \\ -1 & x-1 & 4 \\ -5 & -7 & x-2 \end{pmatrix}$$

Calcule su forma normal de Schmidt.

Ejercicio 215. Sea M el grupo abeliano cociente dado por

$$\frac{\mathbb{Z}^2}{< (1,3), (2,4) >}$$

Calcule una descomposición de M como suma directa de grupos cíclicos.

Ejercicio 216. Sea M el grupo abeliano cociente dado por

$$\frac{\mathbb{Z}^2}{< (2,6) >}$$

Calcule una descomposición de M como suma directa de grupos cíclicos.

Ejercicio 217. Sea M el grupo abeliano cociente dado por

$$\frac{\mathbb{Z}^2}{< (2,4), (-4,4), (2,6) >}$$

Calcule una descomposición de M como suma directa de grupos cíclicos.

Ejercicio 218. Sea M el grupo abeliano cociente dado por

$$\frac{\mathbb{Z}^3}{< (2,1,4), (-1,2,4), (3,5,6) >}$$

Calcule una descomposición de M como suma directa de grupos cíclicos.

Ejercicio 219. Sea M el grupo abeliano cociente dado por

$$\frac{\mathbb{Z}^3}{< (2,1,4), (-1,2,4), (3,5,6), (2,0,8) >}$$

Calcule una descomposición de M como suma directa de grupos cíclicos.

Ejercicio 220. Sea M el grupo abeliano cociente dado por

$$\frac{\mathbb{Z}^3}{< (2,9,10), (0,3,-6), (0,0,6) >}$$

Calcule una descomposición cualquiera de M como suma directa de grupos cíclicos. Calcule la descomposición de M según el Teorema 198.

Capítulo 7

Aplicaciones.

7.1. Grupos abelianos finitamente generados.

Lema 221. *Sean a, b enteros, y sean d y m su máximo común divisor y mínimo común múltiplo respectivamente. Entonces*

$$(\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z}) \cong (\mathbb{Z}/d\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$$

Demostración: El primer módulo es isomorfo al cociente de $\mathbb{Z}^2$ por el submódulo cuya representación matricial es

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

La forma normal de Schmidt de esta matriz es

$$\begin{pmatrix} d & 0 \\ 0 & m \end{pmatrix}$$

cuyo cociente asociado es el segundo módulo. □

Corolario 222. *Sea a un entero mayor que 1, y sea $a = p_1^{e_1} \dots p_n^{e_n}$ una factorización de a en primos distintos. Entonces*

$$(\mathbb{Z}/a\mathbb{Z}) \cong \oplus_{i=1}^{n} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})$$

Demostración: Es una aplicación iterada del Lema 221 a las potencias de los primos, que son primos relativos. □

Lema 223. *Sean A, A' grupos abelianos finitos y L, L' grupos abelianos libres tales que $A \oplus L \cong A' \oplus L'$. Entonces $A \cong A'$ y $L \cong L'$.*

Demostración: Sea f un isomorfismo de $A \oplus L$ en $A' \oplus L'$. Tenemos que A es el mayor subgrupo finito de $A \oplus L$, es decir, es un subgrupo finito de $A \oplus L$ que contiene a cualquier otro subgrupo finito de $A \oplus L$, por lo que f lo manda a un subgrupo finito de $A' \oplus L'$ con la misma propiedad, que debe por fuerza ser A'. Además, el homomorfismo f induce un isomorfismo entre los cocientes $L \cong (A \oplus L)/A \cong (A' \oplus L')/f(A) = (A' \oplus L')/A' \cong L'$. □

Teorema 224. *(Teorema fundamental de los grupos abelianos finitamente generados) Todo grupo abeliano finitamente generado es una suma directa de un grupo finito (llamado su **subgrupo de torsión**) y un grupo libre. Tanto el grupo de torsión como el rango de la componente libre son invariantes, es decir, el rango de la componente libre es único, y el grupo de torsión es único hasta isomorfismo. Todo grupo abeliano finito es una suma directa de grupos cíclicos cuyos órdenes son potencias de primos. Estos órdenes junto con sus multiplicidades están determinados de manera única y constituyen un conjunto completo de invariantes en cuanto a que dos grupos abelianos finitos son isomorfos si y sólo si tienen el mismo conjunto de estos invariantes.*

Demostración: Sea M un grupo abeliano finitamente generado. Por el Teorema fundamental de los módulos finitamente generados sobre un dominio de ideales principales (Teorema 198), tenemos que M es isomorfo a una suma directa de la forma

$$(\mathbb{Z}/d_1\mathbb{Z}) \oplus (\mathbb{Z}/d_2\mathbb{Z}) \oplus \ldots (\mathbb{Z}/d_r\mathbb{Z}) \oplus \mathbb{Z}^m$$

donde los d_i son enteros diferentes de cero. La suma de los $(\mathbb{Z}/d_i\mathbb{Z})$ con $i = 1, \ldots, r$ es un grupo abeliano finito, y $\mathbb{Z}^m$ es un grupo libre. Por el Lema 223, ambos son invariantes. Por el Corolario 222, cada grupo cíclico $\mathbb{Z}/d_i\mathbb{Z}$ es isomorfo a una suma directa de grupos cíclicos cuyos órdenes son potencias de primos, por lo que dicha propiedad se transfiere a cualquier grupo abeliano finito (pues son sumas directas de grupos cíclicos). La última parte se sigue del hecho de que las potencias de primos que aparecen son precisamente las que dividen a los d_i, y que los d_i son únicos hasta asociados. □

7.2. Descomposición de $k[x]$-módulos.

Notación 225. Sean k un campo, V un k-espacio vectorial, $(u_1, \ldots, u_n)$ base de V sobre k, $T\colon V \longrightarrow V$ una transformación lineal, $T(u_i) = \sum_{j=1}^{n} a_{ij}u_j$, $i = 1, \ldots, n$. Sea $A^t = (a_ij)^t = (a_{ji})$ la matriz de T con respecto a la base $(u_1, \ldots, u_n)$. Recuerde la definición del $k[x]$-módulo $V(T)$ dada en el Ejemplo 121, es decir, la acción de $k[x]$ en V está dada por $(b_0+b_1x+\cdots+b_mxm)\cdot v = b_0v + b_1T(v) + \cdots + b_mT^m(v)$.

Teorema 226. *Como $k[x]$-módulo, $V(T)$ es isomorfo al módulo cociente $k[x]^n/ < f_1, \ldots, f_n >$, donde la representación matricial de $f_1, \ldots, f_n$ es*

$$xI - A = \begin{pmatrix} x - a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & x - a_{22} & \ldots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \ldots & x - a_{nn} \end{pmatrix}$$

Demostración: Sea $\eta : k[x] \longrightarrow V$ dada por $(p_1(x), \ldots, p_n(x)) \mapsto p_1(x) \cdot u_1 + p_2(x) \cdot u_2 + \cdots + p_n(x) \cdot u_n$. Tenemos que η es un homomorfismo de $k[x]$-mdóulos izquierdos, cuya imagen es V. Por el Primer Teorema de Isomorfismo (Teorema 137), basta demostrar que el núcleo de η es el submódulo generado por $f_1, \ldots, f_n$. Note primero que

$$\begin{aligned} \eta(f_i) &= \eta(-a_{i1}, -a_{i2}, \ldots, x - a_{ii}, \ldots, -a_{in}) \\ &= -a_{i1}u_1 - a_{i2}u_2 \cdots + (x - a_{ii})u_i - \cdots - a_{in}u_n \\ &= xu_i - \sum_{j=1}^{n} a_{ij}u_j \\ &= T(u_i) - \sum_{j=1}^{n} a_{ij}u_j \\ &= 0 \end{aligned}$$

por definición de los a_{ij}. Por tanto, tenemos que el núcleo de η contiene al submódulo generado por las f_i. Sea ahora $(p_1(x), \ldots, p_n(x))$ un elemento del núcleo de η. Debemos demostrar que este elemento está generado por las f_i.

Observe primero que

$$\begin{aligned}(x,0,0,\ldots,0) &= f_1 + (a_{11},a_{12},\ldots,a_{1n})\\ (0,x,0,\ldots,0) &= f_2 + (a_{21},a_{22},\ldots,a_{2n})\\ \vdots &= \vdots\\ (0,0,\ldots,0,x) &= f_n + (a_{n1},a_{n2},\ldots,a_{nn})\end{aligned}$$

Tenemos entonces que

$$\begin{aligned}(p_1(x),0,0,\ldots,0) &= \frac{p_1(x)-p_1(0)}{x}(x,0,0,\ldots,0) + (p_1(0),0,0,\ldots,0) =\\ &= q_1(x)f_1(x) + c_1\\ \vdots &= \vdots\\ (0,0,\ldots,0,p_n(x)) &= \frac{p_n(x)-p_n(0)}{x}(0,0,\ldots,0,x) + (0,0,\ldots,0,p_n(0)) =\\ &= q_n(x)f_n(x) + c_n\end{aligned}$$

donde cada c_i es un vector cuyas entradas son constantes. Así, tenemos que

$$(p_1(x),p_2(x),\ldots,p_n(x)) = \sum_{i=1}^{n} q_i f_i + C$$

donde $C = (d_1,d_2,\ldots,d_n)$ es un vector cuyas entradas son constantes. Resta demostrar que $d_i = 0$ para toda $i = 1,\ldots,n$. Aplicando η a la ecuación anterior obtenemos

$$\begin{aligned}0 &= \eta((p_1(x),p_2(x),\ldots,p_n(x)))\\ &= \eta\left(\sum_{i=1}^{n} q_i f_i + C\right)\\ &= \sum_{i=1}^{n} q_i\eta(f_i) + \eta(C)\\ &= 0 + \eta((d_1,d_2,\ldots,d_n))\\ &= d_1u_1 + d_2u_2 + \cdots + d_nu_n\end{aligned}$$

Como las u_i son una base de V, tenemos que $d_i = 0$ para toda $i = 1,\ldots,n$. □

Definición 227. El determinante de la matriz $xI - A$ se llama el **polinomio característico** de A. Las raíces en el campo k de este polinomio se llaman los **valores propios** de la matriz A.

Observación 228. Algunas veces uno se refiere a los *"factores invariantes de A"* cuando en realidad quiere decir los *"factores invariantes de $xI - A$"*.

Lema 229. *El polinomio característico de A es un polinomio mónico de grado n, y es el producto de los factores invariantes de $xI - A$ (hasta asociados). Todos los factores invariantes de $xI - A$ son diferentes de cero, y por tanto pueden elegirse como polinomios mónicos. La forma normal de Schmid para $xI - A$ se ve*

$$\begin{pmatrix} 1 & 0 & 0 & \dots & & & & \\ 0 & 1 & 0 & \dots & & & & \\ 0 & 0 & \ddots & & & & & \\ \vdots & & & d_1(x) & & & & \\ & & & & d_2(x) & & & \\ & & & & & \ddots & & \\ & & & & & & d_s(x) & \end{pmatrix}$$

*donde los $d_i(x)$ son polinomios mónicos no constantes y $d_i(x)$ divide a $d_{i+1}(x)$ para toda $i = 1, \dots, s-1$. El polinomio $d_s(x)$ (es decir, el último factor invariante de la matriz $xI - A$) se llama el **polinomio mínimo** de la matriz A.*

Demostración: En el determinante, el único polinomio de grado n que aparece es cuando se multiplican todos los $x - a_{ii}$. En general, el determinante siempre es el producto de los factores invariantes (hasta asociados), y como el determinante en este caso es un polinomio no nulo, ninguno de los factores invariantes puede ser cero. La forma normal de Schmidt se sigue de este hecho (note que pueden no aparecer unos en la diagonal). □

Corolario 230. *Sean $d_1(x), \dots, d_s(x)$ los factores invariantes no constantes de $xI - A$. Tenemos que como $k[x]$-módulos, $V(T)$ es isomorfo a*

$$\frac{k[x]}{< d_1(x) >} \oplus \frac{k[x]}{< d_2(x) >} \oplus \dots \oplus \frac{k[x]}{< d_s(x) >}$$

Demostración: Se sigue del Teorema 226, del Lema 229, y del Teorema 196. □

Definición 231. Sean k un campo, n un entero positivo, A y B matrices de n por n. Decimos que A es **conjugada** a B (o **similar** a B según otros autores) si existe una matriz invertible P de n por n tal que $A = PBP^{-1}$.

Observación 232. La relación "ser conjugada a" es una relación de equivalencia (véase el Ejercicio 259). Así, en lugar de decir que A es conjugada a B, a veces simplemente decimos que A y B son conjugadas.

Proposición 233. *Sean V, W espacios vectoriales sobre k, T y U transformaciones lineales de V en V y de W en W respectivamente. Sean α y β bases de V y W respectivamente, y sean A y B matrices que representan a T y U es estas bases. Entonces $V(T)$ y $W(U)$ son isomorfos como $k[x]$-módulos si y sólo si A y B son matrices conjugadas.*

Demostración: Recordemos (Ejemplo 136) que un homomorfismo de $V(T)$ en $W(U)$ es una transformación lineal $f : V \longrightarrow W$ tal que $f \circ T = U \circ f$. Este homomorfismo es un isomorfismo de $k[x]$-módulos si y sólo si f es además un isomorfismo de k-espacios vectoriales. Supongamos que existe tal f isomorfismo, y sea Q la matriz de f con respecto a las bases α en V y β en W. De la igualdad $f \circ T = U \circ f$ se sigue que $QA = BQ$, por lo que $B = QAQ^{-1}$, es decir, A y B son matrices conjugadas. Inversamente, si Q es una matriz invertible tal que $B = QAQ^{-1}$, se sigue que $QA = BQ$. Sea $f : V \longrightarrow W$ la transformación lineal cuya matriz en las bases α y β es Q. Tenemos que $f \circ T = U \circ f$, y como Q es invertible, f es un isomorfismo. □

Proposición 234. *Sean $V_i(T_i)$ $k[x]$-módulos tales que $V(T) = \oplus_{i=1}^{n} V_i(T_i)$. Sean α_i bases de los V_i, y sean A_i las matrices de los T_i con respecto a estas bases. Sea α la base de V obtenida al juntar $\alpha_1, \alpha_2, \ldots, \alpha_n$, y sea A la matriz de T con respecto a la base α. Entonces*

$$\mathbf{A} = \begin{pmatrix} A_1 & 0 & 0 & \ldots & & \\ 0 & A_2 & 0 & \ldots & & \\ 0 & 0 & \ddots & & & \\ \vdots & & & & A_{n-1} & \\ & & & & & A_n \end{pmatrix}$$

Es decir, la matriz A se obtiene colocando los bloques A_i diagonalmente y rellenando las demás entradas con ceros.

Demostración: Se sigue de que la transformación lineal T se restringe a cada V_i como T_i. □

Teorema 235. *Sean k un campo, V un k-espacio vectorial, $(u_1, \ldots, u_n)$ base de V sobre k, $T\colon V \longrightarrow V$ una transformación lineal, $T(u_i) = \sum_{j=1}^{n} a_{ij}u_j$, $i = 1, \ldots, n$. Sea $A^t = (a_i j)^t = (a_{ji})$ la matriz de T con respecto a la base $(u_1, \ldots, u_n)$, y sean $d_1(x), \ldots, d_s(x)$ los factores invariantes no constantes de la matriz $xI - A$. Sean $V_i(T_i)$ tales que $V_i(T_i) \cong k[x]/ < d_i(x) >$ para toda $i = 1, \ldots, s$. Sean A_i matrices que representan a las T_i con respecto a algunas bases, y sea B la matriz que se obtiene alineando a los bloque A_i por la diagonal y rellenando las demás entradas con ceros. Entonces A y B son matrices conjugadas.*

Demostración: Por el Corolario 230, el $k[x]$-módulo $V(T)$ es isomorfo a la suma directa de los $V_i(T_i)$. Por la Proposición 234, a esta suma directa le corresponde la matriz B. Por la Proposición 233, A y B son matrices conjugadas. □

7.3. Forma canónica racional.

Definición 236. Sea $d(x)$ un polinomio mónico de grado $m > 0$ en $k[x]$, digamos

$$d(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

La **matriz compañera** de $d(x)$ es la matriz C de m por m dada por

$$\mathbf{C} = \begin{pmatrix} 0 & 0 & 0 & \ldots & & -b_0 \\ 1 & 0 & 0 & \ldots & & -b_1 \\ 0 & 1 & 0 & \ldots & & -b_2 \\ \vdots & & & & & \vdots \\ 0 & & & 0 & 1 & -b_{m-1} \end{pmatrix}$$

Es decir, la entrada c_{ij} de C es 1 si $i = j + 1$, $-b_{i-1}$ si $j = m$, y cero en cualquier otro caso.

Observación 237. Algunos autores definen a la matriz compañera de $d(x)$ como la transpuesta de la matriz dada en la Definición 236.

Observación 238. Sea $d(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$, y sea C la matriz compañera de $d(x)$. Sea $e_1, \ldots, e_m$ la base canónica de k^m. Entonces $Ce_1 = e_2$; $Ce_2 = e_3$; $Ce_3 = e_4$ $\ldots$ $Ce_{m-1} = e_m$; $Ce_m = -b_0e_1 - b_1e_2 - \cdots - b_{m-1}e_m$.

Ejemplo 239. La matriz compañera del polinomio mónico $x^3 - 5x^2 + 7x + 8$ es

$$\begin{pmatrix} 0 & 0 & -8 \\ 1 & 0 & -7 \\ 0 & 1 & 5 \end{pmatrix}$$

Proposición 240. *Sea $d(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$ un polinomio mónico en $k[x]$ de grado $m > 0$, y sea C la matriz compañera de $d(x)$. Sea $V = k^m$, y sea $T : V \longrightarrow V$ la transformación lineal que en la base canónica está representada por la matriz C. Entonces $V(T)$ es isomorfo a $k[x]/ < d(x) >$ como $k[x]$-módulos.*

Demostración: Sea $e_1, \ldots, e_m$ la base canónica de V. Sea $f : k[x] \longrightarrow V$ dada por $f(p(x)) = p(x) \cdot e_1$, donde esta última expresión representa la acción del polinomio $p(x)$ en e_1. Note que $f(1) = 1 \cdot e_1 = e_1$, que $f(x) = x \cdot e_1 = Ce_1 = e_2$, que $f(x^2) = C^2e_1 = C(Ce_1) = Ce_2 = e_3$, y que $f(x^{m-1}) = e_m$, por lo que f es suprayectiva. Por el Primer teorema de isomorfismo (Teorema 137), basta demostrar que el núcleo de f es el submódulo de $k[x]$ generado por $d(x)$. Tenemos que $f(d(x)) = d(x) \cdot e_1 = b_0e_1 + b_1x \cdot e_1 + \cdots + b_{m-1}x^{m-1} \cdot e_1 + x^m \cdot e_1 = b_0e_1 + b_1Ce_1 + \cdots + b_{m-1}C^{m-1}e_1 + C^me_1 = b_0e_1 + b_1e_2 + b_2e_3 + \cdots + b_{m-1}e_m + Ce_m = 0$, por lo que el núcleo de f contiene al submódulo $< d(x) >$. Inversamente, sea $g(x)$ un elemento del núcleo de f, y escribamos $g(x) = q(x)d(x) + r(x)$. Tenemos que demostrar qur $r(x)$ es el polinomio cero. Supongamos que $r(x)$ no es el polinomio cero, sino un polinomio de grado estrictamente menor que el grado de $d(x)$, digamos $r(x) = r_0 + r_1x + \cdots + r_tx^t$ con $t < m$. Como $< d(x) >$ está en el núcleo de f, tenemos que $r(x)$ también está en el núcleo, por lo que $0 = r(x) \cdot e_1 = r_0e_1 + r_1e_2 + \cdots + r_te_{t+1}$. Pero los e_i son linealmente independientes, por lo que $r_i = 0$ para toda i, contradiciendo el hecho de que $r(x)$ no fuera cero. □

Teorema y definición 241. *Sea A una matriz cuadrada con entradas en un campo k. Sean $d_1(x), \ldots, d_s(x)$ los factores invariantes mónicos no constantes de la matriz $xI - A$, y sean $A_1, \ldots, A_s$ las matrices compañeras de los $d_1(x), \ldots, d_s(x)$ respectivamente. Sea B la matriz cuadrada que se obtiene*

alineando los bloques A_i a lo largo de la diagonal y rellenando con ceros los lugares restantes, es decir

$$\mathbf{B} = \begin{pmatrix} A_1 & 0 & 0 & \dots & & \\ 0 & A_2 & 0 & \dots & & \\ 0 & 0 & \ddots & & & \\ \vdots & & & & A_{s-1} & \\ & & & & & A_s \end{pmatrix}$$

Entonces A y B son matrices conjugadas. A la matriz B se le llama la ***forma canónica racional*** *de la matriz A.*

Demostración: Sea $d_i(x)$ un factor invariante cualquiera de $xI - A$ de grado m_i. Por la Proposición 240, $k[x]/ < d_i(x) >$ es isomorfo a un $V_i(T_i)$ donde $V_i = k^{m_i}$ y T_i es la transformación lineal de V_i en V_i cuya matriz con respecto a la base canónica de V_i es A_i. Por el Teorema 235 tenemos que A y B son matrices conjugadas. □

Observación 242. Si se pide que los bloques aparezcan en el orden en que sugieron los factores invariantes, la matriz B es única.

7.4. Forma canónica de Jordan.

Definición 243. Sean a un escalar en k y m un entero positivo. El **bloque de Jordan** de tamaño m con valor propio α es la matriz $J_m(\alpha)$ de m por m dada por

$$\mathbf{C} = \begin{pmatrix} \alpha & 1 & 0 & \dots & & & 0 \\ 0 & \alpha & 1 & 0 & \dots & & 0 \\ 0 & 0 & \alpha & 1 & 0 & \dots & 0 \\ \vdots & & & \ddots & & \ddots & \vdots \\ 0 & 0 & & \dots & & \alpha & 1 \\ 0 & 0 & & \dots & & 0 & \alpha \end{pmatrix}$$

Es decir, la entrada (i, j) de $J_m(\alpha)$ es 1 si $j = i + 1$, α si $j = i$, y cero en cualquier otro caso.

Observación 244. Algunos autores definen al bloque de Jordan $J_m(\alpha)$ como la transpuesta de la matriz dada en la Definición 243.

Observación 245. Sea C el bloque de Jordan de tamaño m con valor propio α. Sea $e_1, \ldots, e_m$ la base canónica de k^m. Entonces $Ce_1 = \alpha e_1$; $Ce_2 = \alpha e_2 + e_1$; $Ce_3 = \alpha e_3 + e_2$ $\ldots$ $Ce_{m-1} = \alpha e_{m-1} + e_{m-2}$; $Ce_m = \alpha e_m + e_{m-1}$. Se sigue que $(C - \alpha I)e_m = e_{m-1}$; $(C - \alpha I)^2 e_m = (C - \alpha I)e_{m-1} = e_{m-2}; \ldots; (C - \alpha I)^{m-1} e_m = e_1; (C - \alpha I)^m e_m = (C - \alpha I)e_1 = 0$.

Ejemplo 246. El bloque de Jordan de tamaño 3 con valor propio -2 es

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

Proposición 247. *Sea $C = J_m(\alpha)$ el bloque de Jordan de tamaño m con valor propio α. Sea $V = k^m$, y sea $T : V \longrightarrow V$ la transformación lineal que en la base canónica está representada por la matriz C. Entonces $V(T)$ es isomorfo a $k[x]/ < (x - \alpha)^m >$ como $k[x]$-módulos.*

Demostración: Sea $f : k[x] \longrightarrow V(T)$ dada por $f(p(x)) = p(x) \cdot e_m$. Tenemos que f es un homomorfismo de $k[x]$-módulos. Por la Observación 245, f es suprayectiva. Por el Primer teorema de isomorfismo (Teorema 137) basta demostrar que el núcleo de f es el submódulo $< (x-\alpha)^m >$. Como $V(T)$ tiene dimensión m, se sigue que el núcleo de f tiene codimensión m en $k[x]$, que es la misma codimensión que tiene $< (x - \alpha)^m >$, por lo que basta demostrar que $(x-\alpha)^m$ está en el núcleo de f. Otra vez por la Observación 245 se tiene $f((x - \alpha)^m) = (x - \alpha)^m e_m = 0$. □

Lema 248. *Sea D un dominio de ideales principales, y sean $\alpha_1, \ldots, \alpha_t \in D$ primos relativos dos a dos en D. Entonces*

$$D/ < \alpha_1 \alpha_2 ... \alpha_t > \cong \oplus_{i=1}^t D/ < \alpha_i > .$$

Demostración: Empiece con el módulo $\oplus_{i=1}^t D/ < \alpha_i >$. Considere la representación matricial diagonal que lo origina. Observe que la forma normal de Schmid de dicha representación consta de unos en la diagonal y una única entrada diferente de uno, a saber, $\alpha_1, \ldots, \alpha_t$. □

Corolario 249. *Sea $d(x)$ un polinomio que se factoriza totalmente en $k[x]$, digamos $d(x) = (x - \alpha_1)^{m_1} \ldots (x - \alpha_t)^{m_t}$. Entonces*

$$k[x]/ < d(x) > \cong \oplus_{i=1}^t k[x]/ < (x - \alpha_i)^{m_i}.$$

Demostración: Es un caso particular del Lema 248 para el dominio de ideales principales $k[x]$. □

Corolario 250. *Sea $d(x)$ un polinomio que se factoriza totalmente en $k[x]$, digamos $d(x) = (x-\alpha_1)^{m_1}\dots(x-\alpha_t)^{m_t}$. Sea B la matriz que se obtiene alineando los bloques de Jordan $J_{m_i}(\alpha_i)$ para $i = 1,\dots,t$ por la diagonal y rellenando las demás entradas con ceros. Sea T la transformación lineal asociada a la matriz B, y sea V el dominio de T. Entonces $V(T)$ es isomorfo a $k[x]/ < d(x) >$ como $k[x]$-módulos.*

Demostración: Se sigue del Corolario 249 y la Proposición 247. □

Teorema y definición 251. *Sea A una matriz cuadrada con entradas en un campo k. Sean $d_1(x),\dots,d_s(x)$ los factores invariantes mónicos no constantes de la matriz $xI - A$, y supongamos que todos ellos se factorizan totalmente sobre k, digamos $d_i(x) = (x-\alpha_{i1})^m_{i1}\dots(x-\alpha_{it_i})^m_{it_i}$. Sea B la matriz cuadrada que se obtiene alineando todos los posibles bloques de Jordan $J_{m_{ij}}(\alpha_{ij})$ a lo largo de la diagonal (en cualquier orden) y rellenando con ceros los lugares restantes. Entonces A y B son matrices conjugadas. A la matriz B se le llama la* ***forma canónica de Jordan*** *de la matriz A. Esta matriz es única excepto por el orden de los bloques de Jordan a lo largo de la diagonal.*

Demostración: Sea T la transformación lineal dada por la matriz A. Sea $d_i(x)$ un factor invariante cualquiera de $xI - A$ de grado m_i. Sea A_i la matriz que se obtiene alineando los bloques de Jordan $J_{m_{ij}}(\alpha_{ij})$ fijando la i y dejando variar la $j = 1,\dots,m_{it_i}$. sean T_i la transformación lineal determinada por la matriz A_i, y sea V_i el dominio de $T - i$. Por el Corolario 250, $k[x]/ < d_i(x) >$ es isomorfo a $V_i(T_i)$. Sea B la matriz que se obtiene alineando los bloques A_i por la diagonal y rellenando con ceros los demás lugares. Por el Teorema 235 tenemos que A y B son matrices conjugadas. La unicidad de la matriz B (hasta permutación de los bloques de Jordan) se sigue de que los bloques de Jordan determinan (las factorizaciones de) los factores invariantes de la matriz $xI - A$. □

7.5. Ejercicios.

Ejercicio 252. Para cada uno de los siguientes cocientes de $\mathbb{Z}^n$, descompónga-lo como suma directa de un grupo finito y un grupo libre. Calcule el rango de la componente libre. Calcule la descomposición de la componente de torsión como suma directa de grupos cíclicos cuyos órdenes son potencias de primos.

- $$\frac{\mathbb{Z}^2}{<(1,3),(2,4)>}$$
- $$\frac{\mathbb{Z}^2}{<(2,6)>}$$
- $$\frac{\mathbb{Z}^2}{<(2,4),(-4,4),(2,6)>}$$
- $$\frac{\mathbb{Z}^3}{<(2,1,4),(-1,2,4),(3,5,6)>}$$
- $$\frac{\mathbb{Z}^3}{<(2,1,4),(-1,2,4),(3,5,6),(2,0,8)>}$$
- $$\frac{\mathbb{Z}^3}{<(2,9,10),(0,3,-6),(0,0,6)>}$$

Ejercicio 253. Calcule el número de grupos abelianos no isomorfos de los siguientes órdenes:

- 8
- 11
- 12
- 16
- 18
- 25
- 180

Ejercicio 254. Calcule la matriz compañera de cada uno de los siguientes polinomios mónicos:

- $x^3 + 5x^2 - 4x + 2$

- $x^2 - 7x + 1$
- $x^3 - 3x + 8$
- x^3
- $x^3 + 1$
- $(x-1)^2(x+2)$

Ejercicio 255. Calcule los bloques de Jordan de cada una de las siguientes potencias:

- $(x-1)^2$
- $(x-1)^3$
- $(x+1)^3$
- $x - 2$
- x^2
- x
- $(x+3)^5$

Ejercicio 256. Para cada una de las siguientes matrices sobre $\mathbb{C}$ (el campo de los número complejos), calcule su polinomio característico, su polinomio mínimo, sus valores propios, sus factores invariantes, su forma canónica racional, y su forma canónica de Jordan.

- $$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
- $$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
- $$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

- $$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
- $$\begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 8 \\ 0 & 5 \end{pmatrix}$$
- $$\begin{pmatrix} 4 & 7 \\ 0 & -5 \end{pmatrix}$$
- $$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

(dar la respuesta por casos)

- $$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$
- $$\begin{pmatrix} -11 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$
- $$\begin{pmatrix} 6 & 7 & 2 \\ 0 & 6 & -4 \\ 0 & 0 & -1 \end{pmatrix}$$
- $$\begin{pmatrix} 6 & 7 & 2 \\ 0 & 6 & -4 \\ 0 & 0 & 6 \end{pmatrix}$$

- $$\begin{pmatrix} 6 & 7 & 2 \\ 0 & 5 & -4 \\ 0 & 0 & 6 \end{pmatrix}$$

Ejercicio 257. Para cada uno de los siguientes conjuntos de factores invariantes, determinar el polinomio característico, el polinomio mínimo, los valores propios, y la forma canónica de Jordan de la matriz original: (nota: se omiten los factores invariantes constantes)

- $d_1(x) = (x-1)(x-5)^2$; $d_2(x) = (x-1)^2(x-5)^3$; $d_3(x) = (x-1)^2(x-5)^4(x+4)^2$
- $d_1(x) = (x+1)(x-1)$; $d_2(x) = (x+1)^3(x-1)^2(x+2)$; $d_3(x) = (x+1)^3(x-1)^2(x+2)$
- $d_1(x) = x+4$; $d_2(x) = x+4$; $d_3(x) = x+4$
- $d_1(x) = x+4$; $d_2(x) = (x+4)^2$; $d_3(x) = (x+4)^3$
- $d_1(x) = x^2$; $d_2(x) = x^3$
- $d_1(x) = x(x+1)(x-2)$
- $d_1(x) = x(x+1)^2(x-2)^2$
- $d_1(x) = x^5(x+1)^2(x-2)$
- $d_1(x) = x(x+1)(x-2)$; $d_2(x) = x(x+1)^2(x-2)^3$

Ejercicio 258. Para cada una de las siguientes formas canónicas de Jordan, determinar los factores invariantes, el polinomio característico, el polinomio mínimo y los valores propios de la matriz original:

- $$\begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}$$
- $$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

- $$\begin{pmatrix} 6 & 1 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$
- $$\begin{pmatrix} 6 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$
- $$\begin{pmatrix} 6 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & -4 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 1 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & -4 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & -4 & 1 \\ 0 & 0 & 0 & -4 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 1 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & -4 & 1 \\ 0 & 0 & 0 & -4 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 1 & 0 & 0 \\ 0 & 5 & 1 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & -4 \end{pmatrix}$$

- $$\begin{pmatrix} 5 & 1 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 5 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 5 \end{pmatrix}$$
- $$\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$$

En las siguientes matrices, se indican sólo los bloques de Jordan (las demás entradas son cero):

- $$\begin{pmatrix} J_2(1) & & & \\ & J_3(1) & & \\ & & J_2(1) & \\ & & & J_2(1) \end{pmatrix}$$
- $$\begin{pmatrix} J_2(0) & & & \\ & J_3(0) & & \\ & & J_2(1) & \\ & & & J_2(2) \end{pmatrix}$$
- $$\begin{pmatrix} J_2(4) & & & & & \\ & J_2(-1) & & & & \\ & & J_3(4) & & & \\ & & & J_2(-1) & & \\ & & & & J_4(4) & \\ & & & & & J_2(-3) \end{pmatrix}$$

- $$\begin{pmatrix} J_2(3) & & & & & & \\ & J_2(3) & & & & & \\ & & J_3(3) & & & & \\ & & & J_2(3) & & & \\ & & & & J_4(3) & & \\ & & & & & J_2(3) \end{pmatrix}$$
- $$\begin{pmatrix} J_7(5) & & & & & & \\ & J_3(2) & & & & & \\ & & J_3(2) & & & & \\ & & & J_4(2) & & & \\ & & & & J_4(6) & & \\ & & & & & J_2(-3) \end{pmatrix}$$
- $$\begin{pmatrix} J_2(7) & & & & & & \\ & J_3(7) & & & & & \\ & & J_2(5) & & & & \\ & & & J_1(5) & & & \\ & & & & J_1(5) & & \\ & & & & & J_1(5) \end{pmatrix}$$
- $$\begin{pmatrix} J_1(0) & & & & & & \\ & J_1(2) & & & & & \\ & & J_1(-2) & & & & \\ & & & J_1(3) & & & \\ & & & & J_1(4) & & \\ & & & & & J_1(-3) \end{pmatrix}$$
- $$\begin{pmatrix} J_1(2) & & & & & & & \\ & J_2(2) & & & & & & \\ & & J_3(2) & & & & & \\ & & & J_2(4) & & & & \\ & & & & J_2(5) & & & \\ & & & & & J_3(5) & & \\ & & & & & & J_1(7) & \\ & & & & & & & J_3(7) \end{pmatrix}$$

- $$\begin{pmatrix} J_1(1) & & & & & & & \\ & J_1(2) & & & & & & \\ & & J_1(3) & & & & & \\ & & & J_1(4) & & & & \\ & & & & J_1(5) & & & \\ & & & & & J_1(6) & & \\ & & & & & & J_1(7) & \\ & & & & & & & J_1(8) \end{pmatrix}$$
- $$\begin{pmatrix} J_2(1) & & & & & & & \\ & J_2(2) & & & & & & \\ & & J_2(3) & & & & & \\ & & & J_2(4) & & & & \\ & & & & J_2(5) & & & \\ & & & & & J_2(6) & & \\ & & & & & & J_2(7) & \\ & & & & & & & J_2(8) \end{pmatrix}$$
- $$\begin{pmatrix} J_1(1) & & & & & & & \\ & J_2(2) & & & & & & \\ & & J_3(3) & & & & & \\ & & & J_4(4) & & & & \\ & & & & J_5(5) & & & \\ & & & & & J_6(6) & & \\ & & & & & & J_7(7) & \\ & & & & & & & J_8(8) \end{pmatrix}$$
- $$\begin{pmatrix} J_1(1) & & & & & & & \\ & J_2(1) & & & & & & \\ & & J_3(1) & & & & & \\ & & & J_4(2) & & & & \\ & & & & J_5(2) & & & \\ & & & & & J_6(3) & & \\ & & & & & & J_7(4) & \\ & & & & & & & J_8(4) \end{pmatrix}$$

Ejercicio 259. Sean A, B y C matrices. Demuestre lo siguiente:

- A es conjugada a A
- si A es conjugada a B entonces B es conjugada a A
- si A es conjugada a B y B es conjugada a C entonces A es conjugada a C.

Ejercicio 260. Sea A una matriz con coordenadas en un campo k. Demuestre que el producto de todos los factores invariantes de $xI - A$ es igual al polinomio característico de A. Concluya que el polinomio mínimo de A divide al polinomi característico de A.

Ejercicio 261. Sea A una matriz con coordenadas en un campo k. Demuestre que todos los factores invariantes de $xI - A$ se factorizan totalmente en $k[x]$ si y sólo si el polinomio característico de A se factoriza totalmente en $k[x]$.

Ejercicio 262. Sean A y A' matrices cuadradas con entradas en un campo k. Suponga que $xI - A$ y $xI - A'$ tienen los mismos factores invariantes. Demuestre que A y A' tienen el mismo polinomio característico, el mismo polinomio mínimo, y la misma forma canónica racional. Si además su polinomio característico se factoriza totalmente sobre k, demuestre que A y A' tienen la misma forma canónica de Jordan.

Ejercicio 263. Dé un ejemplo de matrices cuadradas que tengan los mismos polinomios mímos y los mismos polinomios característicos pero que tengan diferentes factores invariantes. ¿Cuál es el menor tamaño n para el que se puede dar un contraejemplo así?

Ejercicio 264. Sean A y A' matrices cuadradas sobre un campo k. Demuestre que son equivalentes las siguientes condiciones:

- A y A' son conjugadas
- $xI - A$ y $xI - A'$ tienen los mismos factores invariantes
- A y A' tienen la misma forma canónica racional

Si además los polinomios característicos de A y A' se factorizan totalmente sobre k, demuestre que las anteriores condiciones son equivalentes a que A y A' tengan la misma forma canónica de Jordan (hasta permutación de los bloques de Jordan).

Ejercicio 265. Demuestre que dos bloques de Jordan diferentes (ya sea de diferente tamaño o con diferente valor propio) no son matrices conjugadas.

Ejercicio 266. ¿Es posible que la forma canónica racional de una matriz coincida con su forma canónica de Jordan?

Ejercicio 267. Sean A una matriz cuadrada y R su forma canónica racional. Demuestre que la forma canónica racional de R es R.

Ejercicio 268. Sea A una matriz cuadrada cuyo polinomio característico se factoriza totalmente sobre el campo k, y sea J su forma canónica de Jordan.. Demuestre que el polinomio característico de J es igual al polinomio característico de A, y que la forma canónica de Jordan de J es J.

Ejercicio 269. Sea A una matriz cuadrada. Decimos que A es **diagonalizable** si A es conjugada a una matriz diagonal. Demuestre que son equivalentes las siguientes condiciones:

- A es diagonalizable
- la forma canónica de Jordan de A es una matriz diagonal
- el polinomio mínimo de A no tiene raíces múltiples

Ejercicio 270. Sea A una matriz cuadrada. Demuestre que el polinomio característico de A coincide con el polinomio mínimo de A si y sólo si $xI - A$ tiene un único factor invariante no constante.

Ejercicio 271. Sea A una matriz cuadrada. Demuestre que si el polinomio característico de A se factoriza totalmente sobre k y no tiene raíces múltiples, entonces A es diagonalizable. Dé un ejemplo de una matriz diagonalizable cuyo polinomio característico se factoriza totalmente pero tiene raíces múltiples.

Índice alfabético

Bibliografía

[1] The GAP Group. GAP – Groups, Algorithms and Programming. Version 4.3; 2002 (http://www.gap-system.org).

[2] Nathan Jacobson. 1 Basic Algebra I. W H Freeman and Co., 2nd edition, 1985.

El mejor texto para estudiar este tipo de curso es [2].

Yo exhorto a mis alumnos a usar la computadora para generar con facilidad ejemplos de lo que aprendemos en el curso. Uno de los mejores programas de álgebra que hay disponibles sin costo es GAP [1]. Pueden ir a la página de internet indicada y seguir las instrucciones para bajar GAP a su computadora personal.