Anillos y cuerpos

Luis Arenas

August 28, 2020

Contents

Chapter 1

Definiciones básicas

definición 1.1. Un *Anillo* $(A, +, \cdot)$ es un grupo abeliano $(A, +)$ junto con otra operación $\cdot$ que satisface las relaciones siguientes:

1. $a \cdot (b + c) = a \cdot b + a \cdot c$, y $(b + c) \cdot a = b \cdot a + c \cdot a$,
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Si solo se cumple (1), se dice que A es un anillo no asociativo. Si además se cumple la condición siguiente:

3. Existe $1 = 1_A$ tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in A$,

diremos que A es un *anillo unitario*.

En lo sucesivo nos referiremos a las operaciones + y $\cdot$ como suma y producto respectivamente y adoptaremos muchas convenciones usuales como omitir el punto al escribir una multiplicación.

Ejemplo 1.2. El conjunto de enteros pares $2\mathbb{Z}$ es un anillo pero no un anillo unitario. A menudo enfatizaremos este hecho llamando a un anillo de este tipo un anillo no unitario.

Un *homomorfismo de anillos* $\psi : A \to A'$, es un homomorfismo de grupos abelianos que además satisface $\psi(a)\psi(b) = \psi(ab)$. Es un *homomorfismo de anillos unitarios* si además satisface $\psi(1) = 1$.

Ejemplo 1.3. La función $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ definida por $\psi(0+2\mathbb{Z}) = 0+6\mathbb{Z}$, y $\psi(1 + 2\mathbb{Z}) = 3 + 6\mathbb{Z}$, es un homomorfismo de anillos (ya que $(3 + 6\mathbb{Z})^2 = 3 + 6\mathbb{Z}$), pero no de anillos unitarios.

Lema 1.4. *Si $x \in A$ satisface $x + x = x$, entonces $x = 0$.*

Demostración. Si $x+x=x$ sumamos $-x$ a ambos lados de la igualdad y obtenemos $x=0$. □

Proposición 1.5. *Si $a \in A$, entonces $a0 = 0a = 0$.*

Demostración. De hecho, $a0 = a(0+0) = a0 + a0$, y se aplica el lema precedente. □

definición 1.6. Sea $(A, +, \cdot)$ un anillo. Definimos:

- Un subanillo de A es un subgrupo aditivo B que es cerrado bajo productos, es decir si b y c están en B, también lo está el producto bc.
- Si A es un anillo unitario, un subanillo unitario es por definición un subanillo que contiene al 1.
- Si J es un subgrupo del grupo abeliano $(A, +)$, tal que $aJ \subseteq J$ para toda $a \in A$, J se llama un ideal por la izquierda.
- Si J es un subgrupo del grupo abeliano $(A, +)$, tal que $Ja \subseteq J$ para toda $a \in A$, J se llama un ideal por la derecha.
- Si J es un subgrupo del grupo abeliano $(A, +)$, tal que $aJ \subseteq J$ y $Ja \subseteq J$ para toda $a \in A$, J se llama un ideal bilátero.

Respecto de las definiciones precedentes, necesitamos hacer algunas observaciones:

- Un subanillo B de un anillo unitario A, puede ser unitario con las mismas operaciones que A sin ser un subanillo unitario con la definición precedente. Basta conque B contenga un elemento 1_B tal que $1_B b = b$ para todo elemento b de B, pero que esta relación no se cumpla para algún elemento de A. Ciertamente no puede cumplirse para 1_A si este no coincide con 1_B pues por definición $1_A 1_B = 1_B$.
- En general, un ideal J (por cualquier lado) de un anillo A es un subanillo pero no un subanillo unitario, salvo si $A = J$. Esto se demuestra probando que, si 1_A está en el ideal J, entonces $a = a \times 1_A \in aJ \subseteq J$. Puede ser, sin embargo, que J sea un anillo unitario con una unidad distinta 1_J. Veremos más adelante que este fenómeno ocurre realmente para ciertos tipos de anillos, por ejemplo los anillos producto.

- Un subanillo B es un subanillo unitario de A si y sólo si la inclusión es un morfismo de anillos unitarios.

Ejemplo 1.7. $n\mathbb{Z}$ es un ideal bilátero de $\mathbb{Z}$.

Ejemplo 1.8. si A es un anillo y x un elemento de A, entonces xA es un ideal por la derecha y Ax es un ideal por la izquierda. Entonces el subgrupo AxA formado por todas las sumas finitas de la forma $\sum_i a_i x a_i'$ con a y a' en A, es un ideal bilátero de A. El ideal AxA se llama el ideal bilátero generado por x.

Ejemplo 1.9. El conjunto

$$J = \left\{ \left(\begin{array}{cc} 0 & b \\ 0 & d \end{array} \right) \middle| b, d \in \mathbb{R} \right\}$$

es un ideal por la izquierda del anillo $\mathbb{M}_2(\mathbb{R})$ de matrices con coeficientes reales, pero no es un ideal por la derecha, como lo muestran las identidades siguientes:

$$\left(\begin{array}{cc} x & y \\ z & w \end{array} \right) \left(\begin{array}{cc} 0 & b \\ 0 & d \end{array} \right) = \left(\begin{array}{cc} 0 & xb+yd \\ 0 & zb+wd \end{array} \right) \in J,$$

$$\left(\begin{array}{cc} 0 & 1 \\ 0 & 2 \end{array} \right) \left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right) = \left(\begin{array}{cc} 1 & 0 \\ 2 & 0 \end{array} \right) \notin J.$$

Ejemplo 1.10. Sea $A = \mathbb{M}_2(\mathbb{Z})$ el anillo de matrices con coeficientes enteros, y sea $J = \mathbb{M}_2(n\mathbb{Z})$ el subconjunto de matrices cuyos coeficientes son divisibles por n. Entonces J es ideal bilátero de A, como el lector podrá probar como ejercicio. Probaremos en el capítulo de anillos y álgebras de matrices que todo ideal bilátero de A es de esta forma.

Sea J un ideal bilátero de A. Dado que A es un grupo abeliano, el cociente A/J es un grupo abeliano con la suma. Ahora bien

$$(a+J)(b+J) \subseteq ab + aJ + Jb + JJ \subseteq ab + J + J + J = ab + J.$$

Por lo tanto, A/J es tambien un anillo.

Ejemplo 1.11. El ideal $n\mathbb{Z}$ de $\mathbb{Z}$ define el anillo cociente $\mathbb{Z}/n\mathbb{Z}$ de enteros módulo n.

Proposición 1.12. *Sea $\psi : A \to A'$ un homomorfismo de anillos y sea $J = \ker \psi$. entonces J es un ideal bilátero. Por otro lado, todo ideal bilátero J es el núcleo de la proyección $P_J : A \to A/J$, la cual es un homomorfismo de anillos.*

Demostración. De hecho, si $j \in J$, entonces $\psi(aj) = \psi(a)\psi(j) = \psi(a)0 = 0$ y $\psi(ja) = \psi(j)\psi(a) = 0\psi(a) = 0$. La última afirmación es inmediata. □

Proposición 1.13 (Primer Teorema de Isomorfía)**.** *Si A y B son anillos y si $\phi : A \to B$ es un homomorfismo de anillos, se tiene que el homomorfismo inducido $\tilde{\phi} : A/\ker(\phi) \to \phi(A)$ definido por $\tilde{\phi}\Big(a + \ker(\phi)\Big) = \phi(a)$ es un isomorfismo de anillos. Si $\phi : A \to B$ es un homomorfismo de anillos unitarios, entonces también lo es $\tilde{\phi}$.*

Demostración. De hecho, $\tilde{\phi}$ es un isomorfismo de grupos abelianos y es inmediato que preserva productos o unidades si ϕ lo hace. □

Las siguientes proposiciones se demuestran del mismo modo:

Proposición 1.14 (Teorema de la correspondencia)**.** *Si A es un anillo y si I es un ideal bilátero, entonces todo ideal (por cualquier lado) de (A/I) es de la forma J/I donde J es un ideal (del mismo tipo) de A que contiene a I.*

Proposición 1.15 (Teorema de la correspondencia para subanillos)**.** *Si A es un anillo y si I es un ideal bilátero, entonces todo subanillo (o subanillo unitario) de A/I es de la forma B/I donde B es un subanillo (respectivamente un subanillo unitario) de A que contiene a I.*

Proposición 1.16 (Segundo Teorema de Isomorfía)**.** *Si A es un anillo y si $I \subseteq J$ son ideales biláteros, entonces el isomorfismo canónico de $\psi : (A/I)/(J/I) \to A/J$ es un isomorfismo de anillos. Si A es un anillo unitario, entonces ψ es un isomorfismo de anillos unitarios.*

Proposición 1.17 (Tercer Teorema de Isomorfía)**.** *Si A es un anillo, si I es un ideal bilátero de A y si B es un subanillo de A, entonces $B + I$ es un subanillo de A, $B \cap I$ es un ideal de B, y $B + I/I$ es isomorfo a $B/(B \cap I)$. Si B es unitario, este isomorfismo es un isomorfismo de anillos unitarios.*

Nótese que en la última afirmación no se requiere que A sea unitario, el siguiente ejemplo ilustra este punto:

Ejemplo 1.18. Utilizando la notación usual para intervalos en la recta real, sea A el anillo de funciones $f : [0, \infty[\to \mathbb{R}$ que se anulan en un intervalo de la forma $[K, \infty[$ con $K \in \mathbb{R}$. Se deja como ejercicio al lector comprobar que A es un anillo no unitario. Sea B el subanillo de las funciones que se anulan

en $[2, \infty[$. El anillo B es unitario ya que la función característica $\chi_{[0,2[}$ es un elemento unidad de B. Si I es el ideal de funciones que se anulan en $[1, 3[$, la proposición dice que $(B + I)/I$ es isomorfo a $B/(B \cap I)$. El primero de estos anillos es el anillo de funciones en A que se anulan en $[2, 3[$ cocientado con el ideal de funciones que se anulan en $[1, 3[$. El segundo es el anillo de funciones que se anulan en $[2, \infty[$ módulo funciones que se anulan en $[1, \infty[$. De hecho ambos se identifican naturalmente con el anillo de funciones a valores reales en el intervalo $[1, 2[$. Esto último se comprueba utilizando el homomorfismo que lleva a cada función a su restricción en este último intervalo y aplicando el primer teorema de isomorfía.

Ejemplo 1.19. Sea A el anillo de matrices triangulares superiores con coeficientes reales, es decir el anillo de matrices de la forma

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}.$$

Consideremos el ideal I formado por todas las matrices con ceros en la diagonal, mientras B es el subanillo formado por todas las matrices de la forma siguiente:

$$\begin{pmatrix} a & 0 & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}.$$

En este caso es fácil ver que $(B + I)/I \cong B/(B \cap I) \cong \mathbb{R}$.

Para cualquier grupo abeliano A se define el producto na, donde n es un entero y $a \in A$ como sigue:

> na es la suma de n términos $a+\ldots+a$ si $n > 0$, $0a = 0_A$, mientras que, si n es negativo, se utiliza la fórmula $na = -(-n)a$.

Si A es un anillo arbitrario, entonces la suma directa $\mathbb{Z} \oplus A$ es un anillo unitario con el producto $(n, a)(m, b) = (nm, nb + ma + ab)$. El elemento unidad del nuevo anillo es $1_{\mathbb{Z}\oplus A} = (1, 0_A)$. De este modo todo anillo puede asumirse contenido en un anillo unitario. Nótese sin embargo que si A era ya un anillo unitario, el elemento unidad 1_A de A (identificado con $(0, 1_A)$) no es el elemento unidad del nuevo anillo.

A partir de este punto y en el resto de estas notas, todos los anillos se asumen unitarios, a no ser que se especifíque lo contrario. Del mismo

modo, todos los homomorfismos de anillos serán homomorfismos de anillos unitarios, salvo mención expresa de lo contrario. Cuando sea absolutamente necesario utilizaremos la expresión *un anillo no necesariamente unitario* o *una homomorfismo de anillos no necesariamente unitarios*.

Inversos

definición 1.20. Si $a, b \in A$ satisfacen $ab = 1$, se dice que a es inverso por la izquierda de b y que b es inverso por la derecha de a. Si $ab = ba = 1$ se dice que a es el inverso de b. Si a tiene un inverso, se dice que es invertible.

Los inversos por un sólo lado pueden existir, como lo demuestra el ejemplo siguiente:

Ejemplo 1.21. Sea V es un espacio vectorial real, entonces el espacio vectorial $\mathrm{End}_{\mathbb{R}}(V)$ es un anillo con las operaciones de suma y multiplicación siguientes:

$$(f+g)(v) = f(v) + g(v),\ (fg)(v) = f(g(v)).$$

La unidad de este anillo es el elemento I_V definido por $I_V(v) = v$.

Sea V el espacio de sucesiones de números reales. Cada elemento $a \in V$ es un "vector infinito" $a = (a_1, a_2, a_3, \ldots)$. Sean F y E los elementos de $\mathrm{End}_{\mathbb{R}}(V)$ definidos por

$$Ea = (a_2, a_3, a_4, \ldots), \qquad Fa = (0, a_1, a_2, \ldots).$$

Entonces $EF = 1_{\mathrm{End}_{\mathbb{R}(V)}}$ pero $FE \neq 1_{\mathrm{End}_{\mathbb{R}(V)}}$. En particular, F tiene inverso por la izquierda y E por la derecha, pero no son invertibles, como se deduce del siguiente resultado.

Proposición 1.22. *Si a tiene un inverso por la izquierda b y por la derecha b', entonces $b = b'$ y a es invertible.*

Demostración. $b = b1 = b(ab') = (ba)b' = 1b' = b'$. □

El conjunto de los elementos invertibles de un anillo A es un grupo llamado el grupo de unidades de A y se denota A^*.

Ejercicios

1. Demuestre que si a y b son elementos de un anillo A y si X es un subconjunto de A, entonces se tiene $(a+b)X \subseteq aX + bX$.

2. Probar que el anillo del ejemplo 1.18 no es unitario.

3. Escriba demostraciones para las proposiciones 1.14 a 1.17.

4. Probar que todo subgrupo de $\mathbb{Z}$ es un ideal bilátero. Probar que esto no es cierto para el anillo $\mathbb{M}_2(\mathbb{Z})$ de matrices con coeficientes enteros.

5. Encuentre todos los ideales de $\mathbb{R}$.

6. Mas generalmente, probar que todo ideal que contiene a un elemento invertible es igual al anillo completo. Para ideales biláteros, pruebe que es suficiente que algún elemento tenga un inverso por un lado. Es esto cierto en general?

7. Probar que si J e I son ideales por la izquierda de R (por la derecha, biláteros) entonces tambien lo son $I + J$ e $I \cap J$.

8. Probar que si J es un ideal por la derecha, e I es un ideal por la izquierda de R, entonces $IJ = \{\sum_{k=1}^{n} i_k j_k | i_k \in I, j_k \in J\}$ es un ideal bilátero.

9. Probar que si J e I son ideales biláteros, entonces $JI \subseteq J \cap I$.

10. Si A es un anillo unitario y si existen don ideales biláteros I y J de A tales que $I + J = A$, probar que $IJ = I \cap J$. Sugerencia: Escribir $1_A = i + j$ con $i \in I$ y $j \in J$.

Chapter 2

Productos y matrices

En este capítulo estudiaremos las propiedades básicas de los productos de anillos, así como los resultados teóricos que nos permiten determinar si un anillo es o no isomorfo a un producto de anillos mas simples. Probaremos luego que (en el caso unitario, que es el que más nos concierne en estas notas) esto es equivalente a la existencia de ciertos elementos llamados idempotentes centrales. Este hecho hace que la descomposición de un anillo como producto sea más rígida que en el caso de espacios vectoriales o grupos unitarios.

Si A y A' son anillos, su producto cartesiano $A \times A'$ es un anillo con las operaciones siguientes:

$$(a, a') + (b, b') = (a + b, a' + b'), \qquad (a, a')(b, b') = (ab, a'b').$$

Mas generalmente, si $\{A_i\}_{i \in I}$ es una familia arbitraria de anillos, su producto $\prod_{i \in I} A_i$ es un anillo con las operaciones siguientes:

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}, \qquad (a_i)_{i \in I}(b_i)_{i \in I} = (a_i b_i)_{i \in I}.$$

La comprobación de las propiedades básicas a partir de la definición es un largo y tedioso ejercicio de re-escritura que se deja al lector. el principio básico es que, si alguna propiedad se cumple en cada coordenada, ciertamente se cumple en el producto.

Con las notaciones precedentes podemos reformular el problema principal de este capítulo como sigue:

> Determinar si un anillo dado A es isomorfo a un producto de la forma $A_1 \times A_2$ para ciertos anillos A_1 y A_2.

definición 2.1. Si $S \subseteq A$, el centralizador de S es el conjunto

$$C_A(S) = \{x \in A | xs = sx \quad \forall s \in S\}.$$

En particular, $Z(A) = C_A(A)$ se llama el centro de A. Un elemento $x \in Z(A)$ se dice central.

definición 2.2. Un elemento $P \in A$ se dice idempotente si $P^2 = P$.

Si $A \cong A_1 \times A_2$, los elementos $(0,1)$ y $(1,0)$ son idempotentes centrales de A. Inversamente, probaremos que si A tiene idempotentes centrales no triviales, entonces A es un producto.

Lema 2.3. *Si P es un idempotente, entonces $P^c := (1-P)$ es un idempotente.*

Demostración. $(1-P)^2 = 1-P-P+P^2 = 1-P-P+P = 1-P$. □

A P^c se le llama el complemento de P. Tambien se dice que P y P^c son complementarios. Nótese que se satisfacen las relaciones $P + P^c = 1$ y $PP^c = 0$.

Lema 2.4. *Si P es un idempotente central, entonces PA es un anillo con unidad $1_{PA} = P$.*

Nótese, sin embargo, que PA no es un subanillo unitario de A en el sentido definido en el capítulo precedente, ya que $1_A \neq 1_{PA}$.

Demostración. Nótese que PA es un subgrupo dado que $a \mapsto Pa$ es homomorfismo de grupos. Además, dado que P es central,

$$(PA)(PA) = P^2AA = PAA \subseteq PA.$$

Finalmente, si $x \in PA$, podemos escribir $x = Py$ para algún elemento y, de donde $Px = PPy = Py = x$. □

Lema 2.5. *Si P es un idempotente central, entonces $A \cong PA \times P^cA$.*

Demostración. Probaremos primero que A es la suma directa de PA y P^cA. De hecho $A \supseteq PA + P^cA \supseteq (P + P^c)A = A$, de donde $A = PA + P^cA$. Por otro lado, si $x \in PA \cap P^cA$, entonces $x = Px = PP^cx = 0$. Esto prueba que $A = PA \oplus P^cA$ como grupos abelianos.

Falta probar que el isomorfismo de grupos abelianos $PA \times P^cA \cong A$ inducido por la inclusión en cada factor es, de hecho, un isomorfismo de anillos. Si $a \in PA$ y $b \in P^cA$, entonces $ab = PaP^cb = PP^cab = 0$. De aqui sigue que si $a \in A$ se escribe como $a = a_1 + a_2$, con $a_1 \in PA$ y $a_2 \in P^cA$, y si $b \in A$ se escribe como $b = b_1 + b_2$, con $b_1 \in PA$ y $b_2 \in P^cA$, entonces se puede realizar el cálculo siguiente:

$$ab = (a_1 + a_2)(b_1 + b_2) = a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2 = a_1b_1 + a_2b_2.$$

Concluimos que $A \cong PA \times P^cA$ como anillos. □

Nótese que el hecho de que P es central implica que $(Pa)(Pb) = Pab$. Afirmamos que la función $x \mapsto Px$ es un homomorfismo de anillos cuyo núcleo es P^cA. Es claro que se anula en P^cA. Por otro lado, si $Px = 0$ entonces $x = Px + P^cx = P^cx$, lo que prueba la afirmación. Se concluye, gracias al Primer Teorema de Isomorfía, que $PA \cong A/P^cA$, de donde

$$A \cong \frac{A}{P^cA} \times \frac{A}{PA}.$$

Esta última forma es más util para calcular. Es también mas natural, dado que este último isomorfismo es un homomorfismo de anillos unitarios en cada variable, lo que no sucede con $A \cong PA \times P^cA$.

Ejemplo 2.6. En $\mathbb{Z}/6\mathbb{Z}$ el elemento $3 + 6\mathbb{Z}$ es idempotente. Tambien lo es $(1 + 6\mathbb{Z}) - (3 + 6\mathbb{Z}) = 4 + 6\mathbb{Z}$. Se concluye que:

$$\mathbb{Z}/6\mathbb{Z} \cong (3 + 6\mathbb{Z})\mathbb{Z}/6\mathbb{Z} \times (4 + 6\mathbb{Z})\mathbb{Z}/6\mathbb{Z} = 3(\mathbb{Z}/6\mathbb{Z}) \times 4(\mathbb{Z}/6\mathbb{Z}).$$

Por otro lado, se tiene

$$4(\mathbb{Z}/6\mathbb{Z}) \cong \frac{\mathbb{Z}/6\mathbb{Z}}{3\mathbb{Z}/6\mathbb{Z}} \cong \mathbb{Z}/3\mathbb{Z}.$$

Del mismo modo, si recordamos que la imagen de un subgrupo H en el cociente G/K es $(H + K)/K$, tenemos

$$3(\mathbb{Z}/6\mathbb{Z}) \cong \frac{\mathbb{Z}/6\mathbb{Z}}{4(\mathbb{Z}/6\mathbb{Z})} = \frac{\mathbb{Z}/6\mathbb{Z}}{(4\mathbb{Z} + 6\mathbb{Z})/6\mathbb{Z}} \cong \mathbb{Z}/(4\mathbb{Z} + 6\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z},$$

ya que $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$ como se verá en los ejercicios (y con mucho mayor generalidad en un capítulo posterior utilizando las propiedades de los ideales co-maximales), de donde

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

definición 2.7. Sean P_1 y P_2 idempotentes centrales de A. Diremos que $P_1 < P_2$ si $P_1P_2 = P_1$.

Proposición 2.8. *$P_1 < P_2$ si y sólo si $P_1A \subseteq P_2A$.*

Demostración. Si $P_1 < P_2$, entonces $P_1P_2 = P_1$. Luego $P_1A = (P_1P_2)A = P_2(P_1A) \subseteq P_2A$. Por otro lado, si $P_1A \subseteq P_2A$, entonces $P_1 \in P_2A$, y como se tiene $P_2x = x$ para todo $x \in P_2A$, se tiene en particular que $P_1P_2 = P_1$. □

Proposición 2.9. *Sean P_1 y P_2 idempotentes centrales que satisfacen $P_1P_2 = 0$. Si $P = P_1 + P_2$, entonces P es un idempotente central que satisface las relaciones $PA = P_1A \oplus P_2A$ y $PA \cong P_1A \times P_2A$.*

Demostración. Observemos que

$$(P_1 + P_2)^2 = P_1^2 + P_1P_2 + P_2P_1 + P_2^2 = P_1 + P_2.$$

De aquí se tiene que P es un idempotente y es fácil ver que es central. Las restantes afirmaciones son un caso particular de $A \cong PA \times P^cA$, aplicado al anillo PA, dado que P es la unidad de PA y $P - P_1 = P_2$, por lo que P_2 y P_1 son idempotentes complementarios en dicho anillo. □

Proposición 2.10. *Si $P_1, \ldots, P_n$ son idempotentes centrales que satisfacen $P_1 + \ldots + P_n = 1$ y $P_iP_j = 0$ para $i \neq j$, entonces $A \cong P_1A \times \ldots \times P_nA$.*

Demostración. Se procede por inducción, utilizando la proposición anterior. Los detalles se dejan al lector como ejercicio. □

Nótese que este isomorfismo puede escribirse también

$$A \cong \frac{A}{P_1^cA} \times \ldots \times \frac{A}{P_n^cA},$$

donde P_i^c es el complemento del correspondiente idempotente P_i.

El teorema chino de los restos (primera versión)

Sean I y J dos ideales biláteros en un anillo A no necesariamente unitario. Nótese que existe un homomorfismo bien definido

$$\phi : A \to \frac{A}{I} \times \frac{A}{J},$$

definido por la proyección $A \to A/I$ en la primera coordenada y, análogamente, como la proyección $A \to A/J$ en la segunda. No es muy dificil constatar que el núcleo de este morfismo es $I \cap J$. Se concluye que existe un isomorfismo

$$\frac{A}{(I \cap J)} \cong \phi(A).$$

Supongamos ahora que $I + J = A$. En este caso se dice que los ideales son co-maximales. En particular cada elemento $a \in A$ puede escribirse en la forma $a = i + j$ con $i \in I$ y $j \in J$. Concluimos que la clase lateral $a + I$ puede escribirse como $j + I$ con un representante en J. Del mismo modo, una J-clase lateral satisface $b + J = i' + J$ para algún representante i' en I. Concluimos que el elemento $c = i' + j$ satisface $c + I = a + I$ y $c + J = b + J$. Esto prueba que la función ϕ definida mas arriba es epiyectiva. Hemos por lo tanto probado el siguiente resultado, conocido normalmente como el teorema chino de los restos:

Proposición 2.11. *Sea A un anillo no neseriamente unitario, y sean I y J dos ideales que satisfacen $I + J = A$. Entonces existe un isomorfismo*

$$\frac{A}{(I \cap J)} \cong \frac{A}{I} \times \frac{A}{J}.$$

Asumamos ahora que A es un anillo unitario. Entonces la condición $I + J = A$ nos permite escribir $1 = i + j$. En tal caso, los idempotentes centrales del anillo $A/(I \cap J)$ son precisamente $P = i + (I \cap J)$ y $P^c = j + (I \cap J)$. Esto sigue de las identidades:

$$\phi(i) = (i + I, i + J) = (0 + I, 1 + J), \qquad \phi(j) = (j + I, j + J) = (1 + I, 0 + J).$$

Ejemplo 2.12. La identidad $3\mathbb{Z} + 2\mathbb{Z} = \mathbb{Z}$, la que sigue de la descomposición $1 = 4 - 3$, nos dice que:

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Mas aún, los idempotentes centrales que corresponden a esta descomposición son $4 + 6\mathbb{Z}$ y $-3 + 6\mathbb{Z}$. Nótese que cualquier otra descomposición como $1 = 3 - 2$ da lugar a los mismos idempotentes, de hecho $-2 + 6\mathbb{Z} = 4 + 6\mathbb{Z}$.

Ejemplo 2.13. Nótese que $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$. El homomorfismo

$$\phi : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

definido arriba tiene como imagen al subanillo de elementos de la forma $(a + 4\mathbb{Z}, b + 6\mathbb{Z})$ donde a y b tienen la misma paridad, lo que el lector podrá comprobar fácilmente como ejercicio. Se concluye que, en este caso, la igualdad inicial de este ejemplo no nos permite obtener una descomposición del anillo $\mathbb{Z}/12\mathbb{Z}$ como un producto. Este anillo, sin embargo, si tiene una descomposición como producto, la que el lector debiera poder encontrar sin dificultad.

El mismo razonamiento demuestra el siguiente resultado:

Proposición 2.14. *Sean $J_1, \ldots, J_n$ ideales de un anillo A. Entonces existe un homomorfismo inyectivo de anillos*

$$\Phi : A/\left(\bigcap_{i=1}^{n} I_i\right) \to \prod_{i=1}^{n} A/I_i. \quad \square$$

Elementos nilpotentes

Un concepto relacionado con el de elemento idempotente es el de elemento *nilpotente*.

definición 2.15. Un elemento $u \in A$ se llama nilpotente, si $u^n = 0$ para algún n.

Proposición 2.16. *Si u es nilpotente, entonces $1 - u$ tiene inverso multiplicativo.*

Demostración. $(1 - u)(1 + u + u^2 + \ldots + u^{n-1}) = 1 - u^n = 1.$ $\square$

Ejemplo 2.17. En $\mathbb{Z}/243\mathbb{Z}$, $4 + 243\mathbb{Z}$ es invertible, ya que $4 = 1 - (-3)$, y su inverso es $1 + (-3) + (-3)^2 + (-3)^3 + (-3)^4 + 243\mathbb{Z} = 61 + 243\mathbb{Z}$.

Ejercicios

1. Probar que si P_1 y P_2 son idempotentes centrales de R, y si $P = P_1 + P_2 - P_1P_2$, entonces

   a) P es un idempotente central.

   b) $P_1 < P$ y $P_2 < P$.

   c) Si $P_1 < P'$ y $P_2 < P'$, entonces $P < P'$.

   d) Si $P_1 < P_2$, entonces $P = P_2$.

   (Recuerde que $P < P'$ quiere decir $PP' = P$).

2. Probar que si $a \in R$ tiene inverso multiplicativo, y si u es un elemento nilpotente que satisface $ua = au$, entonces $a - u$ tiene inverso multiplicativo.

3. Probar que si P_1 y P_2 son idempotentes centrales de A, entonces

$$A \cong P_1P_2A \times (1 - P_1)P_2A \times P_1(1 - P_2)A \times (1 - P_1)(1 - P_2)A.$$

4. Probar que $Z(A_1 \times A_2) = Z(A_1) \times Z(A_2)$.

5. Probar que si u y v son nilpotentes y si $uv = vu$, entonces $u + v$ es nilpotente.

6. Probar que $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

7. Sea $x \in A$ idempotente. Probar que

   a) Si x es nilpotente, $x = 0$.

   b) Si x es invertible, $x = 1$.

8. Probar que $\mathbb{Z}/2^n\mathbb{Z}$ no puede escribirse como un producto no trivial (sugerencia, probar que todos sus elementos son nilpotentes o invertibles).

9. Probar que si $a \in Z(A)$, entonces aA es un ideal bilátero.

10. Probar que si $A = A_1 \times A_2$, y si $J = A_1 \times \{0\}$, entonces J es un ideal bilátero de A y $A/J \cong A_2$.

11. Dados idempotentes centrales P_1 y P_2, definimos idempotentes centrales $P_1 \wedge P_2 = P_1P_2$ y $P_1 \vee P_2 = P_1 + P_2 - P_1P_2$. Probar las siguientes identidades:

$$P_1 \wedge P_2 = P_2 \wedge P_1, \qquad (P_1 \wedge P_2) \wedge P_3 = P_1 \wedge (P_2 \wedge P_3),$$

$$P_1 \vee P_2 = P_2 \vee P_1, \qquad (P_1 \vee P_2) \vee P_3 = P_1 \vee (P_2 \vee P_3),$$

$$P_1 \vee P_1 = P_1 \wedge P_1 = P_1,$$

$$P \vee 0 = P,\ P \wedge 0 = 0,\ P \vee 1 = 1,\ P \wedge 1 = P,$$

$$(P_1 \vee P_2) \wedge P_3 = (P_1 \wedge P_3) \vee (P_2 \wedge P_3), \qquad (P_1 \wedge P_2) \vee P_3 = (P_1 \vee P_3) \wedge (P_2 \vee P_3),$$

$$(P_1 \vee P_2) \wedge P_1 = P_1, \qquad (P_1 \wedge P_2) \vee P_1 = P_1.$$

12. Un idempotente central P se dice minimal si $P' < P$ implica $P' = 0$ o $P' = P$. Probar que si $1 = P_1 + \ldots + P_n$ en R, y si cada P_i es minimal en R, entonces todo idempotente central de R es de la forma

$$\sum_{i \in A} P_i,$$

donde $A \subseteq \{1, \ldots, n\}$.

13. Encuentre el inverso de 31 en $\mathbb{Z}/3^6\mathbb{Z}$ (sugerencia, $31 = 1 + 30$).

14. Probar que si p no divide a n, entonces $\mathbb{Z}/pn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Puede asumir que $\mathbb{Z}/p\mathbb{Z}$ es cuerpo, es decir, para todo $n \in \mathbb{Z}$ existe r tal que $rn \equiv 1(p)$.

15. Probar que en un anillo conmutativo C el conjunto de elementos nilpotentes es un ideal (llamado el *nilradical*) de C.

Anillos de matrices

En esta sección generalizaremos el concepto de matriz a un anillo cualquiera, lo que nos permitir construir algunos ejemplos más elaborados de anillos no conmutativos. Aqui y en lo sucesivo utilizamos la convención de que $\mathbf{n}$ denota el conjunto $\{1, \ldots, n\}$.

definición 2.18. Sea R un anillo no necesariamente unitario. El anillo de matrices $\mathbb{M}_n(R)$ con coeficientes en R es el grupo abeliano $R^{\mathbf{n}\times\mathbf{n}}$, es decir el grupo de funciones en $\mathbf{n}\times\mathbf{n}$, a valores en R, que identificamos simplemente con arreglos $(a_{j,k})_{j,k=1}^{n}$ de $n\times n$ elementos de R con la adición por componentes. A este grupo abeliano le asociamos la multiplicación definida por

$$(a_{i,j})_{i,j=1}^{n}\,(b_{j,k})_{j,k=1}^{n}=\left(\sum_{j=1}^{n}a_{i,j}b_{j,k}\right)_{i,k=1}^{n}.$$

Todas las propiedades de un anillo se comprueban inmediatamente de la definición.

Ejemplo 2.19. En $\mathbb{M}_2(R)$, la definición se reduce a

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} e & f\\ g & h\end{pmatrix}=\begin{pmatrix} ae+bg & af+bh\\ ce+dg & cf+dh\end{pmatrix}.$$

Es importante, en todos estos ejemplos, tener en mente que el anillo de coeficientes R no necesita ser conmutativo, por lo que el orden de los factores en cada coordenada resulta importante. En particular, es posible definir un anillo de matrices con coeficientes en otro anillo de matrices.

Si R es un anillo unitario, también lo es $\mathbb{M}_n(R)$, con la unidad definida como sigue:

$$1_{\mathbb{M}_n(R)}=\begin{pmatrix} 1_R & 0 & 0 & \cdots & 0\\ 0 & 1_R & 0 & \cdots & 0\\ 0 & 0 & 1_R & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & 1_R\end{pmatrix}.$$

Ejemplo 2.20. La funcion $\psi:\mathbb{M}_2\Big(\mathbb{M}_2(R)\Big)\to\mathbb{M}_4(R)$ definida por

$$\psi\left(\begin{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix} & \begin{pmatrix} e & f\\ g & h\end{pmatrix}\\ \begin{pmatrix} i & j\\ k & l\end{pmatrix} & \begin{pmatrix} n & m\\ o & p\end{pmatrix}\end{pmatrix}\right)=\begin{pmatrix} a & b & e & f\\ c & d & g & h\\ i & j & m & n\\ k & l & o & p\end{pmatrix}$$

es un isomorfismo como el lector puede comprobar como ejercicio. Mas generalmente, puede probarse que el anillo $\mathbb{M}_n\Big(\mathbb{M}_m(R)\Big)$ es isomorfo a $\mathbb{M}_{mn}(R)$.

Este isomorfismo es el que permite realizar las operaciones de suma y producto de matrices *por bloques*. Tendremos bastante que decir sobre este tipo de homomorfismos en los capítulos finales de estas notas.

El anillo R es isomorfo al subanillo de $\mathbb{M}_n(R)$ formado por las matrices de la forma

$$rI_n = \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ 0 & r & 0 & \cdots & 0 \\ 0 & 0 & r & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & r \end{pmatrix}.$$

Nótese sin embargo que este no es el producto de r por una matriz I_n, ni siquiera con una definición apropiada de multiplicación escalar, a no ser que R sea un anillo unitario. A pesar de esto, el conjunto de estas matrices se denota siempre por RI_n. Así definido, RI_n es un subanillo isomorfo a R, por lo que podemos identificarlos. Si R no es untario podemos asumir que está contenido en un anillo unitario R', de donde $\mathbb{M}_n(R) \subseteq \mathbb{M}_n(R')$. Asumiremos que R es unitario en todo lo que sigue. En este caso, la matriz identidad $I_n = 1I_n$ es realmente un elemento de $\mathbb{M}_n(R)$.

Sea $E_{i,j}$ La matriz que tiene un 1 en la intersección de la fila i con la columna j y que tiene un 0 en cada una de las restantes posiciones, entonces se tienen las siguientes identidades:

1. $E_{i,j}E_{j,k} = E_{i,k}$, $E_{i,j}E_{u,k} = 0$, si $u \neq j$.
2. $E_{1,1} + E_{2,2} + \ldots + E_{n,n} = I_n$.
3. $rE_{i,j} = E_{i,j}r$, si $r \in RI_n$.

Además, si A es cualquier anillo con un subanillo isomorfo a R y con elementos $E_{i,j}$ que satisfacen las relaciones (1),(2) y (3), entonces el subconjunto A' de A formado por todas las combinaciones del tipo $a = \sum_{i,j} r_{i,j}E_{i,j}$ es un subanillo y la función que lleva a la matriz $(r_{i,j})_{i,j}$ al elemento $a = \sum_{i,j} r_{i,j}E_{i,j}$ es un homomorfismo de anillos. Más aún, si una de estas expresiones se anula, digamos $\sum_{i,j} r_{i,j}E_{i,j} = 0$, premultiplicando por $E_{u,s}$ y postmultiplicando por $E_{t,u}$ se tiene $r_{s,t}E_{u,u} = 0$. Sumando sobre u estas identidades, se concluye que $r_{s,t} = 0$. Esto implica que $A' \cong \mathbb{M}_n(R)$.

Ejemplo 2.21. Si $n = 2$ entonces

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = aE_{1,1} + bE_{1,2} + cE_{2,1} + dE_{2,2}.$$

Observación 2.22. En general no es cierto que si $\mathbb{M}_n(R) \cong \mathbb{M}_m(R')$ entonces $R \cong R'$. Basta tomar como ejemplo el caso $n = 2$, $m = 1$, con $R = \mathbb{R}$ y $R'' \cong \mathbb{M}_2(\mathbb{R})$. Sin embargo, cuando R es conmutativo, entonces $R \cong RI_n$ se puede caracterizar como el conjunto de matrices que conmutan con cualquier otra, es decir el centro de $\mathbb{M}_n(R)$. En tal caso podemos recuperar la estructura de un anillo R de la estructura de cualquiera de sus anillos de matrices.

Si J es un ideal bilátero de R, el anillo (no unitario, en general) de matrices con coeficientes en J se denota por $\mathbb{M}_n(J)$ de acuerdo a nuestras convenciones previas.

Proposición 2.23. *El subanillo $\mathbb{M}_n(J)$ definido arriba es un ideal bilátero de $\mathbb{M}_n(R)$ y se tiene un isomorfismo natural*

$$\psi : \frac{\mathbb{M}_n(R)}{\mathbb{M}_n(J)} \stackrel{\cong}{\to} \mathbb{M}_n(R/J).$$

Demostración. Denotaremos por $\bar{a}$ la clase lateral $a+J$ para cualquier elemento a de R y hacemos lo mismo con el anillo de matrices. Necesitamos probar que la correspondencia

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \mapsto \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$$

es un isomorfismo. Para ello, gracias al Primer Teorema de Isomorfía, es suficiente probar que la correspondencia

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$$

es un homomorfismo epiyectivo cuyo núcleo es $\mathbb{M}_n(J)$. Cada una de estas afirmaciones es inmediata a partir de las definiciones, o un largo ejercicio de poner y reunir barras. También es claro que $\mathbb{M}_n(J)$, puesto que es el núcleo de un homomorfismo. □

Ejemplo 2.24. El anillo cociente

$$\frac{\mathbb{M}_n(\mathbb{Z})}{\mathbb{M}_n(2\mathbb{Z})}$$

es isomorfo al anillo de matrices con coeficientes en el cuerpo $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$ con 2 elementos.

Proposición 2.25. *Todo ideal bilátero del anillo $\mathbb{M}_n(R)$ es de la forma $\mathbb{M}_n(J)$ para algún ideal J de R.*

Demostración. Sea $\mathbb{I}$ un ideal del anillo de matrices $\mathbb{M}_n(R)$. Sea

$$J = \{a \in R | aI_n \in \mathbb{I}\}.$$

Probaremos que $\mathbb{I} = \mathbb{M}_n(J)$. Es fácil ver que $\mathbb{M}_n(J)$ está contenido en $\mathbb{I}$, pues cada elemento $a \in \mathbb{M}_n(J)$ se escribe en la forma

$$a = \sum_{i,j} a_{i,j} E_{i,j} = \sum_{i,j} a_{i,j} I_n E_{i,j}$$

con $a_{i,j} I_n \in JI_n \subseteq \mathbb{I}$. Sea ahora $b = \sum_{i,j} b_{i,j} E_{i,j} \in \mathbb{I}$. Basta probar que cada $b_{i,j}$ está en J, para lo que observamos que

$$b_{i,j} I_n = \sum_{u=1}^{n} b_{i,j} E_{n,n} = \sum_{u=1}^{n} b_{i,j} E_{n,i} E_{i,j} E_{j,n} = \sum_{u=1}^{n} E_{n,i} b E_{j,n} \in \mathbb{I}.$$

El hecho de que J es un ideal se sigue del hecho de que JI_n es un ideal de RI_n, por ser la intersección de un ideal con el subanillo, y del hecho de que R y RI_n son isomorfos. □

Proposición 2.26. *El paso de un anillo a su anillo de matrices conmuta con la toma de productos en el sentido siguiente:*

$$\mathbb{M}_n(R_1 \times R_2) \cong \mathbb{M}_n(R_1) \times \mathbb{M}_n(R_2).$$

Demostración. Basta ver que si $P = (1, 0)$ es un idempotente central de R, entonces la matriz PI_n es un idempotente central del anillo de matrices $\mathbb{M}_n(R)$, y utilizar la obvia identidad $(PI_n)\mathbb{M}_n(R) = \mathbb{M}_n(PR)$. □

Otras propiedades del anillo de matrices pueden demostrarse por un procedimiento similar.

Ejercicios

1. Describa todos los ideales biláteros de $\mathbb{M}_n(\mathbb{Z})$.
2. Sea $A = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in R \right\}$. Probar que $J = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} | b \in R \right\}$ es un ideal bilátero de A.
3. Probar que el centro de $\mathbb{M}_n(R)$, es decir el conjunto de elementos que conmutan con cada elemento de este anillo, es efectivamente $Z(R)I_n$ donde $Z(R)$ es el centro de R.
4. Calcule el inverso, en $\mathbb{M}_3(\mathbb{Z}/125\mathbb{Z})$ de
$$\begin{pmatrix} 16 & 25 & 40 \\ 5 & 11 & 75 \\ 60 & 25 & 46 \end{pmatrix}.$$
5. Calcule el inverso, en $\mathbb{M}_3(\mathbb{Z}/8\mathbb{Z})$ de
$$B = \begin{pmatrix} 9 & 11 & 1 \\ 4 & 1 & 3 \\ 4 & 2 & 7 \end{pmatrix}.$$
Sugerencia: Probar que $(B-1)^5 = 0$.
6. Sean a, b, c, d matrices de 2 por 2 con coeficientes reales y sea A una matriz de 4 por 4 que tiene una descomposición por bloques del tipo
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$
Suponga que a es invertible y conmuta con c. Probar que A es invertible si y sólo $ad - cb$ es invertible. Se sugiere intentar realizar operaciones por filas o columnas, que cuidados se deben tener?
7. Probar que el aillo de matrices del tipo $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ es isomorfo al cuerpo $\mathbb{C}$ de números complejos. Probar que el anillo de matrices de 4 por cuatro con una descomposición en bloques de 2 por 2 como las del problema anterior en la cual cada bloque es del tipo $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ es isomorfo a $\mathbb{M}_n(\mathbb{C})$.

Chapter 3

Anillos Conmutativos

Sea C un anillo conmutativo y sea $x \in C$. Entonces, $CxC = xC$ es un ideal bilátero que denotaremos también (x) si el anillo ambiente C es claro del contexto. Esto es combeniente a fin de simplificar las notaciones en los cálculos de cocientes que realizaremos más adelante.

Proposición 3.1. *Si C es un anillo conmutativo, un elemento $x \in C$ es invertible si y sólo si $(x) = C$.*

Demostración. Si $xy = 1$, entonces $C = (1) \subseteq (x)$. Conversamente, si $(x) = C$ entonces $1 \in (x)$, luego $1 = xy$ para algún elemento $y \in C$. □

Ejemplo 3.2. Si los únicos ideales de C son $\{0\}$ y C, entonces todo elemento de C distinto de 0 es invertible. En este caso se dice que C es un cuerpo.

Ejemplo 3.3. Si $A = \mathbb{M}_2(\mathbb{R})$, y $a = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, entonces $AaA = A$, ya que

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

En este caso no es cierto que $Aa = AaA$, de hecho

$$Aa = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \middle| b, d \in \mathbb{R} \right\},$$

como el lector puede comprobar fácilmente. Es por esta razón por la que el material de este capítulo, a diferencia del cubierto en los capítulos precedentes, no se extiende al caso de anillos no conmutativos.

En este capítulo, asumiremos siempre que C denota un anillo conmutativo. En este caso, diremos un ideal, en vez de un ideal bilátero. Nótese que, en este contexto, el cociente de un anillo por un ideal es un anillo cociente.

definición 3.4. Sea $\mathfrak{m}$ un ideal de C. Diremos que $\mathfrak{m}$ es maximal si:
1) $\mathfrak{m} \neq C$.
2) Para todo ideal I, si $I \supseteq \mathfrak{m}$ entonces $I = C$ o $I = \mathfrak{m}$.

Ejemplo 3.5. Por el ejemplo 3.2, un anillo conmutativo es cuerpo si y sólo si el ideal $\{0_C\}$ es maximal.

Proposición 3.6. *Un ideal $\mathfrak{m}$ es maximal si y sólo si $C/\mathfrak{m}$ es un cuerpo.*

Demostración. Se sigue inmediatamente del ejemplo precedente que $C/\mathfrak{m}$ es un cuerpo si y sólo si tiene exactamente dos ideales. Del Teorema de la Correspondencia deducimos que esta condición es equivalente a la maximalidad. □

En este capítulo necesitaremos hacer uso repetido del lema de Zorn, que recordamos aquí para conveniencia del lector:

Lema 3.7. *Si X es un conjunto parcialmente ordenado no vacío en el que cada cadena tiene una cota superior, entonces X tiene un elemento maximal.* □

Recuerdese que una cadena en X es un subconjunto de X parcialmente ordenado. Una cota superior de un subconjunto $A \subseteq X$ es un elemento $x \in X$ que satisface $a \leq x$ para todo $a \in A$. Adicionalmente, un elemento maximal se define como una cota superior para el conjunto completo X. Necesitaremos también el siguiente lema:

Lema 3.8. *Si $\mathfrak{C}$ es una cadena no vacía del conjunto de ideales de un anillo conmutativo C entonces $\tilde{I} = \cup_{I \in \mathfrak{C}} I$ en un ideal de C.*

Demostración. Es claro que $\tilde{I}$ es no vacío. Sean a y b dos elementos de $\tilde{I}$. entonces existen ideales $I, J \in \mathfrak{C}$ que satisfacen $a \in I$ y $b \in J$. Por ser $\mathfrak{C}$ una cadena uno de ellos está contenido en el otro. Si $I \subseteq J$, entonces $a, b \in J$ de donde $a - b \in J$, por lo que J es un subgrupo. El otro caso es similar. La demostración de que $\lambda a \in \tilde{I}$ para todo $\lambda \in C$ es directa y no requiere la hipótesis de que $\mathfrak{C}$ es una cadena. La dejamos al lector como ejercicio. □

Proposición 3.9. *Sea C un anillo conmutativo. Si J es un ideal de C, con $J \neq C$, entonces $J \subseteq \mathfrak{m}$ para algún ideal maximal $\mathfrak{m}$. Si $x \in C$ no es invertible, entonces $x \in \mathfrak{m}$ para algún ideal maximal $\mathfrak{m}$.*

Demostración. Utilizaremos el lema de Zorn.

Sea $X = \{I \text{ ideal en } C | I \neq C,\ J \subseteq I\}$. El conjunto X satisface las hipótesis del lema de Zorn. La primera es simple, el conjunto X es no vacío ya que contiene a J. La segunda hipótesis sigue de la siguiente afirmación:

> Si $\mathfrak{C}$ es una cadena en X, entonces $\tilde{I} = \cup_{I \in \mathfrak{C}} I$ es un elemento de X.

Se sigue del lema precedente que $\tilde{I}$ es un ideal. Probaremos que no es igual a C. Para todo $I \in \mathfrak{C}$ se tiene $I \neq C$ y por lo tanto $1 \notin I$. Se sigue que $1 \notin \tilde{I}$, de donde sigue lo pedido.

Por el lema de Zorn, X tiene un elemento maximal. Cualquier tal elemento es un ideal maximal que contiene a J. Para la última afirmación tomamos $J = (x)$. □

En la demostración precedente resulta esencial el hecho de que C es un anillo unitario. La existencia de ideales maximales no está garantizada, en general, para anillos no unitarios. Por cierto, buena parte de la teoría presentada en este capítulo falla también en dicho contexto.

definición 3.10. El radical de Jacobson de C es la intersección de todos los ideales maximales, es decir:

$$\mathfrak{R}(C) = \bigcap_{\mathfrak{m} \in \mathrm{Max}(C)} \mathfrak{m},$$

donde $\mathrm{Max}(C)$ es el conjunto de los ideales maximales de C.

Proposición 3.11. *Sea $x \in C$. Entonces $x \in \mathfrak{R}(C)$ si y sólo si $1 + xy$ es invertible para todo $y \in C$.*

Demostración. Si $1 + xy$ no es invertible, existe un ideal maximal $\mathfrak{m}$ que contiene a $1 + xy$, luego, si $x \in \mathfrak{R}(C) \subseteq \mathfrak{m}$, entonces se tiene $1 = x(-y) + (1 + xy) \in \mathfrak{m}$, lo que contradice la definición de ideal maximal.

Ahora, si $x \notin \mathfrak{R}(C)$, entonces $x \notin \mathfrak{m}$ para algún ideal maximal $\mathfrak{m}$. Se sigue que $x + \mathfrak{m} \neq 0 + \mathfrak{m}$. Como $C/\mathfrak{m}$ es un cuerpo, existe $z + \mathfrak{m}$ tal que $(x + \mathfrak{m})(z + \mathfrak{m}) = 1 + \mathfrak{m}$. SE sigue que $(1 - xz) \in \mathfrak{m}$, es decir $1 + x(-z)$ no es invertible. □

Ejemplo 3.12. El radical de jacobson de $\mathbb{Z}/30\mathbb{Z}$ es la intersección de los ideales $2\mathbb{Z}/30\mathbb{Z}$, $3\mathbb{Z}/30\mathbb{Z}$, y $5\mathbb{Z}/30\mathbb{Z}$, de donde $\mathfrak{R}(\mathbb{Z}/30\mathbb{Z}) = \{0 + 30\mathbb{Z}\}$.

Ejemplo 3.13. El radical de jacobson de $\mathbb{Z}/8\mathbb{Z}$ es su único ideal maximal $\mathfrak{R}(\mathbb{Z}/8\mathbb{Z}) = 2Z/8\mathbb{Z}$.

Ejemplo 3.14. El radical de jacobson de $\mathbb{Z}/12\mathbb{Z}$ es la intersección de los ideales $2\mathbb{Z}/12\mathbb{Z}$, y $3\mathbb{Z}/12\mathbb{Z}$, de donde $\mathfrak{R}(\mathbb{Z}/12\mathbb{Z}) = 6\mathbb{Z}/12\mathbb{Z}$ tiene dos elementos, $0 + 12\mathbb{Z}$ y $6 + 12\mathbb{Z}$.

Ejemplo 3.15. Mas generalmente, si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ donde $p_1, \dots, p_r$ son primos distintos, entonces el radical de jacobson de $\mathbb{Z}/n\mathbb{Z}$ es es $m\mathbb{Z}/n\mathbb{Z}$ donde $m = p_1 p_2 \dots p_n$.

definición 3.16. Un ideal $\wp$ de C es primo si, para todo par de elementos a, b de C, $ab \in \wp$ implica $a \in \wp$ o $b \in \wp$.

definición 3.17. Un anillo conmutativo C es un dominio de integridad si el ideal $\{0\}$ es primo. En otras palabras, C es dominio de integridad si y sólo si, para todo par de elementos a, b de C, $ab = 0$ implica $a = 0$ o $b = 0$. Si a y b son elementos no nulos de C tales que $ab = 0$, se dice que a y b son divisores de 0. Un dominio de integridad es, por lo tanto, un anillo conmutativo sin divisores de 0.

Proposición 3.18. *Un ideal $\wp$ es primo si y sólo si $C/\wp$ es un dominio de integridad.*

Demostración. Esto sigue inmediatamente de la definición, ya que $a + \wp = 0 + \wp$ significa $a \in \wp$. □

definición 3.19. El nilradical de C es la intersección de todos los ideales primos, es decir:

$$\mathfrak{N}(C) = \bigcap_{\wp \in \mathrm{Spec}(C)} \wp,$$

donde $\mathrm{Spec}(C)$ es el conjunto de los ideales primos de C y se llama el espectro de C.

Proposición 3.20. *Sea $x \in C$. Entonces $x \in \mathfrak{N}(C)$ si y sólo si x es nilpotente.*

Demostración. Si $x^n = 0 \in \wp$ y $\wp$ es primo, entonces $x \in \wp$ dado que $0 \in \wp$, como $\wp$ era un ideal primo arbitrario, concluimos $x \in \mathfrak{N}(C)$.

Suponemos ahora que x no es nilpotente. Sea

$$\Sigma = \Big\{ J \text{ ideal en } C | x^n \notin J \text{ para todo } n \in \{1, 2, 3, \ldots\} \Big\}.$$

El conjunto Σ satisface las hipótesis del lema de Zorn, de hecho:

1. Σ es no vacío ya que $(0) \in \Sigma$.
2. Si $\mathfrak{C}$ es una cadena en Σ, entonces $\tilde{J} = \cup_{J \in \mathfrak{C}} J \in \Sigma$ es un ideal, y no contiene a ninguna potencia de x ya que lo mismo es cierto para los elementos de $\mathfrak{C}$.

Por el lema de Zorn, Σ tiene un elemento maximal $\wp$. Probaremos ahora que $\wp$ es primo. Supongamos, por el contrario, que $ab \in \wp$. Si $a \notin \wp$, entonces por la maximalidad, existe n tal que $x^n \in (a) + \wp$, pues este último es un ideal estrictamente mayor a $\wp$. Del mismo modo, si $b \notin \wp$ existe m tal que $x^m \in (b) + \wp$. Pero entonces

$$x^{m+n} \in ((a) + \wp)((b) + \wp) \subseteq (ab) + \wp = \wp,$$

lo que contradice la eleccion de $\wp$. □

Ejemplo 3.21. En el anillo $\mathbb{Z}/12\mathbb{Z}$, el elemento $6+12\mathbb{Z}$ es el único nilpotente distinto de 0, luego $\mathfrak{N}(\mathbb{Z}/12\mathbb{Z}) = \{0 + 12\mathbb{Z}, 6 + 12\mathbb{Z}\}$.

Ejemplo 3.22. En el anillo $\mathbb{Z}$, los ideales primos son los ideales maximales y el ideal $\{0\}$.

Observación 3.23. Todo cuerpo es un dominio de integridad. Luego, todo ideal maximal es primo.

Proposición 3.24. *Todo dominio de integridad finito es un cuerpo.*

Demostración. Sea D un dominio de integridad finito. Sea $x \in D$ distinto de 0, y sea $\phi : D \to D$ la función definida por $\phi(y) = xy$. Por ser D un dominio de integridad, ϕ es inyectiva. Luego es epiyectiva. Luego $1 = \phi(y) = xy$ para algún $y \in D$. □

Corolario 3.24.1. *En un anillo conmutativo finito, todo ideal primo es maximal.*

Corolario 3.24.2. *Si C es un anillo conmutativo finito, entonces $\mathfrak{N}(C) = \mathfrak{R}(C)$.*

Corolario 3.24.3. *Si C es un anillo conmutativo finito, y si $1+xy$ invertible para todo $y \in C$, entonces x nilpotente.*

El teorema Chino de los restos (segunda versión)

Sean $J_1, \ldots, J_n$ ideales de un anillo conmutativo C. Probamos en el capítulo 2 que existe un homomorfismo inyectivo de anillos

$$\Phi : C/\left(\bigcap_{i=1}^{n} I_i\right) \to \prod_{i=1}^{n} C/I_i. \tag{3.1}$$

Además vimos que si $n = 2$, la condición $I + J = C$ era suficiente para garantizar la epiyectividad. Generalizaremos aquí ese resultado utilizando el concepto de comaximalidad.

definición 3.25. Dos ideales I y J de C son *comaximales* si $I+J = (1)$. Mas generalmente si $J_1, \ldots, J_n$ son ideales de C tales que J_r y J_s son comaximales para $r \neq s$, diremos que $J_1, \ldots, J_n$ son comaximales a pares.

Lema 3.26. *Si J es comaximal con I_1 e I_2 entonces es comaximal con $I_1 \cap I_2$.*

Demostración. La hipótesis implica que $a_1+b_1 = a_2+b_2 = 1$ con $a_i \in J$ y $b_i \in I_i$. multiplicando ambas igualdades se tiene $(a_1a_2+a_1b_2+a_2b_1)+b_1b_2 = 1$, donde el término entre paréntesis está en J y $b_1b_2 \in I_1 \cap I_2$. Se sigue que $1 \in J + I_1 \cap I_2$. □

Utilizando el lema precedente, se obtiene por iteración la siguiente generalización de la Proposición 2.11:

Proposición 3.27. *Sean $J_1, \ldots, J_n$ ideales de C, comaximales a pares. Entonces existe un isomorfismo de anillos*

$$\Phi : C \Big/ \left(\bigcap_{i=1}^{n} J_i\right) \xrightarrow{\cong} \prod_{i=1}^{n} C/J_i.$$

Demostración. El hecho de que J_1 sea comaximal con cada uno de los ideales $J_2, \ldots, J_n$ nos dice que es comaximal con su intersección $J = \bigcap_{i=1}^{n} J_i$. Se sigue que $C/(J_1 \cap J) \cong (C/J_1) \times (C/J)$ y se termina por inducción. □

De hecho, la comaximalidad permite remplazar intersecciones por productos.

Proposición 3.28. *Si I_1 e I_2 ideales comaximales de C, entonces $I_1 \cap I_2 = I_1 I_2$.*

Demostración. Claramente $I_1 \cap I_2 \supseteq I_1 I_2$. Sea $1 = u_1 + u_2$ con $u_1 \in I_1$ y $u_2 \in I_2$. Entonces todo elemento $a \in I_1 \cap I_2$ se escribe como $a = u_1 a + a u_2 \in I_1 I_2$. □

La proposición 2.11 tiene una conversa:

Proposición 3.29. *Si el homomorfismo Φ definido en (3.1) es epiyectivo, entonces I_1 e I_2 son comaximales.*

Demostración. Sea $I = I_1 \cap I_2$. Si Φ es epiyectivo, sean $a_2 + I$ y $a_1 + I$ las preimagenes de $(1 + I_1, 0 + I_2)$ y $(0 + I_1, 1 + I_2)$ en C/I respectivamente. Entonces $a_1 \in I_1$ y $a_2 \in I_2$. Además, $a_2 + I$ y $a_1 + I$ son idempotentes complementarios. En particular $a_1 + a_2 + I = 1 + I$. Se sigue que $1 \in a_1 + a_2 + I \subseteq I_1 + I_2 + I \subseteq I_1 + I_2$. □

Cuerpo de cocientes

El cuerpo $\mathbb{Q}$ de los números racionales se construye como el conjunto de todas las fracciones de la forma $\frac{m}{n}$ con m y n enteros con la convención de que $\frac{m}{n} = \frac{t}{s}$ si y sólo si $ms = nt$. Este procedimiento puede extenderse a un dominio de integridad arbitrario. De hecho, si D es un dominio de integridad, se define

$$\mathfrak{Quot}(D) = \{(a, b) | a, b \in D,\ b \neq 0\} / \equiv,$$

donde la relación de equivalencia $\equiv$ está dada por

$$(a, b) \equiv (c, d) \iff ad = bc.$$

La clase de equivalencia de (a, b) se denota $\frac{a}{b}$. En el conjunto $\mathfrak{Quot}(D)$ se definen operaciones de suma y multiplicación mediante

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Estas operaciones están bien definidas, lo que se comprueba con un cálculo directo. Por ejemplo, para la suma, si $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$, entonces

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

mientras que

$$\frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd' + b'c'}{b'd'},$$

pero

$$(ad + bc)b'd' - (a'd' + b'c')bd = (ab' - a'b)dd' - (cd' - c'd)bb' = 0.$$

Similarmente se prueba que la suma y el producto son asociativos, por ejemplo

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf},$$
$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf}.$$

Lo mismo se aplica a la ley distributiva. Además el elemento $\frac{0}{1}$ es un neutro aditivo y el elemento $\frac{1}{1}$ un neutro multiplicativo:

$$\frac{a}{b} + \frac{0}{1} = \frac{1a + 0b}{1b} = \frac{a}{b}, \qquad \frac{a}{b} \times \frac{1}{1} = \frac{1a}{1b}.$$

En particular $\mathfrak{Quot}(D)$ es un anillo. De hecho $\frac{a}{b} = \frac{0}{1}$ si y sólo si $a = 0$ y $\frac{a}{b} = \frac{1}{1}$ si y sólo si $a = b$. En particular, todo elemento no nulo del anillo $\mathfrak{Quot}(D)$ es de la forma $\frac{a}{b}$ con $a \neq 0$, luego $\frac{b}{a} \in \mathfrak{Quot}(D)$. Como $\frac{a}{b} \times \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$. El anillo $\mathfrak{Quot}(D)$ es un cuerpo. El dominio D se identifica con el subanillo de elementos de la forma $\frac{a}{1}$, de hecho

$$\frac{a}{1} + \frac{c}{1} = \frac{1a + 1c}{1 \times 1}, \qquad \frac{a}{1} \times \frac{c}{1} = \frac{ac}{1 \times 1},$$

y si $\frac{a}{1} = \frac{c}{1}$ entonces $a = c$.

Ejemplo 3.30. $\mathbb{Q} = \mathfrak{Quot}(\mathbb{Z})$.

Ejemplo 3.31. Un cuerpo es su propio cuerpo de cocientes.

Ejemplo 3.32. El anillo $K[X]$ de polinomios con coeficientes en un cuerpo K es un dominio de integridad, y su cuerpo de cocientes se denota $K(X)$. Este cuerpo recibe el nombre de cuerpo de funciones racionales con coeficientes en K. Sus elementos se escriben como cocientes de polinomios.

Ejercicios

1. Sea $A = \mathbb{M}_2(R)$. Sea
$$a = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$
Probar que $I = Aa$ es un ideal por la izquierda y que $J = aA$ es un ideal por la derecha (de modo que IJ es un ideal bilátero). Probar que IJ no está contenido en $I \cap J$ y que este último no es un ideal (por ningún lado).

2. Probar que $\mathfrak{R}(A \times B) = \mathfrak{R}(A) \times \mathfrak{R}(B)$ y $\mathfrak{N}(A \times B) = \mathfrak{N}(A) \times \mathfrak{N}(B)$.

3. sean m y n enteros. Probar que existe un único divisor positivo d de n tal que $(m + n\mathbb{Z})(\mathbb{Z}/n\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z}$. Probar que $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. Probar que d es un divisor común de n y m. Concluir que si m y n son relativamente primos, entonces la imagen de m en $\mathbb{Z}/n\mathbb{Z}$ es invertible.

4. Probar que si n y m son relativamente primos, entonces $m\mathbb{Z}$ y $n\mathbb{Z}$ son comaximales. Conchuir que $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

5. Probar que un anillo conmutativo finito sin elementos nilpotentes es un producto de cuerpos.

6. Probar que en un dominio de integridad, la intersección de dos ideales no nulos es no nula.

7. Sea C un anillo conmutativo que cumple las siguientes hipótesis:

   - C es un dominio de integridad.
   - C tiene un número finito de ideales maximales.

   Probar que $\mathfrak{R}(C) \neq \{0\}$.

8. Sea C un dominio de integridad que contiene a un cuerpo K como subanillo. Probar que si la K-dimensión de C es finita, entonces C es un cuerpo.

9. Sea C un anillo que contiene a un cuerpo K como subanillo. Probar que si la K-dimensión de C es finita, entonces todo ideal primo de C es maximal.

10. Sea C un anillo que contiene a un cuerpo K como subanillo. Probar que si la K-dimensión de C es finita, entonces todo elemento x con la propiedad de que $1 + xy$ es invertible para todo $y \in C$ es nilpotente.

11. Sea X un conjunto, y sea $\mathfrak{p}(X)$ la colección de todos los subconjuntos de X. Probar que $\mathfrak{p}(X)$ es un anillo conmutativo con las operaciones $AB = A \cap B$ y $A + B = (A - B) \cup (B - A)$. Probar que todo elemento de $\mathfrak{p}(X)$ es idempotente central. Pobar que para todo subconjunto A de X se tiene $\mathfrak{p}(X) \cong \mathfrak{p}(A) \times \mathfrak{p}(A^c)$.

12. Probar que si todo ideal maximal de $\mathfrak{p}(X)$ es principal, entonces X es finito.

13. Una colección $\mathfrak{A}$ de subconjuntos de X se llama un filtro si:

    (a) $A, B \in \mathfrak{A}$ implica $B \cap A \in \mathfrak{A}$.

    (b) $A \in \mathfrak{A}$ y $B \supseteq A$ implican $B \in \mathfrak{A}$.

    (c) $\emptyset \notin \mathfrak{A}$.

    El conjunto $C(\mathfrak{A})$ se define por:

    $$C(\mathfrak{A}) = \{B \subseteq X | B^c \in \mathfrak{A}\}.$$

    Probar que $\mathfrak{A}$ es un filtro si y sólo si $C(\mathfrak{A})$ es un ideal propio.

14. Utilizar el ejercicio precedente para probar que todo filtro está contenido en un ultrafiltro (filtro maximal).

15. Sea K un cuerpo, y sea $K[x]$ el anillo de polinomios con coeficientes en K. Pruebe que $K[x]$ es un dominio de integridad. El cuerpo de cocientes de este anillo recibe el nombre de cuerpo de funciones racionales.

Chapter 4

Dominios Euclideanos y Principales

En todo lo que sigue, D denotará un dominio de integridad. A menudo diremos sólamente un dominio, por brevedad. En este capítulo caracterizaremos algunos tipos de dominios que tienen una estructura similar al anillo de enteros, por lo que el estudio de estos anillos es similar a lo que se cubre usualmente en un curso bsico de teora de números (aritmtica).

definición 4.1. Sea D un dominio, y sea $g : D - \{0\} \to \mathbb{N}$ una función que satisface:

$$\forall m, n \in D \ \exists q, r \in D \text{ tal que } n = qm + r \text{ con } g(r) < g(m) \text{ o } r = 0.$$

Tal función g recibe el nombre de algoritmo de Euclides en D. Si tal función existe, se dice que D es un dominio euclideano (DE). La existencia de un algoritmo de Euclides en D tiene importantes consecuencias en su estructura.

Ejemplo 4.2. El anillo $\mathbb{Z}$ es un DE con la función $g(n) = |n|$. Por lo general se asume, en los cursos básicos de aritmética, que el resto debe positivo, pero esto no es necesario, y de hecho es más conveniente en ocasiones considerar restos negativos, como veremos luego.

Ejemplo 4.3. El anillo $\mathbb{Z}[i] \subseteq \mathbb{C}$ es un DE con la función $g(a+bi) = |a+bi| = a^2 + b^2$. De hecho, basta con ver que cada punto de $\mathbb{Q}[i]$ está a distancia menor a uno de un punto de $\mathbb{Z}[i]$, ya que si $m/n = q + \alpha$ con $g(\alpha) < 1$, entonces $m = qn + r$, donde $r = n\alpha$ satisface $g(r) < g(n)$. Por otro lado, de la representación gráfica de $\mathbb{Z}[i]$ como puntos del plano cartesiano con

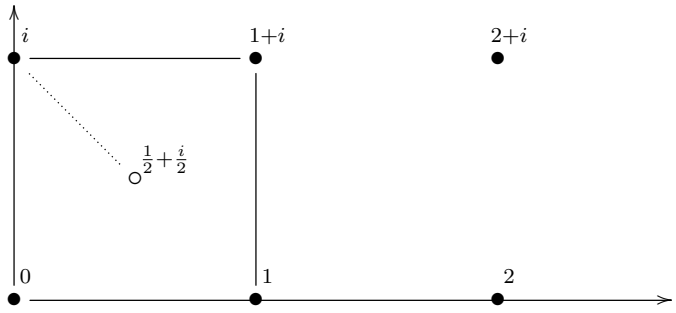


Figure 4.1: El punto mas lejano del conjunto de puntos reticulares $\mathbb{Z}[i]$.

coordenadas enteras, se obtiene que la mayor distancia a la que un complejo puede encontrarse de $\mathbb{Z}[i]$ es $\sqrt{2}$, que es la distancia de un vértice, diganos i, del cuadrado de vértices $\{0, 1, i, 1+i\}$, al centro del mismo, como se observa en la Figura 5.1.

Ejemplo 4.4. El anillo de polinomios $\mathbb{R}[x]$, es un DE con la función $g(f(x)) = \deg(f)$. Más generalmente, si k es un cuerpo arbitrario, el conjunto de polinomios con coeficientes en k, es decir

$$k[x] = \{ax^n + \ldots + a_1x + a_0 | n \in \mathbb{Z}_{\geq 0},\ a_n, \ldots, a_0 \in k\},$$

es un anillo con las operaciones usuales. Este anillo es un DE con el grado como algoritmo de Euclides. De hecho, para todo par de polinomios f y g con $\deg(f) = n \geq m = \deg(g)$ podemos escribir

$$f(x) = a_nx^n + \ldots + a_0, \qquad g(x) = b_mx^m + \ldots + b_0,$$

de donde $f(x) = g(x)(a_n/b_n)x^{n-m} + f_0(x)$ con $\deg(f_0) < \deg(f)$ por lo que el resultado se obtiene por inducción en el grado de f. Simplemente iteramos este proceso, restando siempre múltiplos de g hasta obtener un polinomio de grado inferior a g.

Proposición 4.5. *En un DE todo ideal es principal.*

Demostración Sea I un ideal en el dominio euclideano D. Sea $m \in I$ tal que $g(m)$ en minimal. Sea $n \in I$ arbitrario. Entonces $n = mq + r$ con

$g(r) < g(m)$ o $r = 0$. Por definición de m, la alternativa $g(r) < g(m)$ es imposible, por lo que solo puede ser $r = 0$, es decir $m|n$. Como $n \in I$ es arbitrario, $I = (m)$. □

definición 4.6. Un dominio de integridad D donde cada ideal es principal recibe el nombre de dominio de ideales principales (DIP). En un DIP, para todo par de elementos n y m el ideal $I = (m) + (n)$ es un ideal principal. Un generador d de I recibe el nombre de máximo común divisor de m y n.

Dados elementos m y n en D, diremos que m divide a n o que m es un divisor de n, en simbolos $m|n$, si existe $t \in D$ tal que $n = mt$. En particular $m|n$ si y sólo si $(n) \subseteq (m)$. Dado que el máximo común divisor d de m y n satisface $(d) = (n) + (m)$, existen r y s en D tales que $d = rn + ms$. Concluimos que todo divisor común de n y m debe dividir a d. Por otro lado, como (d) contiene a (m) y (n), se tiene que d es efectivamente un divisor común de m y n en el sentido queacabamos de definir, de allí su nombre.

En el caso de un DE, existe un algoritmo sencillo para encontrar el máximo común divisor de dos números n y m, así como para escribirlo como una combinación del tipo $nu+mv$. Para ello, dividimos n por m obteniendo:

$$n = q_0 m + r_0,$$

con $g(r_0) < g(m)$. A continuación dividimos de nuevo e iteramos

$$m = q_1 r_0 + r_1,\ r_0 = q_2 r_1 + r_2, \ldots, r_i = q_{i+2} r_{i+1} + r_{i+2}, \ldots$$

con $g(r_0) > g(r_1) > \ldots$.

Proposición 4.7. *En este algorithmo, el último resto distinto de* 0 *que se obtiene es el máximo común divisor.*

Demostración Observemos primero que $g(m) > g(r_0) > g(r_1) > \ldots$ es una cadena decreciente de números naturales, por lo que el procedimiento siempre termina, es decir, debe llegarse eventualmente a un resto $r_{k+1} = 0$.

Por simplicidad, escribimos $(n, m) = (n) + (m)$. Como $n - q_0 m = r_0$ y $n = q_0 m + r_0$, se tiene que $r_0 \in (n, m)$ y $n \in (m, r_0)$. Concluimos que $(n, m) = (m, r_0)$. El mismo argumento prueba la cadena de identidades:

$$(n, m) = (m, r_0) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = (r_k, 0) = (r_k).$$

Concluimos que r_k es el máximo común divisor. □

Para encontrar u y v tales que $r_k = um + vn$, lo escribimos en forma iterada como $r_k = u_t r_{t-2} + v_t r_{t-1}$, donde adoptamos la convención de que $m = r_{-1}$ y $n = r_{-2}$. Partimos escribiendo $u_{k+1} = 0$, $v_{k+1} = 1$, y calculamos hacia atras mediante la recurrencia

$$u_{t-1} = v_t, \qquad v_{t-1} = u_t - v_t q_{t-1},$$

hasta llegar a $u = u_0$ y $v = v_0$.

Ejemplo 4.8. Calcularemos el maximo común divisor de 148 y 256. Comenzamos dividiendo 256 por 148.

$$256 = 1 \times 148 + 108.$$

A continuacuón dividimos el divisor por el resto, e iteramos:

$$148 = 1 \times 108 + 40,\ 108 = 2 \times 40 + 28,\ 40 = 1 \times 28 + 12,$$

$$28 = 2 \times 12 + 4,\ 12 = 3 \times 4 + 0.$$

El último resto distinto de 0 es el máximo común divisor, es decir 4. Para encontrar u y v, ponemos la información obtenida en una tabla como sigue:

t	q_t	r_t	u_t	v_t
0	1	108		
1	1	40		
2	2	28		
3	1	12		
4	2	4		
5	3	0		

.

Escribimos 0 y 1 en la última fila como condición inicial:

t	q_t	r_t	u_t	v_t
0	1	108		
1	1	40		
2	2	28		
3	1	12		
4	2	4		
5	3	0	0	1

.

A continuación rellenamos las últimas dos columnas en sentido inverso utilizando la recurrencia:

t	q_t	r_t	u_t	v_t
0	1	108	11	-19
1	1	40	-8	11
2	2	28	3	-8
3	1	12	-2	3
4	2	4	1	-2
5	3	0	0	1

.

Constatamos finalmente que $4 = 11 \times 256 - 19 \times 148$.

Ejemplo 4.9. El anillo $\mathbb{Z}$ es un DE con la función $g(n) = |n|$. Por lo general se asume que el resto debe positivo, pero esto no es necesario. De hecho, admitiendo restos negativos se obtiene un algoritmo mucho mas eficiente para calcular el maximo común divisor, puesto que puede requerirse $|r| < \Big[|n/2|\Big]$. En el caso precedente obtenemos:

$$256 = 2 \times 148 - 40, \quad 148 = (-4)(-40) - 12,$$

$$-40 = 3(-12) - 4, \quad -12 = (3)(-4),$$

lo que nos dá la tabla

t	q_t	r_t	u_t	v_t
0	2	-40	-11	19
1	-4	-12	-3	-11
2	3	-4	1	-3
3	3	0	0	1

.

La diferencia de signo se debe a que este cálculo produce el máximo común divisor -4 en vez de 4.

definición 4.10. Sea D un dominio de integridad. Sean $n, n' \in D$. Diremos que n' es asociado de n, si $n'|n$ y $n|n'$. Equivalentemente, dos elementos, n y n' son asociados si y sólo si $(n) = (n')$. Observese que si $n = tn'$ y $n' = t'n$ entonces $tt' = 1$. Se concluye que dos elementos, n y n' son asociados si y sólo si existe $u \in D^*$ tal que $n' = un$. Los asociados de 1 son las unidades de D.

definición 4.11. Sea D un dominio de integridad. Sea $p \in D - \{0\}$. El elemento p se dice primo, si para todo par de lementos a y b en D, $p|ab$ implica $p|a$ o $p|b$. Equivalentemente, $p \neq 0$ es primo si y sólo si el ideal (p) es primo. En particular, todo asociado de un primo es un primo.

Proposición 4.12. *Sea D un DIP. Un elemento $p \in D$ es primo si y sólo si (p) es maximal.*

Demostración. Si (p) es maximal, en particular es primo. Por otro lado, si (p) no es maximal, entonces está propiamente contenido en un ideal maximal (p'). En particular, p' divide a p. Se sigue que $p = tp'$, y como p no divide a p', pues p y p' no son asociados dado que la contención es propia, p debe dividir a t. Luego $t = ps$, de donde $sp' = 1$ y p es una unidad, pero esto es imposible ya que (p') es un ideal propio de D. □

Proposición 4.13. *Todo elemento de un DIP D que no es una unidad es divisible por un elemento primo.*

Demostración. Esto es inmediato ya que todo ideal está contenido en un ideal maximal. □

Proposición 4.14. *En un DIP D, cada elemento no nulo es producto de primos y unidades.*

Demostración. Por la proposición precedente, en un DIP todo elemento $n \notin D^*$ puede escribirse en la forma $n = p_1 n_1$. Si n_1 no es una unidad podemos repetir el proceso y escribir $n = p_1 p_2 n_2$. Iterando, si el algún momento se llega a algún $n_r \in D^*$, se habrá escrito n como producto de primos y unidades. En principio, la otra alternativa sería obtener una cadena infinita estrictamente ascendente de ideales

$$(n) \subset (n_1) \subset (n_2) \subset \dots.$$

Afirmamos que esto no puede ocurrir. Para ello definimos el conjunto

$$I = \{a \in D | n_t \text{ divide a } a \text{ para algún } t \in \mathbb{N}\} = \bigcup_{t \in \mathbb{N}} (n_t).$$

Este conjunto es un ideal por ser la unión de una cadena de ideales. Como D es un DIP, necesariamente se tiene $I = (d)$ para algún elemento $d \in D$.

En particular, $d \in I$, por lo que debe ser divisible por algún elemento n_t, de donde $n_{t+1} \in I = (d) \subseteq (n_t)$, lo que contradice el hecho de que la cadena es estrictamente ascendente. □

La descomposición de un elemento n no es única, dado que siempre es posible remplazar un primo por uno de sus asociados y cambiar las unidades. Por ejemplo, en $\mathbb{Z}$ se tiene

$$4 = 2 \times 2 = (-2) \times (-2) = (-1) \times 2 \times (-2).$$

Sin embargo, esta es la única excepción. Antes de demostrarlo necesitamos un lema.

Lema 4.15. *Si p y q son primos del DIP D, y si p divide a q, entonces p y q son asociados.*

Demostración. Si p divide a q entonces $(q) \subseteq (p)$. Por otro lado, el ideal (q) es maximal. Se concluye que $(q) = (p)$. □

Proposición 4.16. *Sea D un DIP. Sea*

$$n = up_1^{\alpha_1} \dots p_r^{\alpha_r} = vq_1^{\beta_1} \dots q_s^{\beta_s}, \tag{4.1}$$

donde $p_1, \dots, p_r$ son primos no asociados por pares y lo mismo ocurre con $q_1, \dots, q_s$. Entonces $s = r$, y existe una permutación σ de $\mathbf{r} = \{1, \dots, r\}$ tal que p_i es asociado a $q_{\sigma(i)}$ y $\alpha_i = \beta_{\sigma(i)}$.

Demostración. Por inducción en r. Si $r = 0$, entonces n es una unidad y no hay nada que probar. Supongamoslo cierto para $r = t - 1$ y lo probaremos para $r = t$. Como p_t es primo debe dividir a algún q_j y por lo tanto ser asociado a él. reenumerando $q_1, \dots, q_s$ si es necesario, podemos suponer que $j = s$. Digamos $q_s = wp_r$ con $w \in D^*$. Entonces simplificando en (4.1) se tiene

$$up_1^{\alpha_1} \dots p_r^{\alpha_r - 1} = (vw^{-1})q_1^{\beta_1} \dots q_s^{\beta_s - 1}.$$

Si $\alpha_r > 1$, el lado izquierdo es aún divisible por p_1 por lo que tambien lo es el derecho. Se concluye que $\beta_s > 1$. Iterando este procedimiento se tiene $\alpha_r = \beta_s$. simplificando $p_r^{\alpha_r}$ a ambos lados se tiene:

$$up_1^{\alpha_1} \dots p_{r-1}^{\alpha_{r-1}} = (vw^{-r})q_1^{\beta_1} \dots q_{s-1}^{\beta_{s-1}},$$

por lo que se puede aplicar la hipótesis de inducción. Esto concluye la prueba. □

Teorema Chino de los Restos (tercera versión).

En el caso en que $C = D$ es un DIP, es posible dar una sencilla caracterización de los ideales comaximales.

Proposición 4.17. *Sea D un DIP, y sean m y n dos elementos de D. Entonces las siguientes condiciones son equivalentes:*

i) (n) y (m) son comaximales.

ii) n y m son relativamente primos, es decir, no tienen divisores comunes.

iii) No existe ningún primo que divida simultáneamente a n y a m.

Demostración Es claro que (ii) implica (iii). Si r es un divisor común, entonces $(n) \subseteq (r)$ y también $(m) \subseteq (r)$, de donde $(n) + (m) \subseteq (r)$, lo que contradice (i), luego (i) implica (ii). Finalmente, si $(m) + (n)$ no es (1), debe estar contenido en un ideal maximal, el cual debe ser de la forma (p) con p primo, luego p divide a m y n. Así (iii)implica (i). □

Esto implica que el teorema chino de los restos adopta la siguiente forma:

Proposición 4.18. *Sea D un DIP Sean $m_1, \ldots, m_n$ elementos de D, relativamente primos a pares. Entonces existe un isomorfismo de anillos*

$$\Phi : D/(m_1 \ldots m_n) \xrightarrow{\cong} \prod_{i=1}^{n} D/(m_i). \quad \square$$

En otras palabras:

Proposición 4.19. *Sea D un DIP Sean $m_1, \ldots, m_n$ elementos de D, relativamente primos a pares. Entonces, dados $a_1, \ldots, a_n \in D$ existe $b \in D$ tal que $b \equiv a_i \pmod{m_i}$ para $i = 1, \ldots, n$. Dos soluciones cualesquiera son congruentes módulo $m_1 \ldots m_n$.*

Este es el resultado conocido normalmente como teorema chino de los restos.

Ejemplo 4.20. Considerese el polinomio f que tiene la descomposición $f(x) = up_1(x)^{\alpha_1} \ldots p_n(x)^{\alpha_n}$ en el anillo de polinomios $K[x]$, donde K es un cuerpo. El anillo cociente definido por f tiene la estructura dada por:

$$k[x]/\Big(f(x)\Big) \cong \prod_{i=1}^{n} k[x]/\Big(p_i(x)^{\alpha_i}\Big).$$

en particular, si $f(x)$ es libre de cuadrados el k-álgebra $k[x]/\Big(f(x)\Big)$ es un producto de cuerpos.

Evaluación de polinomios y el polinomio minimal

Sea K un cuerpo y sea A un anillo arbitrario tal que K está contenido en el centro $Z(A)$ de A. Entonces, para todo elemento $a \in A$ existe un único homomorfismo de anillos $\phi_a : K[x] \to A$ tal que, para todo elemento $\alpha \in K$ se tiene $\phi_a(\alpha) = \alpha$, mientras que $\phi_a(x) = a$. Este homomorfismo se define, para todo polinomio $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x + \alpha_0$, mediante la fórmula siguiente:

$$\phi_a\Big(f(x)\Big) = \alpha_n a^n + \alpha_{n-1}a^{n-1} + \ldots + \alpha_1 a + \alpha_0.$$

Este homomorfismo recibe el nombre de evaluación en a. El elemento $\phi_a(f)$ es usualmente denotado $f(a)$.

El núcleo $\ker(\phi_a)$ es un ideal de $K[x]$, y por lo tanto es principal. Su generador mónico $m_a(x) = m_{K,a}(x)$ recibe el nombre de polinomio minimal de a. Se sigue de la definición que $m_a(a) = 0$ y que $f(a) = 0$ si y sólo si $f(x)$ es divisible por $m_a(x)$. Nótese que si $K \subset L \subseteq Z(A)$ con L y K cuerpos, el anillo de polinomios $K[x]$ puede verse como un subanillo de $L[x]$. Viendo a $m_{K,a}(x)$ como elemento de $L[x]$, la ecuación $m_{K,a}(a) = a$, nos dice que $m_{K,a}(x)$ es divisible por el polinomio minimal sobre L, el cual denotamos $m_{L,a}(x)$. En general $m_{K,a}(x) \neq m_{L,a}(x)$. Por ejemplo, si $A = L$, todo elemento $a \in L$ tiene el polinomio minimal $m_{L,a}(x) = x - a$ (ya que ninguna constante se anula al evaluar), pero este sólo puede coincidir con su polinomio minimal sobre K si $a \in K$. Si $m_{K,a}(x) = 0$, diremos que a es trascendente sobre K. Este concepto es utilizado especialmente en el caso de cuerpos.

Supongamos ahora que a no es trascendente. Nótese que por el algoritmo de división, $m_{K,a}(x)$ puede caracterizarse como el polinomio con coeficientes en K de menor grado que se anula al evaluarlo en a. La imagen de $K[x]$ en A bajo el homomorfismo de evaluación en a se denote $K[a]$. El primer teorema de isomorfía nos dice que

$$K[a] \cong K[x]/(m_{K,a}).$$

Este es un espacio vectorial sobre K de dimensión $\deg(m_{K,a})$.

Ejemplo 4.21. Si $a \in K$, entonces $K[a] = K$, por lo que se tiene el isomorfismo $K[x]/(x - a) \cong K$.

Ejemplo 4.22. Si $i \in \mathbb{C}$ tiene el significado usual, entonces $m_{\mathbb{R},i}(x) = x^2+1$. Por otro lado $m_{\mathbb{C},i}(x) = x - i$. Nótese que $x^2 + 1 = (x - i)(x + i)$. También se tiene $\mathbb{R}[i] = \mathbb{C}$.

Algebras sobre cuerpos

Dado un anillo conmutativo C, un álgebra sobre C, o una C-álgebra, es un anillo A junto con un homomorfismo $\phi : C \to A$ tal que $\phi(C)$ está contenido en el centro $Z(A)$ del álgebra A. Si $C = k$ es un cuerpo, la función ϕ es automáticamente inyectiva y por lo tanto el anillo A tiene un subanillo $\phi(k) \subseteq Z(A)$ isomorfo a k. Podemos identificar a k con su imagen en A. De acuerdo a los resultados de la sección anterior, para cada elemento a de A existe un homomorfismo $\phi_a : k[x] \to A$ llamado evaluación en a que extiende ϕ y satisface $\phi(x) = a$. El elemento $\phi_a[f(x)]$ se denota simplemente $f(a)$. La imagen del homomorfismo ϕ_a es el álgebra $k[a] \cong k[x]/(m_a)$ donde m_a es el polinomio minimal de a. El álgebra A es un espacio vectorial sobre k. Si su dimensión es finita, necesariamente $m_a \neq 0$, puesto que $k[a] \cong k[x]$ para un elemento trascendente, y el anillo de polinomios tiene dimensión infinita como espacio vectorial sobre k.

Sea $a \in A$. La función $T_a : A \to A$, definida por $T_a(b) = ab$ es K-lineal. De hecho define un homomorfismo de A en el anillo de endomorfismos $\mathrm{End}_K(A)$. Si A tiene dimensión finita, la función lineal T_a tiene un determinante y una traza bien definidos. Escribimos

$$N(a) = \det(T_a) \qquad \mathrm{Tr}(a) = \mathrm{tr}(T_a).$$

Es inmediato, de las propedades elementales del determinante y la traza de matrices, que $N(ab) = N(a)N(b)$ y que Tr es una función lineal que satisface $\mathrm{Tr}(ab) = \mathrm{Tr}(ba)$.

Proposición 4.23. *En cualquier K-álgebra de dimensión finita A, las siguientes afirmaciones son equivalentes:*

1. $N(a) \neq 0$
2. *La función lineal T_a es inyectiva.*
3. *La función lineal T_a es epiyectiva.*
4. $a \in A^*$.
5. $ab \neq 0$ *para todo b en A.*

Demostración. Se sigue de las propiedades elementales de los determinantes que (1)-(3) son equivalentes. Es inmediato de la definición de T_a que (2) y (5) son equivalentes. Finalmente, probaremos la equivalencia de las otras afirmaciones con (4). Si $ab = 1$, entonces $1 = N(ab) = N(a)N(b)$, por lo que (4) implica (1). Por otro lado, si T_a es epiyectiva, entonces $ab = 1$ para algún $b \in A$. Se sigue que $T_a \circ T_b = \mathrm{Id}$, de donde, dado que T_a y T_b son funciones lineales en un espacio vectorial de dimensión finita, son inversas y se tiene $T_b \circ T_a = \mathrm{Id}$. Evaluando ambos lados de esta identidad en 1 se tiene $ba = 1$, por lo que b es el inverso de a. Esto prueba que (3) implica (4). □

Ejercicios

1. Encuentre el máximo común divisor, en $\mathbb{Z}$, de 1492 y 2016.

2. Encuentre el máximo común divisor, en $\mathbb{Z}[i]$, de $14 + 12i$ y $9 + 15i$.

3. Encuentre el máximo común divisor $d(x) \in \mathbb{R}[x]$, de $4x^2+x+1$ y x^5+4. Encuentre polinomios $s(x)$ y $t(x)$ tales que

$$(4x^2 + x + 1)s(x) + (x^5 + 4)t(x) = d(x).$$

4. Juan debe pagar 7.000 pesos por un reloj. Tanto el como el relojero disponen de un número grande de billetes de 17.000 y 23.000 pesos. Determine como debe realizarse la transacción.

5. Demuestre que $2+i$ y $2-i$ son relativamente primos en $\mathbb{Z}[i]$. Utilice este resultado para probar que el caballo puede llegar de cualquier casilla de un tablero de ajedrez infinito a cualquier otra (ver figura 5.2A).

6. Repita el ejercicio anterior para un caballo que se mueve en un tablero hexagonal, como el mostrado en la Figura 5.2B.

7. Generalice los dos ejercicios anteriores a caballos que pueden moverse n casillas en una dirección, y luego m casillas en una dirección diferente. Que condiciones en m y n aseguran que pueda cubrirse todo el tablero?

8. Probar que $\mathbb{Z}[\sqrt{-2}]$ es un dominio euclideano.

9. Sea $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ la raiz cúbica de la unidad de parte imaginaria positiva. Probar que $\mathbb{Z}[\omega]$ es un dominio euclideano.

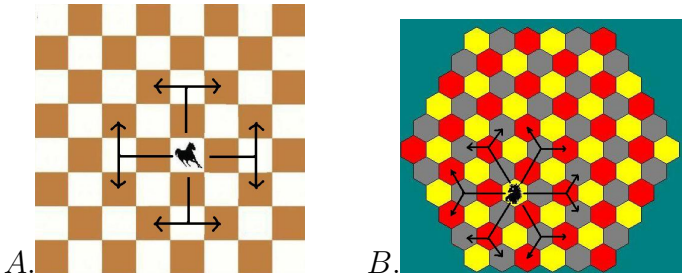


Figure 4.2: El caballo y sus movimientos (A) y Un tablero hexagonal (B).

10. Sea $D = \mathbb{Z}[\sqrt{-5}]$. Probar que en D el ideal $(3, 4+\sqrt{-5})$ no es 1, pero 3 y $4+\sqrt{-5}$ no tienen ningún divisor común. Probar que D no es un dominio euclideano. Sugerencia: Probar que la norma $N(a+b\sqrt{-5}) = a^2 + 5b^2$ es multiplicativa y que no hay elementos z que satisfacen $3 = N(z)$.

11. Sean $\lambda_1, \ldots, \lambda_n$ elementos distintos de un cuerpo K. Sea $f(x) = (x - \lambda_1)\cdots(x - \lambda_n)$. Encuentre polinomios $g_1, \ldots, g_n$ cuyas proyecciones a $K[x]/(f)$ sean los idempotentes centrales minimales de ese anillo. Sugerencia: considere los polinomios $h_i = f/(x-\lambda_i)$ y sus proyecciones en cada cociente.

12. Probar que si K es un cuerpo, y si $\alpha_1, \ldots \alpha_n$ son elementos distintos de K, entonces para todo $\beta_1, \ldots \beta_n \in K$, existe un polinomio $f(x) \in K[x]$, de grado menor a n, tal que $f(\alpha_i) = \beta_i$ para $i = 1, \ldots, n$.

13. Utilizar el algoritmo de división para encontrar el m.c.d. d de $7 - 5\omega$ y $12 + 11\omega$ en $\mathbb{Z}[\omega]$. Exprese d en la forma $d = s(7 - 5\omega) + t(12 + 11\omega)$ con s y t en $\mathbb{Z}[\omega]$.

14. Encontrar polinomios $s(x)$ y $t(x)$, con $\deg s(x) \leq 2$ y $\deg t(x) \leq 1$, tales que
$$\frac{s(x)}{x^3 - 1} + \frac{t(x)}{x^2 + 2} = \frac{1}{(x^3 - 1)(x^2 + 2)}.$$

15. Encontrar enteros a, b, c, y t con $0 \leq a \leq 16$, $0 \leq b \leq 10$, y $0 \leq c \leq 12$,

tales que

$$t + \frac{a}{17} + \frac{b}{11} + \frac{c}{13} = \frac{23}{11 \cdot 13 \cdot 17}.$$

16. Probar que en cualqueir anillo conmutativo C y para elementos cualesquiera x e y en C se tiene $f(x+y) \equiv f(x) + f'(x)y \ (\mathrm{mod} y^2)$, donde $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$ si $f(x) = \sum_{i=1}^{n} a_i x^i$.

17. Probar que si D es un DIP, p un primo de D, $t \in D$, $n \in \mathbb{Z}$, y si

$$\underbrace{1_D + \ldots + 1_D}_{n \text{ veces}} \notin (p),$$

entonces, para cada entero positivo s, existe una única solución en $D/(p^s)$ de la ecuación $x^n = \overline{1 + pt}$, que satisface $x \equiv 1 \pmod{p}$.

Chapter 5

Introducción a la Teoría de Cuerpos

Sea K un cuerpo arbitrario. Sea $\phi : \mathbb{Z} \to K$ el único homomorfismo, es decir el que lleva a n en

$$\underbrace{1_k + \ldots + 1_k}_{n \text{ times}}.$$

La imagen de ϕ es un dominio de integridad. Por el primer teorema de isomorfía, es a la vez isomorfa a un cociente de $\mathbb{Z}$. Luego debe ser isomorfo a $\mathbb{Z}$ o a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ para algún primo p. En el primer caso diremos que K tiene característica 0. En el segundo, que la característica es p.

Sean K y L dos cuerpos y sea $\phi : K \to L$ un homomorfismo de anillos no trivial. Entonces $\ker(\phi)$ es un ideal de K, luego sólo puede ser 0. Se concluye que todo homomorfismo de cuerpos es inyectivo y por lo tanto K puede identificarse a un subcuerpo de L. En particular, K y L tienen la misma característica. Nótese que esta identificación depende de ϕ. Si K es un subcuerpo de L diremos que L es una extensión de K o que L/K es una extensión de cuerpos. Nótese que L es un espacio vectorial sobre K. El grado $[L : K]$ de la extensión está definido por $[L : K] = \dim_K L$. En estos apuntes, consideraremos el grado como un elemento de $\mathbb{N} \cup \{\infty\}$, aunque es posible discriminar entre extensiones infinitas utilizando la teoría de cardinales infinitos. Diremos, en lo sucesivo que la extensión L/K es finita si su grado es un elemento de $\mathbb{N}$. En lo sucesivo, adoptaremos las convenciones comunes referentes a la dimensión infinita como $a\infty = \infty\infty = \infty$.

Proposición 5.1. *Si $F \subseteq K \subseteq L$ son cuerpos entonces se tiene la identidad*

$$[L : F] = [L : K][K : F].$$

Demostración Sea B una base de L como espacio vectorial sobre K y sea A una base de K como espacio vectorial sobre F. Basta probar que el conjunto $\{ab|a \in A, b \in B\}$ es una base de L sobre F. Probamos primero que generan. Sea $\alpha \in L$. Como B es base de L como sobre K, existen $b_1, \ldots, b_t \in B$ y $x_1, \ldots, x_t \in K$ tales que $\alpha = \sum_{i=1}^{t} x_i b_i$. Como cada x_i está en K, existen $a_{i1}, \ldots, a_{ir_i} \in A$ y $y_{i1}, \ldots, y_{ir_i} \in F$ tales que $x_i = \sum_{j=1}^{r_i} y_{ij} a_{ij}$. Se concluye que

$$\alpha = \sum_{i=1}^{t} \sum_{j=1}^{r_i} y_{ij}(a_{ij} b_i),$$

de donde se tiene lo pedido. Para la independencia lineal se observa que toda combinación lineal de elementos ab puede escribirse en la forma

$$\sum_{i=1}^{t} \sum_{j=1}^{r} y_{ij}(a_i b_j),$$

donde se han agregado coeficientes nulos de ser necesario. Si

$$\sum_{i=1}^{t} \sum_{j=1}^{r} y_{ij}(a_i b_j) = 0,$$

podemos escribir

$$\sum_{j=1}^{r} \left(\sum_{i=1}^{t} y_{ij} a_i \right) b_j = 0,$$

donde el término entre paréntesis está en K de donde por la independencia lineal de B sobre K se tiene

$$\sum_{i=1}^{t} y_{ij} a_i = 0,$$

y por a independencia lineal de A sobre F se tiene finalmente $y_{ij} = 0$. □

Ejemplo 5.2. $[\mathbb{C} : \mathbb{R}] = 2$ ya que $\{1, i\}$ es una base de $\mathbb{C}$ sobre $\mathbb{R}$.

Ejemplo 5.3. Si $p(x)$ es un polinomio primo en $K[x]$ de grado n, que podemos suponer mónico, entonces el ideal (p) es maximal en este anillo y se tiene que $L = K[x]/(p)$ es un cuerpo. Si se identifica K con su imágen en L, podemos considerar a L como una extensión de K. Como todo elemento del cociente se escribe de manéra única como un polinomio en $\overline{x}$ de grado a lo más $n-1$ (por el algoritmo de la división), se tiene que $[L : K] = n$.

El ejemplo anterior es muy importante por la siguiente razon. Si L/K es cualquier extensión y si $\alpha \in L$, entonces $K[\alpha] \cong K[x]/(m_{\alpha,K})$, donde $m_{\alpha,K}$ es el polinomio minimal de α en K. Como $K[\alpha]$ está contenida en un cuerpo debe ser un dominio de integridad, por lo que $m_{\alpha,K}$ debe ser primo o 0. En este caso, el polinomio $m_{\alpha,K}(x)$ se denomina el polinomio irreducible de α sobre K y se denota también $\mathrm{irr_K}(\alpha, \mathrm{x})$.

Si $m_{\alpha,K}(x) = 0$ se dice que α es trascendente sobre K y se tiene $K[\alpha] \cong K[x]$. Si $m_{\alpha,K}$ es un polinomio primo, el anillo $K[\alpha]$ es un cuerpo y $[K[\alpha] : K] = \deg(m_{\alpha,K})$. En este caso se dice que α es algebraico sobre K.

Ejemplo 5.4. Sean $K \subseteq L$ cuerpos. Un elemento α de L está en K si y sólo si $\deg(\mathrm{irr}_K(\alpha, x)) = 1$.

Ejemplo 5.5. Sea $a \in L$ un elemento que satisface $a^2 \in K$ pero $a \notin K$ entonces el polinomio irreducible de a sobre K es $x^2 - a$.

Ejemplo 5.6. Si L/K es una extensión cuadrática, es decir $[L : K] = 2$, entonces para cada elemento α de L que no esté en K se tiene $L = K[\alpha]$, siendo el polinomio irreducible de α un polinomio de la forma $x^2 + ax + b$. Además, si la característica no es 2, entonces 2 es invertible en K, y por lo tanto el elemento $\beta = x - \frac{a}{2}$ satisface que $\beta^2 \in K$ pero $\beta \notin K$. Se concluye que toda extensión cuadratica sobre un cuerpo de característica distinta de 2 tiene esta forma.

Ejemplo 5.7. Más generalmente, si L/K es una extensión de grado primo, es decir $[L : K] = p$, entonces para cada elemento α de L que no esté en K se tiene $L = K[\alpha]$.

Ejemplo 5.8. Si un polinomio cúbico $f(x) \in K[x]$ no tiene raices en K (y por lo tanto no tiene factores lineales en $K[x]$) entonces es irreducible. En particular toda raiz $\alpha \in L$ de un tal polinomio satisface $[K[\alpha] : K] = 3$.

Ejemplo 5.9. El polinomio $x^4 + 4$ no tiene raices en $\mathbb{Q}$ pero se factoriza como un producto de polinomios cuadráticos irreducibles

$$x^4 + 4 = (x^2 + 2)^2 - (2x)^2 = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

Ejemplo 5.10. $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. En particular, cada elemento de $\mathbb{Q}[\sqrt[3]{2}]$ se escribe de manéra única de la forma $a + b\sqrt[3]{2} + c\sqrt[3]{4}$.

Ejemplo 5.11. Si la extensión L/K es finita y si $\alpha \in L$, entonces el grado de $\mathrm{irr}_K(\alpha, x)$ debe dividir a $[L : K]$, ya que

$$[L : K] = [L : K(\alpha)][K(\alpha) : K].$$

Extensiones algebraicas y clausura algebraica

Recordemos que α es algebraico sobre K si y sólo si α satisface un polinomio no nulo con coeficientes en K o equivalentemente, si $K[\alpha]$ tiene dimensión finita como espacio vectorial sobre K. Es claro de la definición que si α es algebraico sobre K y si F es un subcuerpo de L que contiene a K entonces α es algebraico sobre F.

definición 5.12. Una extensión L/K se dice algebraica si todo elemento de L es algebraico sobre K.

Se sigue de la definición que una extensión L/K es algebraica si y sólo si para todo α en L, la extensión $K[\alpha]/K$ es finita. Por lo tanto, es inmediato que toda extensión finita es algebraica.

Proposición 5.13. *Sea $L = K[\alpha_1, \ldots, \alpha_r]$. Si cada α_i es algebraico sobre K entonces L/K es finita, En particular, L/K es algebraica.*

Demostración Para $i = 1, \ldots, r$ definimos $L_i = K[\alpha_1, \ldots, \alpha_i]$. Si α_i es algebraico sobre K entonces es algebraico sobre L_{i-1} de donde $[L_i : L_{i-1}] = [L_{i-1}[\alpha_i] : L_{i-1}] < \infty$. Por la multiplicatividad del grado e inducción se obtiene lo pedido. □

Corolario 5.13.1. *Si $\alpha, \beta \in L$ son algebraicos sobre un cuerpo $K \subseteq L$, también lo son $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ y, si además $\beta \neq 0$, también lo es el cociente α/β.*

Demostración Basta ver que todos los elementos mencionados en este corolario pertenecen a la extensión finita $K[\alpha, \beta]$ de K. □

El siguiente resultado es ahora inmediato:

Proposición 5.14. *Si L/K es una extensión, el conjunto*

$$L_{\text{alg}} = \{\alpha \in L | \alpha \text{ es algebraico sobre } K\}$$

es un subcuerpo de L. □

El cuerpo L_{alg} recibe el nombre de clausura algebraica de K en L.

Proposición 5.15. *Si $K \subseteq F \subseteq L$ son cuerpos tales que F/K es algebraica y $\alpha \in L$ es algebraico sobre F entonces es algebraico sobre K.*

Demostración Si α satisface un polinomio $f(x) = a_n x^n + \ldots + a_1 x + a_0$ con coeficientes en F entonces es algebraico sobre $F' = K[a_0, \ldots, a_n]$. Como $[F' : K] < \infty$ por la proposición anterior, se tiene que

$$[F'[\alpha] : K] = [F'[\alpha] : F'][F' : K] < \infty$$

y por lo tanto $F'[\alpha]/K$ es algebraica y en particular α es algebraico sobre K. □

En particular, se concluye que si L/F y F/K son extensiones algebraicas, entonces L/K es algebraica.

Un cuerpo K se dice algebraicamente cerrado si todo polinomio en $K[x]$ tiene una raiz en K. Equivalentemente, K es algebraicamente cerrado si y sólo si todo polinomio en $K[x]$ tiene un divisor lineal $x - \alpha$. Esto es equivalente a decir que los únicos polinomios primos en $K[x]$ son múltiplos escalares de polinomios de la forma $x - \alpha$. En particular, todo polinomio $f(x) \in K[x]$ se escribe de la forma $f(x) = \lambda \prod_{i=1}^{t} (x - \alpha_i)^{r_i}$. Los elementos $\alpha_1, \ldots, \alpha_t$ son las raices del polinomio y los exponentes $r_1, \ldots, r_t$ son sus multiplicidades. Si K es algebraicamente cerrado y L/K es cualquier extensión, se tiene necesariamente que $L_{\text{alg}} = K$ (ejercicio).

definición 5.16. Una clausura algebraica de un cuerpo K es una extensión algebraica L/K tal que L es algebraicamente cerrado.

Probaremos ahora la existencia de al menos una clausura algebraica de un cuerpo dado. Esta demostración requiere ciertos conocimientos mínimos

sobre cardinales infinitos, pero es relativamente elemental desde un punto de vista algebraico. Demostraremos en un capítulo posterior que dos clausuras algebraicas de un mismo cuerpo son isomorfas. Esto permite hablar de *La* clausura algebraica de un cuerpo K. Se la denota $\overline{K}$. Este resultado requiere del teorema de extensión de homomorfismos.

Proposición 5.17. *Para todo cuerpo K existe una clausura algebraica.*

Demostración Sea X un conjunto infinito cuya cardinalidad es estrictamente mayor a la del conjunto Y donde $Y = K[x] \times \mathbb{Z}$. Nótese que si L/K es algebraico entonces la cardinalidad de L es a lo más igual a la de Y, ya que cada polinomio en $K[x]$ tiene a lo más una cantidad finita de raices en L. Podemos suponer que $K \subseteq X$ ya que de otro modo remplazamos X por $X \cup K$. Sea Σ el conjunto de estructuras de cuerpo $(F, \square, *)$, con $K \subseteq F \subseteq X$ que satisfacen las condiciones siguientes:

- Para todo $a, b \in K$ se tienen $a \square b = a + b$ y $a * b = ab$.
- F/K es algebraica.

Existe un orden natural en Σ tal que $(F, \square, *) > (F', \square', *')$ si $F \supseteq F'$ y las operaciones en F extienden las de F'. Afirmamos que Σ satisface las hipótesis del lema de Zorn y que un elemento maximal de Σ es necesariamente un cuerpo algebraicamente cerrado. Esto terminará la demostración.

Como $(K, +, .)$ es un elemento de Σ, este no es vacío. Si se tiene una cadena $\{(F_\lambda, \square_\lambda, *_\lambda)\}_{\lambda \in \Lambda}$ en Σ se define una cota superior $(F, \square, *)$ donde $F = \bigcup_\lambda F_\lambda$ y para definir las operaciones $\square$ y $*$ tomamos λ suficientemente grande de modo que $a, b \in F_\lambda$ y se define $a \square b = a \square_\lambda b$ y $a * b = a *_\lambda b$. Dejamos al lector la comprobación de que la estructura $(F, \square, *)$ está bien definida, es de hecho un cuerpo, y se tiene $(F, \square, *) \in \Sigma$.

Sea ahora $(F, \square, *)$ un elemento maximal de Σ. Supongamos que no es algebraicamente cerrado. Entonces existe un polinomio $f(x)$ irreducible con coeficientes en F que no tiene raices en F. Sea $L = F[x]/(f)$. Como L es algebraico sobre K, su cardinalidad es a lo sumo la de Y. Como X tiene una cardinalidad infinita mayor que Y, $X \backslash F$ tiene al menos la cardinalidad de L (recuerdese que $\tau + \tau = \tau$ para todo cardinal infinito τ). Se sigue que existe una función inyectiva $\psi : L \to X$ que es la identidad en F. Se concluye que $(\psi(L), \clubsuit, \spadesuit)$, donde $\clubsuit$ y $\spadesuit$ son las imágenes de las operaciones de L, es una estructura de cuerpo que extiende $(F, \square, *)$ y es algebraica sobre K lo que contradice la maximalidad. $\square$

Trazas y Normas

Recordemos que en el capítulo anterior se definió la norma y la traza de un elemento a de una K-álgebra de dimensión finita A como el determinante y la traza del operador multiplicación T_a. Esta definición se aplica en particular si $A = L$ es una extensión algebraica de K. Sea $a \in L$, y sea $m_a(X) = m_{K,a}(X)$ su polinomio minimal sobre K. A la norma de a como un elemento de la K-álgebra L se la denota $N_{L/K}(a)$. Del mismo modo, la traza de a como un elemento de L se denota $\mathrm{Tr}_{L/K}(a)$. Nótese que esta definición ciertamente depende de la extensión finita L/K. De hecho se tiene el siguiente resultado:

Proposición 5.18. *Si $a \in L \subseteq E$ con E/K finita, se tiene:*

$$N_{E/K}(a) = N_(L/K)(a)^{[E:L]}, \qquad \mathrm{Tr}_{E/K}(a) = [E : L]\mathrm{Tr}_(L/K)(a).$$

Demostración Sea $\{e_1, \ldots, e_r\}$ una base de E/L. Como K espacio vectorial, se tiene $E \cong \bigoplus_{i=1}^{r} Le_i$ y

$$T_{E,a}\left(\sum_i l_i e_i\right) = a\sum_i l_i e_i = \sum_i (al_i)e_i = \sum_i T_{L,a}(l_i)e_i,$$

donde $T_{E,a}$ y $T_{L,a}$ denotan la función lineal *multiplicación por a* en los cuerpos E y L respectivamente. El resultado es ahora inmediato. □

Proposición 5.19. *Sea $a \in E$ donde E es una clausura algebraica de K. Sea $L = K[a]$. Sea*

$$m_{K,a}(X) = \prod_{i=1}^{r}(X - a_i)^{d_i} \tag{5.1}$$

la factorización en E del polinimio irreducible $m_{K,a}(X) \in K[X]$. Entonces

$$N_{L/K}(a) = a_1^{d_1} \cdots a_r^{d_r}, \qquad \mathrm{Tr}_{L/K}(a) = d_1 a_1 + \cdots + d_r a_r.$$

Demostración Sea

$$m_a(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$$

el polinomio minimal de a. Nótese que $\{1, a, a^2, \ldots, a^{n-1}\}$ es una base de L como K espacio vectorial. En esta base, la matriz de T_a es

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix},$$

de donde de tiene que

$$\det(T_a) = (-1)^n a_0 = a_1^{d_1} \cdots a_r^{d_r}, \qquad \operatorname{tr}(T_a) = -a_{n-1} = d_1 a_1 + \cdots + d_r a_r.$$

La segunda identidad en cada caso se obtiene desarrollando el producto en (5.1). □

Ejercicios

1. Sea L/K una extensión cuadrática. Probar que si la característica de K no es 2, entonces existe $a \in L$ con $a \notin K$ tal que $a^2 \in K$.

2. Probar que $\mathbb{C}$ no tiene extensiones cuadráticas.

3. Probar que $\mathbb{C}$ es la única extensión cuadrática de $\mathbb{R}$.

4. Probar que en un cuerpo de característica p se tiene, para todo $r \in \mathbb{N}$, la identidad $(x+y)^{p^r} = x^{p^r} + y^{p^r}$.

5. Si K es un cuerpo de característica 2, probar que existen matrices $A \in \mathbb{M}_2(K)$ que satisfacen $A^2 = I$ pero que no son diagonalizables

6. Probar que si E es el cuerpo generado, sobre un cuerpo K, por las raices de un cierto polinomio $f(x) \in K[x]$ de grado n, entonces $[E : K] \leq n!$. Calcule el grado sobre $\mathbb{Q}$ de las suiguientes extensiones:

   (a) $\mathbb{Q}(\sqrt[4]{3})$,
   (b) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$,
   (c) $\mathbb{Q}(\sqrt{1+2i})$,
   (d) $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$.

7. Calcule el grado sobre $\mathbb{Q}$ de las suiguientes extensiones: $\mathbb{Q}[\sqrt[r]{p}]$ (p primo), $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$, $\mathbb{Q}(\sqrt{a+bi})$ ($a^2+b^2 = p$ es primo), $\mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$.

8. Probar que si $\alpha \in \mathbb{C}$, entonces α es algebraico sobre $\mathbb{Q}$ sí y sólo si existe un polinomio $f(x)$ con coeficientes racionales, tal que $f(\alpha) = \frac{1}{\alpha^2}$.

9. Sea $a = \sqrt{2} + \sqrt{3}$ y sea $L = \mathbb{Q}(a)$. Sea $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   (a) Probar que $\sqrt{6} \in L$ (sugerencia: calcule a^2).

   (b) Probar que $L \neq \mathbb{Q}(\sqrt{6})$.

   (c) Probar que $L = K$.

   (d) Encontrar el polinomio irreducible de a sobre $\mathbb{Q}$.

10. Sea ω una raiz cúbica primitiva de la unidad. Sea $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, y sea $K = \mathbb{Q}(\omega\sqrt[3]{2})$. Probar que $[L : K] = 2$, pero $[\mathbb{R} \cap L : \mathbb{R} \cap K] = 3$.

11. Probar que si E y F son subcuerpos de un cuerpo L, tales que

$$[F : E \cap F] \leq \infty,$$

    entonces

$$EF = \left\{ \sum_{i=1}^{n} e_i f_i \middle| e_i \in E, f_i \in F \text{ para } i = 1, \ldots, n \right\}$$

    es cuerpo (sugerencia: considere primero el caso $F = k(a)$ con $k \subseteq E \cap F$).

12. Probar que si $K = F(a) \subseteq L$, entonces $[EK : E] \leq [K : F]$ para todo cuerpo $E \subseteq L$ que contenga a F.

13. Probar que si K/F es una extensión finita con $K \subseteq L$, entonces $[EK : EF] \leq [K : F]$ para todo cuerpo $E \subseteq L$ que contenga a F.

14. Probar que el conjunto de números constructibles es un cuerpo.

15. Probar que Si $K \subseteq L$ son cuerpos y $a \in L$, entonces a es algebraico sobre K sí y sólo si existe un K-espacio vectorial V de dimensión finita contenido en L, tal que $aV \subseteq V$.

16. Utilice la definición de cuerpo algebraicamente cerrado dada en el texto para probar en detalle que si k es algebraicamente cerrado, todo $f(x) \in k[x]$ puede escribirse como

$$f(x) = u \prod_{i=1}^{n} (x - \lambda_i)^{\alpha_i},$$

con $\lambda_1, \ldots, \lambda_n, u \in k$.

Chapter 6

Construcciones con regla y compás

Una regla es un trozo de madera que nos permite, dados dos puntos en una superficie plana, trazar la recta que estos punto determinan, y que contiene tanto el segmento entre estos dos puntos, como también sus prolongaciones mas allá de dichos puntos. Del mismo modo, el compás es un artefacto que nos permite trazar un círculo dados su centro y su radio. Para fijar ideas, debemos suponer que cada objeto, punto recta o círculo, es construido en base a objetos preliminares previamente construidos u objetos básicos. Uno podría comenzar con un conjunto arbitrariamente grande de objetos básicos, pero para efectos de estos apuntes, asumiremos un conjunto reducido de ellos, a saber:

1. Un punto dado O que llamaremos el origen de coordenadas.
2. Una recta $\mathfrak{R}$, que contiene a O, que llamaremos la recta real.
3. Un segundo punto $U \in \mathfrak{R}$ que se encuentra, por definición a una distancia unitaria de O en la dirección positiva (también por definición).

Diremos que un objeto geométrico es constructible si puede *construirse* a partir de los elementos mencionados mas arriba. Esto puede precisarse como sigue:

> Una construcción es una sucesión de objetos geométricos cada uno de los cuales es uno de los objetos básicos mencionados mas arriba o puede obtenerse de un subconjunto de los objetos precedentes mediante una de las siguientes operaciones básicas:

1. Dadas dos rectas no paralelas, tomar el punto de intersección.
2. Dado un círculo y una recta, o dos círculos, tomar cualquiera de los puntos de intersección entre ellos.
3. Dados dos puntos distintos, tomar la recta que los contiene.
4. Dados dos puntos distintos A y B, tomar el círculo centrado en A que contiene a B.

El lector puede convencerse fácilmente de que estas operaciones básicas codifican apropiadamente lo que el geómetra efectivamente hace al utilizar sus herramientas físicas *regla* y *compás*, con quizás una salvedad. Muchos compases pueden fijarse en una posición y por lo tanto utilizarse para trasladar longitudes, como por ejemplo, copiar el radio de un círculo con un centro dado, en un círculo con un centro diferente. Esto no genera, sin embargo, ninguna diferencia en la teoría, dado que es relativamente sencillo construir un círculo alrrededor de cualquier punto del plano cuyo radio sea igual al de un círculo dado. Para ello es necesario recordar que puede trazarse una perpendicular a una recta dada, ya sea desde cualquier punto exterior, o a travez de de cualquier punto de esta. Recordaremos dicha construcción a continuación:

> Sea A un punto de una recta L. Sean B y C los puntos de intersección de dicha recta con cualquier círculo centrado en A (para fijar ideas podemos utilizar el círculo que pasa por alguno de los puntos básicos O o U). Entonces el círculo Γ centrado en B y que pasa por C, se encuentra con el círculo Δ centrado en C y que pasa por B, en dos puntos D y E. La recta DE es perpendicular a L. Si tomamos un punto F fuera de L, podemos repetir el proceso utilizando los puntos G y F en los que algún círculo Θ centrado en F corta a L. Para fijar ideal puede tomarse el círculo que pasa por cualquier punto constructible en L, como los que fueron utilizados para construir L, o bien O si es que $L = \mathfrak{R}$.

Pudiendo trazar perpendiculares, podemos también trazar paralelas, que pueden verse como perpendiculares de perpendiculares a una curva dada. Finalmente, dados puntos constructibles A, B y C es posible construir cada

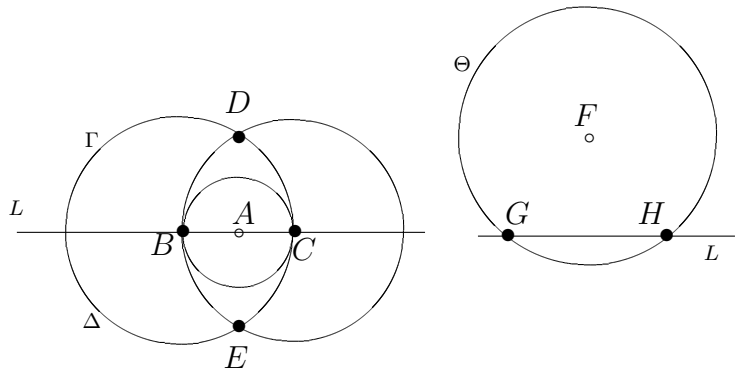


Figure 6.1: Construyendo perpendiculares.

lado del paralelógramo $ABCD$ y el cuarto vértice D es un punto cuya distancia a C es igual a la distancia entre A y B.

El purista puede encontrar fácilmente una segunda objeción. El geómetra recurre a menudo a la selección arbitraria de un punto en una recta o círculo o de un círculo de radio arbitrario o "suficientemente grande" alrededor de un punto. Esto se resuelve simplemente observando que dados dos puntos en una recta (que los tenemos), es posible construir una infinidad de puntos a distancia arbitrariamente grande, y dada la posibilidad de bisectar un segmento como se hizo en la construcción arriba mencionada, los puntos constructibles en dicha recta forman un conjunto denso. La posibilidad de trazar paralelas y, mediante el uso de círculos apropiados, constrir puntos arbitrariamente lejanos en estas paralelas, nos permite ver que, de hecho, los puntos constructibles forman un conjunto denso del plano. Por lo que también tenemos círculos y rectas que intersectan a cualquier círculo o recta prefijado, de manera no trivial, en un punto arbitrariamente cercano a cualquier punto dado de este objeto.

A continuación tomaremos un sistema de coordenadas en el plano, es decir identificaremos el plano con el espacio vectorial $\mathbb{R}^2$ de modo que los puntos O y U se identifican con los pares $(0,0)$ y $(1,0)$. En particular, el subespacio vectorial $\mathbb{R}(1,0)$ generado por $(1,0)$ se identifica con la recta $\mathfrak{R}$ generada por O y U, mintras que el subespacio $\mathbb{R}(0,1)$ es la recta perpendicular a $\mathfrak{R}$ en O.

El principal objetivo de este capítulo es obtener una caracterización de los puntos constructibles del plano en términos de sus coordenadas. Para ello necesitamos una definición algebraica.

definición 6.1. Un elemento $\alpha \in \mathbb{C}$ se dice constructible si existe una cadena de subcuerpos de $\mathbb{C}$

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_t$$

tales que $L_0 = \mathbb{Q}$, $\alpha \in L_t$, y $[L_{i+1} : L_i] = 2$ para todo i.

Se sigue de inmediato de la definición que para todo número complejo constructible α, el grado de su polinomio irreducible $m(x) = \mathrm{irr}_{\alpha,\mathbb{Q}}$ es

$$\deg(m) = \Big[\mathbb{Q}(\alpha) : \mathbb{Q}\Big] = \frac{[L_t : \mathbb{Q}]}{\Big[L_t : \mathbb{Q}(\alpha)\Big]},$$

en particular es una potencia de 2. Se sigue que una raiz de un polinomio cúbico irreducible no es constructible.

Proposición 6.2. *El conjunto K de números complejos constructibles es un cuerpo.*

Demostración El punto clave de la demostración es probar que dados dos números complejos constructibles α y β existe una cadena de extensiones

$$E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_N$$

Tales que

- $E_0 = \mathbb{Q}$,
- $\alpha, \beta \in E_t$, y
- $[E_{i+1} : E_i] = 2$ para todo $i = 0, \ldots, N-1$.

Para esto se toman dos cadenas

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_t, \quad \text{y} \quad L'_0 \subseteq L'_1 \subseteq L'_2 \subseteq \ldots \subseteq L'_s$$

Tales que $L_0 = L'_0 = \mathbb{Q}$, $\alpha \in L_t$, $\beta \in L'_s$ donde cada cuerpo es una extensión cuadrática del precedente en cada secuencia y tomamos a continuación la secuencia compuesta

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_t \subseteq L_tL'_0 \subseteq L_tL'_1 \subseteq L_tL'_2 \subseteq \ldots \subseteq L_tL'_s.$$

El resto de la demostración se deja al lector (Ejercicio 1). □

Proposición 6.3. *Un punto $(\alpha, 0) \in \mathfrak{R}$ es constructible si y sólo si α es constructible.*

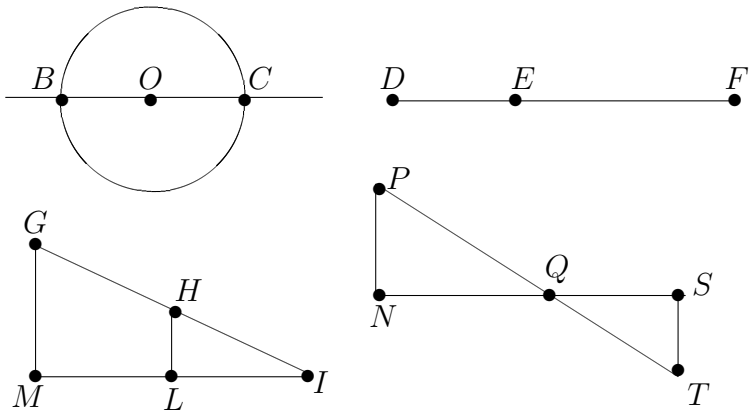


Figure 6.2: Demostración de que K' es un cuerpo.

Demostración Sea $K' = \{\alpha \in \mathbb{R} | (\alpha, 0) \text{ es constructible}\}$. Basta ver que $K = K'$. Probaremos primero que K' es un cuerpo. Si el origen está en O como se vé en la Figura 7.2, podemos usar el círculo centrado en el origen que pasa por B para obtener C y viceversa, de modo que podemos, en general, olvidar el signo. Como ya hemos probado que es posible transladar distancias (radios) de un punto a otro, bastará con tener construcciones geométricas de la suma, resta, producto y cociente de distancias ya consruidas. Esto se muestra en la Figura 7.2. Para obtener la suma $\alpha + \beta$ de dos números en K basta con construir un punto D a distancia α a la izquierda de un punto E y un punto F a la derecha de E a distancia β. La resta se obtiene similarmente construyendo tanto D como F al mismo lado de E. El cociente se obtiene a partir de similaridades de triángulos rectángulos. Si el lado NP mide 1, el lado NQ mide β, mientras el lado SQ mide α, entonces el largo del lado ST es el cociente α/β. El producto se obtiene de modo similar. Si el lado HL mide β y el lado MI mide α, mientras el lado LI mide 1, entonces el lado GM mide $\alpha\beta$. Nótese que la construcción precedente sólo funciona si $\alpha > 1$. Si este no fuera el caso podemos construir la distancia $(n\alpha)\beta$ para n suficientemente grande y luego dividir como ya vimos.

Supongamos ahora que el punto $(0, \alpha)$ es constructible. entonces podemos construir un triángulo rectángulo como el triángulo IMG de la Figura 7.2,

cuyo lado IM mide $1 - \frac{\alpha}{4}$ y el lado IG mide $1 + \frac{\alpha}{4}$, por lo que el lado GM mide

$$\sqrt{\left(1 + \frac{\alpha}{4}\right)^2 - \left(1 - \frac{\alpha}{4}\right)^2} = \sqrt{\alpha}.$$

Para realizar esta construcción simplemente construimos el segmento IM del largo correcto, el círculo de radio $1 + \frac{\alpha}{4}$ centrado en I y la perpendicular a IM por M. El punto de intersección de estos últimos es G.

De lo anterior se concluye que si α es cualquier número contenido en un cuerpo L_t para el cual existe una cadena de cuerpos

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_t \subseteq \mathbb{R}$$

tales que $L_0 = \mathbb{Q}$, $\alpha \in L_t$, y $[L_{i+1} : L_i] = 2$ para todo $i.$, entonces $(\alpha, 0)$ es constructible. De hecho, la condición $L_t \subseteq \mathbb{R}$ no compromete la generalidad pues podemos remplazar L_i por $L_i \cap \mathbb{R}$ si fuese necesario. Concluimos que $K \subseteq K'$. La conversa se obtiene de las siguientes observaciones:

- La recta que une dos puntos cuyas coordenadas pertenecen a cierto cuerpo $F \subseteq \mathbb{R}$ tiene una ecuación de la forma $AX + By + C = 0$ con A, B, y C en F. De hecho si los puntos son (a, b) y (c, d), podemos tomar $A = d - b$, $B = c - a$ y $C = bc - ad$. Un cálculo similar prueba que un círculo cuyo centro tiene coordenadas en F y cuyo radio pertenece también a F está descrito por una ecuación con coeficientes en F.

- Si dos rectas no paralelas L y L' tienen ecuaciones de la forma $Ax + By + C = 0$ y $A'x + B'y + C' = 0$, con A, B, C, A', B', y C' en cierto cuerpo F, el punto en que se intersectan es $P = \left(\frac{B'C - BC'}{A'B - AB'}, \frac{A'C - AC'}{AB' - A'B}\right)$, el cual tiene sus coordenadas en F.

- La intersección entre la recta de ecuación $Ax + By + C = 0$ y el círculo $(x - a)^2 + (y - b)^2 = R^2$, con $\{A, B, C, a, b, R\} \subseteq F$, consiste en dos puntos cuyas coordenadas (x, y) están dadas por

  $$y - b = -\frac{A}{B}(x - a) - \frac{D}{B},$$

  y

  $$x - a = \frac{AD \pm \sqrt{A^2D^2 - (A^2 + B^2)(R^2B^2 + D^2)}}{A^2 + B^2},$$

  donde $D = C + Aa + Bb$. Las coordenadas de estos puntos están en una extensión cuadrática de F.

- La intersección entre el círculo de ecuación $(x-a)^2+(y-b)^2=R^2$ y el de ecuación $(x-c)^2+(y-d)^2=r^2$, es la misma que la intersección de cualquiera de estos círculos con la recta $(c-a)x+(d-b)y+t=0$, donde
$$t=a^2+b^2+r^2-c^2-d^2-R^2.$$

□

Proposición 6.4. *El punto* $(\alpha,0)\in\mathfrak{R}$*, donde* α *esel largo del lado de un cubo de lado* 2 *no es constructible (no se puede duplicar el cubo con regla y compás).*

Demostración Basta ver que $\sqrt[3]{2}$ no es un número constructible, lo que es inmediato dado que su polinomio irreducible es x^3-2, el cual tiene grado 3. □

Proposición 6.5. *Una recta que subtiende un ángulo de* 20 *grados con la recta real no puede construirse con regla y compás.*

Demostración Observese que si el ángulo MIG de la figura 7.2 tuviese 20 grados, donde M e I son puntos constructibles, el punto G es el punto donde la perpendicular a la recta IM corta a IG por lo que si IG fuese constructible, también lo sería el punto G. Se sigue que el cociente $a=\text{sen}(20^o)$ entre los largos de MG e IG es un número constructible. Pero utilizando las fórmulas para el seno y coseno de una suma y los valores conocidos para estas funciones en el ángulo de 60^o, es fácil ver que $a^3-3a(1-a^2)=\frac{1}{2}$ por lo que $x=2a$ satisface la ecuación $x^3-3x+1=0$, la que carece de raices racionales. De hecho si $\frac{n}{m}$ fuese una raiz, con n y m coprimos, tendríamos $n^3=(3n-m)m^2$, lo que no es posible, salvo si $m=1$ y en tal caso $n^3=3n-1$, lo que no tiene soluciones enteras. Concluimos que x^3-3x+1 es irreducible, lo que contradice la constructibilidad de x. □

A continuación identificaremos cada punto (a,b) del plano con un número complejo $a+bi$.

Proposición 6.6. *Un punto* (a,b) *del plano es constructible si y sólo si* $a+bi$ *es un número complejo constructible.*

Demostración Dado que los ejes de coordenadas son constructibles, y podemos trazar perpendiculares desde cualquier punto a cualquier recta, es fácil ver que el punto (a, b) es constructible si y sólo si lo son los puntos $(a, 0)$ y $(b, 0)$, es decir si a y b son constructibles. Bastará por lo tanto ver que esta última condición es equivalente a que $a + bi$ sea un número complejo constructible.

Es claro que si a y b son constructibles, también lo es $a + bi$, ya que $i = \sqrt{-1}$ es constructible. Por otro lado si $z = a + bi$ es constructible, también lo es su conjugado complejo $\bar{z} = a - bi$ ya que cualquier secuencia de cuerpos

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_t,$$

con $z \in L_t$ nos dá una secuencia de conjugados

$$\bar{L}_0 \subseteq \bar{L}_1 \subseteq \bar{L}_2 \subseteq \ldots \subseteq \bar{L}_t,$$

con $\bar{z} \in \bar{L}_t$. Se sigue que $z + \bar{z} = 2a$ es constructible y por lo tanto también $b = i(a - z)$. □

En general, un subcuerpo K de $\mathbb{C}$ consiste de elementos $z = a + bi$ con a y b en K si y sólo si K cumple las condiciones siguientes:

1. K es invariante bajo la conjugación compleja.
2. K contiene a la unidad imaginaria $i = \sqrt{-1}$.

Dejamos como ejercicio para el lector encontrar ejemplos de cuerpos que cumplan una de estas condiciones, pero no la otra.

Un polígono P se dice constructible si cada vértice de $P + z$ es constructible para algún número complejo z. Si esto ocurre para algún número complejo z_0, también ocurre para $z_0 + c$ para cualquier $c \in \mathbb{C}$ constructible.

En los ejercicios del capítulo 11 veremos que el polinomio ciclotómico

$$\phi_{p^m}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = x^{(p-1)p^{m-1}} + x^{(p-1)p^{m-2}} + \cdots + x^{p^{m-1}} + 1$$

es irreducible. Utilizando este hecho podemos probar el siguente resultado:

Proposición 6.7. *Sea p un número primo impar y sea $m \geq 1$ un entero. Un polígono regular de p^m lados no puede construirse con regla a menos que $m = 1$ y p es un primo de Fermat.*

Demostración Dado que el centro de un polígono regular con vértices constructibles es constructible, por ser el promedio de los vértices, si el polígono de n lados es constructible, existen dos números complejos z y z' (digamos, dos vértices consecutivos) cuyo cociente es la raiz de la unidad $\eta = e^{2\pi i/n}$. Se sigue que η es constructible y por lo tanto el grado

$$\Big[\mathbb{Q}(\eta) : \mathbb{Q}\Big]$$

es una potencia de 2. Como el polinomio ciclotómico $\phi_{p^m}(x)$ es irreducible, se tiene que

$$\Big[\mathbb{Q}(\eta) : \mathbb{Q}\Big] = \deg(\phi_{p^m}) = (p-1)p^{m-1}$$

es una potencia de 2. Si p es un primo impar, esto necesariamente implica que $m = 1$ y $p - 1$ es una potencia de 2. Esto último ocurre si y sólo si p es un primo de Fermat. □

Conversamente, si η es constructible, también lo es el polígono regular de lado 1 por el mismo argumento. Se sigue que la principal dificultad para provar la conversa consiste en probar la existencia de suficientes extensiones intermedias entre $\mathbb{Q}$ y $\mathbb{Q}(\eta)$. Esto puede hacerse vía teoría de Galois como veremos en un capítulo posterior. Terminaremos este capítulo mostrando como el conocimiento de las extensiones intermedias nos permite efectivamente construir un polígono con regla y compás.

Proposición 6.8. *Es posible construir el pentágono de lado* 1 *con regla y compás.*

Demostración Sea $\eta = e^{2\pi i/5}$. Basta ver que $\alpha = \eta + \bar{\eta}$ genera una extensión cuadrática. Para ello recordemos que η satisface la ecuación

$$1 + \eta + \eta^2 + \eta^3 + \eta^4 = 0,$$

es decir

$$\eta + \eta^2 + \eta^3 + \eta^4 = -1.$$

por otro lado $\bar{\eta} = \eta^{-1} = \eta^4$, y además

$$\alpha^2 = (\eta + \eta^4)^2 = \eta^2 + 2 + \eta^3,$$

por lo que concluimos que $\alpha + (\alpha^2 - 2) = -1$. Es decir

$$\alpha^2 + \alpha - 1 = 0.$$

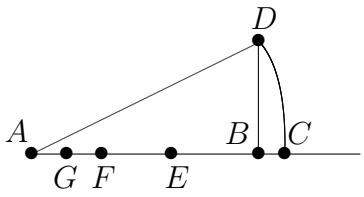


Figure 6.3: Part of the construction of a pentagon.

□

Veamos ahora como se puede transformar la demostración precedente en una auténtica construcción geométrica.

Se construye un triángulo ABD rectángulo en B que satisface $AB = 2BD$, y sea C el punto donde el círculo AD centrado en A corta a la recta AB. Nótese que $AC = BD\sqrt{5}$. Sea E el punto del segmento AB que satisface $CE = BD$. Sea F el punto medio de AE y sea G el punto medio de AF. Nótese que

$$\frac{AG}{BD} = \frac{\sqrt{5}-1}{4} = \frac{\alpha}{2} = \mathrm{Re}(\eta),$$

de donde, si H es el punto de intersección de la perpendicular en G con el círculo de radio BD alrededor de A, el ángulo GAH tiene 72 grados.

Ejercicios

1. Probar, en detalle, que el conjunto de números constructibles es un cuerpo.

2. Pruebe que si un polinomio con coeficientes racionales tiene una raiz constructible, todas sus raices lo son.

3. Pruebe que un círculo cuyo centro tiene coordenadas en un cuerpo F y cuyo radio pertenece también a F está descrito por una ecuación con coeficientes en F.

4. Probar que si m y n son relativamente primos, y si pueden construirse polígonos regulares de n y m lados con regla y compás, entonces puede construirse el polígono de nm lados.

5. Utilice la Proposición 6.7 para dar otra demostración de que no se puede trisectar el ángulo.

6. Probar que se puede construir un ángulo de 24 grados con regla y compás.

7. Si X es un conjunto arbitrario dado de puntos en el plano complejo, caracterize (en términos de extensiones de cuerpos) el conjunto de puntos que pueden obtenerse a partir de ellos con regla y compás.

8. Si a usted se le entrega una hoja donde hay dibujados dos segmentos cuya proporción es la mayor raiz de la ecuación $x^3 + x^2 - 2x - 1 = 0$, puede construir un heptágono utilizando dichos segmentos y usando sólo la regla y el compás?

9. Existe un conjunto finito de puntos en el plano a partir del cual cualquier otro punto sea constructible?

10. En este ejercicio probaremos que $f(x) = x^4 + 8x + 12$ es un polinomio de grado 4 cuyas raices no son constructibles.

    (a) Probar que para cualquier número complejo y, la ecuación $f(x) = 0$ es equivalente a

    $$(x^2 + y)^2 = -8x - 12 + 2yx^2 + y^2.$$

    (b) Probar que si y es raiz del polinomio cúbico $g(x) = x^3 - 12x - 4$, entonces

    $$\left(x\sqrt{2y} - \frac{4}{\sqrt{2y}}\right)^2 = -8x - 12 + 2yx^2 + y^2.$$

    (c) Muestre que las observaciones anteriores permiten, para cualquier raiz y de g, descompones la ecuación $f(x) = 0$ en dos ecuaciones cuadráticas.

    (d) Utilice las relaciones entre coeficientes y raices de una ecuación cuadrática para probar que $\sqrt{2y}$ es suma de dos raices de f. Concluya que y está en el cuerpo generado por las raices de f.

    (e) Pruebe que g es irreducible.

    (f) Concluya que las raices de f no son constructibles.

Chapter 7

Cuerpos Finitos

Sea K un cuerpo finito. En particular K no puede tener característica 0, de donde K contiene una imagen isomorfa del cuerpo $\mathbb{F}_p$ para algún primo p. Se sigue que K es un espacio vectorial de dimensión finita sobre $\mathbb{F}_p$ de grado $n = [K : \mathbb{F}_p]$. Se concluye que $|K| = p^n$. El grupo multiplicativo $K^* = K - \{0\}$ tiene $p^n - 1$ elementos. A continuación determinaremos la estructura de este grupo. En particular, probaremos que es un grupo cíclico.

La función ϕ de Euler se define como $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. El teorema chino de los restos implica que $\phi(nm) = \phi(n)\phi(m)$ si n y m son relativamente primos. El número de elementos de un orden dado en un grupo cíclico puede calcularse fácilmente en términos de ϕ. De hecho, tenemos el siguiente resultado:

Lema 7.1. *Si m divide a n, existen $\phi(m)$ elementos de orden m en el grupo cíclico $C_n = \mathbb{Z}/n\mathbb{Z}$.*

Demostración El orden o_a del elemento $a + n\mathbb{Z}$ divide a m si y sólo si $ma + n\mathbb{Z} = 0 + n\mathbb{Z}$. Es decir, $o_a | m$ si y sólo si ma es divisible por n, o equivalentemente a es divisible por $m' = n/m$. En particular, $o_a = m$ si y sólo si a es divisible por m' y no por ningún divisor de n mayor a m'. En otras palabras $(a) + (n) = (m')$. Esto es equivalente a decir que $(a/m') + (n/m') = (1)$, por lo que hay $\phi(n/m') = \phi(m)$ elecciones posibles para a/m' módulo m, lo que nos dá $\phi(m)$ elecciones posibles para a módulo $mm' = n$. □

Corolario 7.1.1. $\sum_{d|n} \phi(d) = n$.

Lema 7.2. *Si G es un grupo abeliano finito, donde hay a lo más n soluciones de la ecuación $g^n = e$ para cada n entonces G es un grupo cíclico.*

Demostración Sea $N = |G|$. Basta ver que existe un elemento de orden N. Supongamos que G tiene $\psi(n)$ elementos de orden n para cada n. Entonces $\sum_{d|N} \psi(d) = N$. Si $\psi(N) = 0$, existe algún n con $\psi(n) > \phi(n)$. Tomemos un divisor n de N minimal tal que $\psi(n) > \phi(n)$. En particular, G tiene elementos de orden n. Un elemento $g \in G$ de orden n genera un subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z}$ y por lo tanto $\psi(d) \geq \phi(d)$ para todo divisor d de n. Se concluye que el número de elementos cuyo orden divide a n es $\sum_{d|n} \psi(d) > \sum_{d|n} \phi(d) = n$, contradiciendo la hipótesis. □

Proposición 7.3. *Si K es un cuerpo arbitrario y si Γ es un subgrupo finito de K^* entonces Γ es cíclico.*

Demostración La hipótesis del resultado precedente es inmediata, ya que un polinomio de grado n no puede tener mas de n raices. □

Corolario 7.3.1. *Si K es un cuerpo finito con p^n elementos, entonces K^* es un grupo cíclico de orden $p^n - 1$.* □

Corolario 7.3.2. *Si K es un cuerpo finito con p^n elementos, entonces cada elemento de K es raiz de la ecuación $x^{p^n} = x$.* □

Corolario 7.3.3. *Un cuerpo L de característica p puede contener a lo más un cuerpo con p^n elementos para cada $n \in \mathbb{N}$.*

Demostración El polinomio $x^{p^n} - x$ tiene a lo más p^n raices. □

Lema 7.4. *Sea L un cuerpo arbitrario de característica p. Si a y b están en L, entonces $(a + b)^p = a^p + b^p$.*

Demostración Por inducción se demuestra el teorema del binomio

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

de la manera usual. También puede deducirse a partir de la propiedad universal de los polinomios como veremos en el próximo capítulo. A continuación tomamos $n = p$ y observamos que cada coeficiente binomial $\binom{p}{k}$ es divisible por p. □

Lema 7.5. *Si L es un cuerpo arbitrario de característica p, las raices del polinomio $x^{p^n} - x$ son un subcuerpo de L.*

Demostración Es claro que si a y b son raices, también lo son ab y $1/a$. El hecho de que $a + b$ es una raiz sigue del lema precedente. Como L tiene característica positiva, $-1 = 1 + \ldots + 1$ es también raiz y por lo tanto lo es $-a = (-1)a$. □

Lema 7.6. *Si L es un cuerpo algebraicamente cerrado de característica p, el polinomio $x^{p^n} - x$ tiene p^n raices distintas en L.*

Demostración Basta ver que $x^{p^n} - x$ no tiene raices dobles en L. Sea

$$x^{p^n} - x = \prod_{i=1}^{T} (x - \lambda_i)^{s_i}.$$

Entonces evaluando en $x - \lambda$ se tiene

$$(x^{p^n} - x) + (\lambda^{p^n} - \lambda) = (x + \lambda)^{p^n} - (x + \lambda) = \prod_{i=1}^{T} (x + \lambda - \lambda_i)^{s_i},$$

de donde si $\lambda = \lambda_j$ es una raiz, se tiene

$$(x^{p^n} - x) = x^{s_j} \prod_{i \neq j} (x + \lambda_j - \lambda_i)^{s_i}.$$

Basta, por lo tanto ver que 0 no es una raiz doble de $x^{p^n} - x$, lo que es inmediato. □

Proposición 7.7. *Si L es un cuerpo algebraicamente cerrado de característica p, entonces L contiene un subcuerpo con p^n elementos para cada n.*

Demostración Inmediata de los dos lemas precedentes. □

Se sigue de la unicidad de la clausura algebraica que existe un único cuerpo con p^n elementos salvo isomorfismos. A continuación daremos una demostración elemental de este resultado.

Lema 7.8. *Sea K un cuerpo con p^n elementos. Entonces existe $\alpha \in K$ tal que $K = \mathbb{F}_p[\alpha]$.*

Demostración Para cada m menor que n, existe a lo más un subcuerpo con p^m elementos. El número total de elementos contenidos en algún subcuerpo propio no puede exeder

$$\sum_{m<n} p^m = \frac{p^n - 1}{p - 1} < p^n.$$

En particular, existe un elemento α en K que no está contenido en ningún subcuerpo menor. Se sigue que $K = \mathbb{F}_p[\alpha]$. □

Corolario 7.8.1. *Existen polinomios primos de cualquier grado en* $\mathbb{F}_p[x]$. □

Lema 7.9. *Sea K un cuerpo con p^n elementos. Sea f un polinomio primo de grado n en $\mathbb{F}_p[x]$. Entonces $K \cong \mathbb{F}_p[x]/\Big(f(x)\Big)$.*

Demostración Sea L un cuerpo algebraicamente cerrado que contiene a K. Sea α una raiz de $f(x)$ en L. Entonces $\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/\Big(f(x)\Big)$ es un subcuerpo de L y la extensión $\mathbb{F}_p[\alpha]/\mathbb{F}_p$ tiene grado n, por lo que $|\mathbb{F}_p[\alpha]| = p^n$. Por la unicidad, se tiene $\mathbb{F}_p[\alpha] = K$. □

Proposición 7.10. *Existe un único cuerpo con p^n elementos para todo $n \in \mathbb{N}$ salvo isomorfismos.*

Demostración Inmediato del lema y el corolario precedentes. □

El único cuerpo con p^n elementos se denota $\mathbb{F}_{p^n}$. Como cada clausura algebraica L de $\mathbb{F}_p$ puede escribirse en la forma $L = \bigcup_n L_n$ con cada L_n canónicamente isomorfo a $\mathbb{F}_{p^n}$, se sigue que existe una única clausura algebraica de $\mathbb{F}_p$ salvo isomorfismos. Denotaremos este cuerpo por $\overline{\mathbb{F}_p}$.

Ejercicios

1. Encuentre todos los polinomios irreducibles de grado 2, 3, y 4 en $\mathbb{F}_2[x]$.
2. Calcule cuantos polinomios irreducibles de grado 8 hay en $\mathbb{F}_2[x]$. Calcule cuantos polinomio irreducibles de grado 6 hay en $\mathbb{F}_3[x]$.
3. Probar que un pilinomio de grado t en $\mathbb{F}_p[x]$ es primo si y sólo si no tiene raices en $\mathbb{F}_{p^s}$ para ningún $s \leq t/2$.
4. Determine si x^6+x+1 tiene o no raices en $\mathbb{F}_4$. Lo mismo para x^5+x+1.

5. Calcule los grados de todos los divisores primos en $\mathbb{F}_2[x]$ del polinomio

$$x^{60} + x^{57} + x^{54} + \ldots + x^3 + 1.$$

6. Encuentre el menor entero r tal que $\mathbb{F}_{7^r}$ contiene una raiz onceava primitiva de la unidad.

7. Sea $\alpha \in \mathbb{F}_8 - \{0, 1\}$ tal que $\alpha^3 \neq \alpha + 1$. Probar que $\alpha^3 = \alpha^2 + 1$.

8. Sea α una raiz de $x^5 + x^2 + 1$ en $\mathbb{F}_{32}$. Encuentre un polinomio f de grado no mayor a 4 tal que $\alpha^8 = f(\alpha)$.

9. Sea K un cuerpo de característica p y sea $a \in K$. Sea $F(x) = x^p - x + a$.

   (a) Probar que si α es raiz de F, también lo es $\alpha + 1$. Concluir que $F(x)$ tiene raices distintas.

   (b) Probar que si F tiene una raiz en K, entonces tiene todas sus raices en K.

   (c) Suponga que $K = \mathbb{F}_p$ y que $a = 1$. Probar que F no tiene raices en K.

   (d) con las hipótesis del punto anterior, probar que para toda raiz α de F se tiene $\alpha^{p^p} = \alpha$. Concluir que $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^p}$.

10. Sea q un primo que divide a $p - 1$. Probar que existe $\alpha \in \mathbb{F}_{p^q}$ tal que $\alpha^q = \mathbb{F}_p$ y $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^q}$ (sugerencia: si q^t divide a $p - 1$, entonces q^{t+1} divide a $p^q - 1$).

11. Sea $K/\mathbb{F}_p$ una extensión finita. Probar que $\wp : K \to K$ definido por $\wp(u) = u^p$ es un automorfismo de K que fija a $\mathbb{F}_p$. Probar que los elementos de $\mathbb{F}_p$ son los únicos elementos fijos por $\wp$.

12. Sea $f(x)$ un polinomio con coeficientes en $\mathbb{F}_2$. Probar que $f'(x) = 0$ sí y sólo si $f(x) = g(x)^2$ para algún polinomio g con coeficientes en $\mathbb{F}_2$.

13. Sea $f(x)$ un polinomio con coeficientes en $\mathbb{F}_p$. Probar que $f'(x) = 0$ sí y sólo si $f(x) = g(x)^p$ para algún polinomio g con coeficientes en $\mathbb{F}_p$.

14. Sea K un cuerpo de característica p. Probar que para todo par de elementos a y b en K, se tiene que $a^p = b^p$ implica $a = b$.

15. Probar que la aplicación $\phi : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ definida por $\phi(a) = a^p$ es un homomorfismo epiyectivo para todo entero r.

16. Sea $f(x)$ un polinomio con coeficientes en $\mathbb{F}_p^r$ para algún entero r. Probar que $f'(x) = 0$ sí y sólo si $f(x) = g(x)^p$ para algún polinomio g con coeficientes en $\mathbb{F}_{p^r}$.

17. Probar que si p es un primo impar, el cuerpo $\mathbb{F}_{p^r}$ contiene $\frac{p^r+1}{2}$ cuadrados perfectos.

18. Probar que si p es un primo impar, todo elemento de $\mathbb{F}_{p^r}$ es suma de dos cuadrados perfectos.

Chapter 8

Polinomios sobre anillos conmutativos

Sea C un anillo conmutativo no necesariamente unitario. Se define el anillo $C[[x]]$ de series de potencias en x con coeficientes en C, como el anillo de todas las series formales del tipo:

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + \ldots,$$

Con $a_0, a_1, \ldots \in C$. Si tenemos series de potencias $f(x)$ y $g(x)$ definidas por

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots, \qquad g(x) = b_0 + b_1x + b_2x^2 + \ldots,$$

la suma $f(x) + g(x)$ y el producto $f(x)g(x)$ se definen mediante las fórmulas

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+(a_3+b_3)x^3+(a_4+b_4)x^4+\ldots,$$

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 + c_5x^5 + \ldots,$$

donde c_n se define por las formulas

$$\begin{array}{rcl} c_0 & = & a_0b_0, \\ c_1 & = & a_1b_0 + a_0b_1, \\ c_2 & = & a_2b_0 + a_1b_1 + a_0b_2, \\ c_3 & = & a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3, \\ \vdots & \vdots & \vdots \end{array}$$

o mas generalmente $c_n = \sum_{i=0}^{n} a_ib_{n-i}$. Con estas definiciones $A = C[[x]]$ es efectivamente un anillo conmutativo. Si C es unitario, también lo es $C[[x]]$.

La unidad de $C[[x]]$ es la serie de potencias $1_{C[[x]]} = 1 + 0x + 0x^2 + \ldots$. Adoptaremos la convención de omitir los términos con coeficiente 0, de modo que la unidad se escribirá simplemente 1. Del mismo modo, escribirémos x^n por $1x^n$ y $\ldots - a_n x^n + \ldots$ en vez de $\ldots + (-a_n)x^n + \ldots$.

Sea $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$. Si existe N tal que $a_n = 0$ para $n > N$, entonces f se dice un polinomio. Los polinomios forman un subanillo $C[x]$ de $C[[x]]$. Por iteración, pueden definirse los anillos $C[x_1, \ldots, x_n]$ y $C[[x_1, \ldots, x_n]]$, e incluso anillos mixtos como $C[x][[y]]$.

La propiedad fundamental de los polinomios es que pueden evaluarse en cualquier elemento del anillo. De hecho, como ya hemos visto en los capítulos anteriores para polinomios con coeficientes en un cuerpo, muchas veces es necesario evaluarlos en elementos que no están en el anillo. A continuación estudiaremos una generalización del concepto de evaluación. Recordemos que, como se definió en el capítulo 4, si C es un anillo conmutativo, una C-algebra es un par (B, ϕ) donde B es un anillo y $\phi : C \to B$ es un homomorfismo tal que $\phi(C) \subseteq Z(B)$.

Propiedad Universal del Anillo de Polinomios. *Si (B, ϕ) es un C-algebra, dado cualquier $a \in B$, existe un homomorfismo de anillos $\tilde{\phi} : C[x] \to B$ con las propiedades siguientes:*

- $\tilde{\phi}(x) = a$,
- *la restricción de $\tilde{\phi}$ a C es ϕ.*

Cuando ϕ es la identidad o una inclusión canónica, o si el homomorfismo ϕ es claro del contexto, la imagen $\tilde{\phi}(f(x))$ se denota simplemente $f(a)$ y a la función $\tilde{\phi}$ se la denomina evaluación en a. Una consecuencia de esta propiedad universal es que $f(a)g(a) = g(a)f(a)$ para todo $a \in B$. En otras palabras, polinomios en la misma variable conmutan. Mas generalmente, se tiene el siguiente resultado:

Propiedad Universal del Anillo de Polinomios en n variables. *Sea (B, ϕ) un C-algebra. Si $a_1, \ldots, a_n$ son elementos de B que conmutan por pares (es decir $a_i a_j = a_j a_i$ para todo i, j), entonces existe una funcion $\tilde{\phi} : C[x_1, \ldots, x_n] \to B$ con las propiedades siguientes:*

- $\tilde{\phi}(x_i) = a_i$,
- *la restricción de $\tilde{\phi}$ a C es ϕ.*

El principio de extensión de identidades

Un caso particular de interes es aquel donde $C = \mathbb{Z}$. Nótese que todo anillo es una $\mathbb{Z}$-álgebra. Los elementos de $\mathbb{Z}[x_1, \ldots, x_n]$ se denominan polinomios enteros Recordemos que todo polinomio real en n-variables puede escribirse como una serie de Taylor, de donde todo polinomio en $\mathbb{R}[x_1, \ldots, x_n]$ que se anule identicamente en $\mathbb{R}^n$ es 0 como elemento del anillo de polinomios $\mathbb{R}[x_1, \ldots, x_n]$. Esta observación permite extender cualquier identidad entre polinomios enteros que se sepa cierta como funciones reales a cualquier anillo conmutativo. Los ejemplos siguientes ilustran este punto:

1. Si a, b son elementos de un anillo y $ab = ba$ entonces

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

2. Si A es una matriz con coeficientes reales, y si $\tilde{A}$ es la transpuesta de la matriz de cofactores de A entonces $A\tilde{A} = \det(A) I_n$. Sea $X = (x_{i,j})_{i,j=1}^n$ con coeficientes en el anillo de polinomios

$$B = \mathbb{Z}[x_{i,j} | 1 \leq i, j \leq n].$$

   Esta se conoce como la matriz genérica. Dado que la identidad $X\tilde{X} = \det(X) I_n$ se cumple al asignar cualquier valor real a las variables $x_{i,j}$, debe ser una identidad en el anillo $\mathbb{M}_n(B)$. Se tiene que es también una identidad en $\mathbb{M}_n(C)$ para cualquier anillo conmutativo C.

3. Sea ahora

$$B' = \mathbb{Z}[x_{i,j}, y_{i,j} | 1 \leq i, j \leq n].$$

   Si $X = (x_{i,j})_{i,j=1}^n$ y $Y = (y_{i,j})_{i,j=1}^n$, se dice que (X, Y) es un par genérico de matrices. La identidad $\det(X)\det(Y) = \det(XY)$ se cumple al evaluar en elementos cualesquiera de $\mathbb{R}$ y por lo tanto en cualquier anillo conmutativo.

En particular, de los ejemplos 2 y 3 se sigue que un elemento de $\mathbb{M}_n(C)$ es invertible si y sólo si su determinante lo es, en cuyo caso su inverso es $[\det C]^{-1}\tilde{C}$.

Ejemplo 8.1. La matrix

$$\begin{pmatrix} \bar{5} & \bar{4} & \bar{8} \\ \bar{7} & \bar{3} & \bar{6} \\ \bar{5} & \bar{5} & \bar{5} \end{pmatrix}$$

con coeficientes en $\mathbb{Z}/3\mathbb{Z}$ es invertible. Dejamos como ejercicio para el lector el cálculo de su inverso.

El subanillo generado por un elemento

Sea (A, ϕ) una C-algebra. Sea u un elemento de A. el anillo generado por u sobre C es el subanillo más pequeño de A que contiene a $\phi(C)$ y u y se le denota por $C[u]$. Puede también caracterizarse como la imagen del homomorfismo $\phi_u : C[x] \to A$ que extiende ϕ y satisface $\phi_u(x) = u$. En particular, $C[u] \cong C[x]/\ker(\phi_u)$. Mas generalmente, si $u_1, \ldots, u_n$ son elementos de A que conmutan, el anillo $C[u_1, \ldots, u_n]$ es la imagen de $\phi_{u_1,\ldots,u_n}$ y se tiene $C[u_1, \ldots, u_n] \cong C[x_1, \ldots, x_n]/\ker(\phi_{u_1,\ldots,u_n})$.

Ejemplo 8.2. El anillo $\mathbb{Z}[i]$ es el anillo de números complejos de la forma $a + bi$ con a y b enteros, ya que $i^n \in \{1, -1, i, -i\}$ para todo n.

Ejemplo 8.3. El anillo $\mathbb{Z}[\sqrt{2}]$ es el anillo de números reales de la forma $a + b\sqrt{2}$ con a y b enteros, ya que $(\sqrt{2})^n \in \mathbb{Z} \cup \sqrt{2}\mathbb{Z}$ para todo n.

Estos ejemplos motivan los resultados siguientes:

Proposición 8.4 (Algoritmo de división para polinomios mónicos)**.** *Si f es un polinomio mónico de grado d con coeficientes en C, entonces todo elemento de $C[x]$ puede escribirse de manera única en la forma $r(x) + q(x)f(x)$ con $\deg(r) < \deg(f)$.*

Demostración. Sea $u = x + (f) \in C[x]/(f)$. Por cierto $f(u) = 0$ en este anillo. Supongamos que $h(x)$ es un elemento de $C[x]$ con $h(x) = ax^n + \ldots$ y $\deg(h) = n > \deg(f)$, entonces $h_1(x) = h(x) - af(x)$ es un polinomio de grado menor a h y que satisface $h_1(u) = h(u)$. Se sigue ahora del principio de inducción completa que existe un polinomio $r(x)$ de grado menor a f tal que $r(u) = h(u)$, es decir $h(x) - r(x) \in (f)$, y por lo tanto $h(x) - r(x) = q(x)f(x)$ para algún polinomio $q(x)$. Para probar la unicidad basta ver que un polinomio mónico no puede dividir a otro polinomio de menor grado. Pero si $f(x) = x^d + \ldots$ (donde los puntos representan términos de grado menor) y si $h(x) = ax^m + \ldots$, entonces $f(x)h(x) = ax^{m+d} + \ldots$ tiene grado $m + d$. □

Proposición 8.5. *Si u satisface un polinomio mónico f de grado d con coeficientes en C, entonces todo elemento a de $C[u]$ puede escribirse en la forma $a = r(u)$ con* $\deg(r) < \deg(f)$.

Demostración. Sigue de la proposición anterior que para todo $h(u) \in C[u]$ se tiene $h(u) = r(u) + q(u)f(u) = r(u)$ con $\deg(r) < \deg(f)$. □

Ejemplo 8.6. El anillo $\mathbb{Z}[\frac{1}{2}]$ es el anillo de números racionales de la forma $\frac{n}{2^t}$ con n entero. En este caso, es imposible escribir $\frac{1}{2^t}$ como un polinomio en $\frac{1}{2}$ de grado menor a t. Sea $f(x)$ un polinomio con coeficientes enteros tal que $f(\frac{1}{2}) = 0$. Si $f(x) = a_n x^n + \ldots + a_0$, se deduce desarrollando $2^n f(\frac{1}{2})$ que 2 divide a a_n. Luego $f(x) - (2x-1)\frac{a_n}{2}x^{n-1}$ es un polinomio de grado menor que f que cumple la misma propiedad. Se concluye por inducción que $f(x)$ es divisible por $2x - 1$. Luego $\mathbb{Z}[\frac{1}{2}] \cong \mathbb{Z}[x]/(2x-1)$.

Para tratar anillos como el del ejemplo precedente, probaremos una generalización del resultado anterior.

Proposición 8.7. *Si $f(x) = a_d x^d + \ldots$ es un polinomio de grado d con coeficientes en C, y si S es un conjunto completo de representantes de $C/(a_d)$ que incluye al* 0*, entonces todo elemento $h(x) \in C[x]$ de grado m puede escribirse en la forma $r(x) + x^d g(x) + q(x)f(x)$ donde* $\deg(r) < \deg(f)$ *y $g(x)$ es un polinomio de grado no mayor a $m - d$ con coeficientes en S. Si a_d no es un divisor de* 0*, esta representación es única.*

Demostración. Supongamos que $h(x)$ es un elemento de $C[x]$ con $h(x) = bx^n + \ldots$. Entonces existe $s \in S$ con $b - s = ta_d$ para algún $t \in C$. Luego $h_1(x) = h(x) - sx^n - tx^{n-d}f(x)$ tiene grado menor que h, y se concluye por inducción completa. Para probar la unicidad, supongamos que

$$h(x) = r(x) + x^d g(x) + q(x)f(x) = r_0(x) + x^d g_0(x) + q_0(x)f(x),$$

con r, r_0 de grado menor a d y g, g_0 con coeficientes en S. Entonces tenemos

$$(q_0(x) - q(x))f(x) = [r(x) - r_0(x)] + x^d[g(x) - g_0(x)]. \tag{8.1}$$

Supongamos que $q_0(x) \neq q(x)$. Sea $q_0(x) - q(x) = bx^r + \ldots$. El término de mayor grado en $(q_0(x) - q(x))f(x)$ es abx^{r+d}. El polinomio $g(x) - g_0(x)$ no puede tener ningún coeficiente no nulo divisible por a, y los términos de

grado mayor o igual a d en el lado derecho de (8.1) son exactamente los términos de $x^d[g(x) - g_0(x)]$. Se concluye que $q_0(x) = q(x)$, luego

$$r(x) - r_0(x) = -x^d[g(x) - g_0(x)].$$

Como el lado izquierdo tiene sólo términos de grado menor que d y el lado derecho tiene sólo términos de grado mayor o igual a d, deben ser ambos 0. □

Ejemplo 8.8. En el anillo $\mathbb{Z}[x]/(2x)$ cada elemento tiene una única representación de la forma $n+\bar{x}^{i_1}+\ldots+\bar{x}^{i_s}$ con $n \in \mathbb{Z}$ y enteros positivos $i_1, \ldots, i_s$ distintos. Este elemento no puede representarse por un polinomio de grado inferior al máximo de los i_t. De hecho, este anillo es isomorfo al subanillo de $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}[x]$ formado por los pares $\Big(n, f(x)\Big)$ tales que el resto de dividir n por 2 es $f(0)$. Para comprobar esto basta considerar el homomorfismo

$$\phi : \mathbb{Z}[x] \to \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}[x]$$

que envía a $f(x)$ en $\Big(f(0), \overline{f(x)}\Big)$, donde la barra horizontal indica reducción módulo 2.

Ejemplo 8.9. Sea $R = \mathbb{Z}/6\mathbb{Z}$. Tomamos $f(x) = 3x + 1 \in R[x]$. Obsérvese que $\{0, 1, 2\}$ es un conjunto completo de representantes de $\mathbb{Z}/3\mathbb{Z} = R/(3)$. Sin embargo x tiene al menos dos representaciones diferentes, a saber:

- $x = 2(3x + 1) - 2$, donde $q(x) = 2$, $g(x) = 0$, y $r(x) = -2$.
- $x = x$, donde $q(x) = 0$, $g(x) = x$, y $r(x) = 0$.

Por cierto, 3 es un divisor de 0.

Ejemplo 8.10. Sea $R = \mathbb{Z}$ tomando $f(x) = 3x + 1 \in R[x]$ se tiene que $\{1, 2, 3\}$ es un conjunto completo de representantes de $\mathbb{Z}/3\mathbb{Z}$ que no contiene al 0. El elemento $3x^2$ tiene al menos dos representaciones diferentes, a saber:

- $3x^2 = (x-1)(3x+1) + x(2) + 1$, donde $q(x) = x$, $g(x) = 2$, y $r(x) = 1$.
- $3x^2 = (-1)(3x + 1) + x(3x + 3) + 1$, donde $q(x) = 0$, $g(x) = 3x + 3$, y $r(x) = 1$.

Cálculos por teorema de isomorfía

Recordemos el segundo teorema de isomorfía. Según el cual si $I \subseteq J$ son ideales de C, existe un isomorfismo natural

$$\phi : C/J \xrightarrow{\cong} C/I \Big/ J/I.$$

Este resultado puede aplicarse para calcular cuocientes en anillos de polinomios. Ilustraremos esto con 2 ejemplos:

Ejemplo 8.11. Se nos pide determinar el conjunto de enteros primos p para los cuales el ideal principal (p) es primo en $\mathbb{Z}[i]$. Para ello observamos que $\mathbb{Z}[i]$ se identifica con el cociente $\mathbb{Z}[x]/(x^2+1)$. Luego

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[x]/(p, x^2+1) \cong \mathbb{F}_p[x]/(x^2+1).$$

Se concluye que (p) es primo en $\mathbb{Z}[i]$ si y sólo si (x^2+1) es primo en $\mathbb{F}_p[x]$. Veamos que este es el caso si y sólo si -1 es un cuadrado módulo p. Para esto observemos primero que todo polinomio con coeficientes en $\mathbb{Z}/p\mathbb{Z}$ se escribe en la forma $q(x)(x^2+1)+(ax+b)$. Se sigue que si (x^2+1) no es primo en $\mathbb{Z}/p\mathbb{Z}[x]$, existen a, b, c, d, y λ en $\mathbb{Z}/p\mathbb{Z}$ con $(ax+b)(cx+d) = \lambda(x^2+1)$. dividiendo por constantes puede suponerse que $a = c = \lambda = 1$, de donde $(x+b)(x+d) = x^2+1$. Se sigue que $b+d = 0$ y $bd = 1$, es decir $b(-b) = 1$. Por otro lado, cada b que satisface esta relación nos dá $(x-b)(x+b) = x^2+1$. Tal elemento b tiene orden $\frac{p-1}{4}$ en el grupo $(\mathbb{F}_p)^*$, por lo que no puede existir si $p \in 4\mathbb{Z}+3$. Se concluye que todo primo de la forma $4t+3$ genera un ideal primo en $\mathbb{Z}[i]$. Por otro lado, si $p = 4t+1$, siempre existe un elemento $b \in \mathbb{Z}/p\mathbb{Z}$ tal que $b^2 = -1$, ya que $(\mathbb{F}_p)^*$ es cíclico, y si a es un generador podemos tomar $b = a^{\frac{p-1}{4}}$.

Ejemplo 8.12. Calcularemos el cociente $\mathbb{Z}[i]/(1+i)$. Primero observamos que una preimagen bajo la evaluación en i de $1+i$ es el polinomio $1+x$, por lo que al identificar $\mathbb{Z}[i]$ con $\mathbb{Z}[x]/(1+x^2)$ se tiene el isomorfismo $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}[x]/(1+x, x^2+1)$. Cocientando ahora por $(1+x)$ (es decir evaluando en -1) se tiene que la imagen de x^2+1 es 2 y por lo tanto $\mathbb{Z}[x]/(1+x, x^2+1) \cong \mathbb{Z}/(2) = \mathbb{F}_2$. Se concluye que $\mathbb{Z}[i]/(1+i) \cong \mathbb{F}_2$. En particular, esto demuestra que el ideal principal $(1+i)$ es maximal en el anillo $\mathbb{Z}[i]$.

Ejemplo 8.13. Los ideales $(2, x)$ y $(3, x)$ en $\mathbb{Z}[x]$ son comaximales. Luego

$$\mathbb{Z}[x]/(2,x) \times \mathbb{Z}[x]/(3,x) \cong \mathbb{Z}[x]/\Big((2,x) \cap (3,x)\Big) = \mathbb{Z}[x]/(6,x). \qquad (8.2)$$

Dado que $(2,x)(3,x) = (6,2x,3x,x^2) = (6,x)$ (ya que $x = 3x - 2x$). Como $\mathbb{Z}[x]/(n,x) \cong \mathbb{Z}/n\mathbb{Z}$, el isomorfismo en (8.2) es el ya conocido isomorfismo $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Ejemplo 8.14. Los ideales (2) y (x) en $\mathbb{Z}[x]$ no son comaximales, aún cuando 2 y x no tienen factores comunes, de hecho son ambos primos. En particular, esto prueba que $\mathbb{Z}[x]$ no es un DIP. De hecho $\mathbb{Z}[x]/(2,x) \cong \mathbb{F}_2$ como se vió en el ejemplo precedente. La imagen del homomorfismo canónico

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x) \cong \mathbb{F}_2[x] \times \mathbb{Z},$$

no contiene al elemento $\Big(1 + (2), 2 + (x)\Big)$, pues si así fuese tendríamos

$$\Big(g + (2), g + (x)\Big) = \Big(1 + (2), 2 + (x)\Big),$$

de donde $g = 1 + 2r$ y $g = 2 + xs$, es decir $1 = 2r - xs$, y evaluando en 0 se tiene $1 = 2r(0)$.

Ejercicios

1. Sea $f \in \mathbb{R}[x_1, \ldots, x_n]$ tal que $f(a_1, \ldots, a_n) = 0$ para todo $a_i \in \mathbb{Z}$. Probar que $f = 0$ (sugerencia: inducción).

2. Sea K un cuerpo y sea A una K-algebra.

   a)Probar que A es un espacio vectorial sobre K.

   b) Si $\dim_K(A)$ es finita, probar que $\mathfrak{N}(A) = \mathfrak{R}(A)$.

Chapter 9

Factorización Unica

En este capítulo retomamos el problema de la factorización única. En todo el capítulo D representa un dominio de integridad. Recordemos que un elemento $p \in D$ se dice primo si para todo par de lementos a y b en D, $p|ab$ implica $p|a$ o $p|b$.

definición 9.1. Un elemento m de un dominio D se dice irreducible si para todo a y b en D, $ab = m$ implica $a \in D^*$ o bien $b \in D^*$. En particular, solo sus asociados y las unidades dividen a un irreducible.

Proposición 9.2. *Todo primo en un dominio de integridad es irreducible.*

Demostración Si $p = ab$ con p primo, entonces $p|a$ o $p|b$, sin pérdida de generalidad digamos $p|a$. Entonces $a = tp$ para algún t, pero entonces $tb = 1$, es decir $b \in D^*$. □

definición 9.3. Sea $n \in D$. Diremos que n es producto de primos, si existe una unidad u, primos $p_1, \ldots, p_t$ en D, y enteros no negativos $\alpha_1, \ldots, \alpha_t$, tales que $n = up_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$. Sin pérdida de generalidad, puede asumirse que para ningun par $i \neq j$ los elementos p_i y p_j son asociados.

Proposición 9.4. *Sea $n \in D$, tal que n es producto de primos, digamos $n = up_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ como arriba. Si además $n = vq_1^{\beta_1}, \ldots, q_s^{\beta_s}$ es una descomposición de n en irreducibles, ningun par (i, j) con q_i y q_j asociados, entonces $t = s$ y existe una permutación σ de $\{1, \ldots, n\}$ tal que p_i es asociado de $q_{\sigma(i)}$, y $\alpha_i = \beta_{\sigma(i)}$, para $i = 1, \ldots, n$.*

Demostración Por definición de primo p_1 debe dividir a algún q_j, como q_j es irreducible, los elementos p_1 y q_j deben ser asociados. La demostración termina por inducción en $\alpha_1 + \ldots + \alpha_t$. □

Sigue de la demostración anterior que un irreducible es producto de primos si y sólo si es primo.

Proposición 9.5. *El elemento mn es producto de primos si y sólo si m y n son ambos producto de primos. En tal caso la descomposición de mn se obtiene combinando las de m y n, agrupando los asociados.*

Demostración Es inmediato que si m y n son productos de primos, también lo es nm. Sea $nm = up_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$. Si nm es una unidad, tambien lo son n y m. Usamos inducción en $\alpha_1 + \ldots + \alpha_t$. Por definición de primo p_1 debe dividir o bien a m o bien a n. Supongamos que $m = p_1 m'$. Entonces $nm' = nm/p_1$ es producto de primos. Por hipótesis de inducción n y m' son producto de primos. En particular, $m = p_1 m'$ es producto de primos. La última afirmación es inmediata por unicidad. □

definición 9.6. Diremos que D es un dominio de factorización única (DFU) si cada elemento de D es producto de primos. Nótese que todo irreducible en un DFU es primo. En particular un DIP es un DFU.

definición 9.7. Dos elementos m y n en un DFU D se dicen relativamente primos, si ningún primo que divide a n divide a m e inversamente.

Proposición 9.8. *Si m, n son relativamente primos, y si $d|n$, y $d|m$ entonces $d \in D^*$.*

Demostración Basta considerar un primo que divida a d. □

definición 9.9. Si $\{p_1, \ldots, p_t\}$ es el conjunto de primos que dividen a m o n, y si

$$m = up_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}, \qquad n = vp_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t}$$

(donde α_i o β_i puede ser 0), entonces al elemento

$$\text{M.C.D.}(n, m) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_t^{\gamma_t},$$

donde $\gamma_i = \min\{\alpha_i, \beta_i\}$, se le llama el maximo común divisor de m y n. Es fácil probar que todo divisor común de n y m divide a su máximo común divisor.

En general no es cierto en un DFU que $(m) + (n) = (d)$ si d es el maximo común divisor de n y m. Veremos ejemplos de esto mas adelante.

Anillos de polinomios y factorización única

Es fácil ver que el anillo $D[x]$ no necesita ser un DIP, aún si D lo es, como lo demuestra el siguiente ejemplo.

Ejemplo 9.10. Los elementos 3 y x son relativamente primos en $\mathbb{Z}[x]$, pero $\mathbb{Z}[x]/(3,x) \cong \mathbb{Z}/3\mathbb{Z}$. En particular, el ideal $(3,x)$ no es principal (si lo fuese debiera ser (1), ya que este es en M.C.D. de 3 y x).

Sin embargo, si tenemos el resultado correspondiente para DFU's. Antes de probarlo, necesitamos algunos lemas. En todo lo que sigue, D denotará un DFU, y Q denotará su cuerpo de cocientes.

definición 9.11. Un polinomio $h(x) \in D[x]$ se dice primitivo si sus coeficientes son relativamente primos. Equivalentemente, $h(x)$ es primitivo si $h(x) = ug(x)$ con $u \in D$ y $g(x) \in D[x]$ implica $u \in D^*$.

Lema 9.12. *Todo polinomio $f(x) \in Q[x]$ puede escribirse como $f(x) = ah(x)$ con $h(x) \in D[x]$ primitivo y $a \in Q$. Ademas, Si $f(x)$ está en $D[x]$, entonces, necesariamente, $a \in D$. Finalmente, si $f(x) = ah(x) = a'h'(x)$ son dos representaciones de este tipo, entonces $a'/a \in D^*$.*

Demostración Para la existencia factorizamos los denominadores y despues cualquier factor común.

Sea $f(x) \in D[x]$, y $f(x) = ah(x)$, con $a = \frac{m}{s}$. Entonces s divide a ma_t para todo coeficiente a_t de $f(x)$. Como estos coeficientes son relativamente primos, debe dividir a m, luego $a \in D$.

Si $f(x) = ah(x) = a'h'(x)$, entonces $h(x) = (a'/a)h'(x)$, de donde $a'/a \in D$ y por simetría $a/a' \in D$. □

Observación 9.13. Un polinomio $f(x) \in D[x]$ es primitivo si y sólo si su imagen en $D/(p)[x]$ es no trivial para todo primo p de D.

Lema 9.14. *Si $g(x)$ y $f(x)$ son primitivos en $D[x]$, tambien lo es su producto $h(x) = f(x)g(x)$.*

Demostración Sea p un primo de D. Como f y g son primitivos, sus imágenes en $D/(p)[x]$ son no triviales, luego lo mismo es cierto para $h = fg$, ya que si C es un dominio de integridad también lo es $C[x]$. Como p es un primo arbitrario de D, h es primitivo. □

La proposición siguiente es de importancia en si misma:

Proposición 9.15. *Sea $p(x) \in D[x]$ de grado mayor o igual a 1. Entonces $p(x)$ es primo en $D[x]$ si y sólo si es primo en $Q[x]$ y primitivo en $D[x]$.*

Demostración Supongamos que $p(x)$ es primo en $D[x]$. Si $p(x) = rp_0(x)$ con $p_0(x)$ primitivo, entonces, por definición de primo, $r \in D^*$, luego $p(x)$ es primitivo. Si $p(x)|f(x)g(x)$ en $Q[x]$, entonces existe $t(x)$, tal que $p(x)t(x) = f(x)g(x)$. Si $t(x) = st_0(x)$ con $t_0(x)$ primitivo, si $f(x) = af_0(x)$ con $f_0(x)$ primitivo, y si $g(x) = ag_0(x)$ con $g_0(x)$ primitivo, entonces $p(x)t_0(x) = uf_0(x)g_0(x)$ con $u \in D^*$. Luego $p(x)|f_0(x)$ o $p(x)|g_0(x)$ en $D[x]$. Por lo tanto, $p(x)|f(x)$ o $p(x)|g(x)$ en $Q[x]$.

Supongamos ahora que $p(x)$ es primo en $Q[x]$ y primitivo. Sean $f(x)$ y $g(x)$ en $D[x]$ tales que $p(x)|f(x)g(x)$ en $D[x]$. Entonces $p(x)|f(x)$ o $p(x)|g(x)$ en $Q[x]$. Digamos, para fijar ideas, $p(x)|f(x)$. Entonces existe $t(x) \in Q[x]$, tal que $p(x)t(x) = f(x)$. Si $t(x) = st_0(x)$ con $t_0(x)$ primitivo, y si $f(x) = af_0(x)$ con $f_0(x)$ primitivo,entonces $p(x)t_0(x) = uf_0(x)$ con $u \in D^*$. Luego, $p(x)$ divide a $f_0(x)$ y por lo tanto a $f(x)$, ya que $a \in D$. Se concluye que $p(x)$ es primo en $D[x]$. □

Proposición 9.16. *Si D es un DFU entonces $D[x]$ es un DFU.*

Demostración Sea $f(x) \in D[x]$. Entonces, como $Q[x]$ es un DE (y por lo tanto un DFU), podemos escribir

$$f(x) = up_1(x)^{\alpha_1} \dots p_n(x)^{\alpha_n},$$

donde cada $p_i(x)$ es primo en $Q[x]$ y $u \in Q[x]^* = Q^*$. Sea $p_i(x) = b_i p_i'(x)$ con $p_i'(x)$ primitivo, entonces

$$f(x) = mp_1'(x)^{\alpha_1} \dots p_n'(x)^{\alpha_n},$$

con $m \in D$ y $p_i'(x)$ primo en $D[x]$. Ahora bien, cada primo (unidad) de D es primo (unidad) de $D[x]$ (ejercicio), luego m es producto de primos y unidades en $D[x]$. Se concluye que $f(x)$ es producto de primos y $D[x]$ es un DFU. □

Corolario 9.16.1. *Si D es un DFU, para todo entero positivo n, $D[x_1, \dots, x_n]$ es un DFU.*

Ejemplo 9.17. Si k es un cuerpo, el anillo $k[x_1, \dots, x_n]$ es un DFU.

Ejemplo 9.18. El anillo $\mathbb{Z}[x_1, \ldots, x_n]$ es un DFU, ya que $\mathbb{Z}$ es un DFU.

Ejemplo 9.19. El anillo $\mathbb{Z}[x, y, x^{-1}, y^{-1}]$ es un DFU, ya que es una localización de $\mathbb{Z}[x, y]$.

Terminaremos este capítulo mostrando como el método para calcular cocientes en anillos de polinomios explicado al final del capítulo 8 permite encontrar primos en anillos de la forma $\mathbb{Z}[\alpha]$.

Ejemplo 9.20. Probaremos que 29 no es primo en $\mathbb{Z}[i]$. De hecho

$$\mathbb{Z}[i]/(29) \cong \mathbb{Z}[x]/(x^2 + 1, 29) \cong \mathbb{F}_{29}[x]/(x^2 + 1),$$

Donde $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ (p primo) es el cuerpo con p elementos. Basta ahora comprobar si -1 es o no un cuadrado en $\mathbb{F}_{29}$. De hecho $12^2 \equiv 1 \pmod{29}$.

El mismo tipo de razonamiento prueba lo siguiente:

Proposición 9.21. *El primo p de $\mathbb{Z}$ es primo en el anillo $\mathbb{Z}[\alpha]$, donde α es raiz del polinomio mónico irreducible $f(x) \in \mathbb{Z}[x]$, si y sólo si la reducción de $f(x)$ módulo p (es decir, la imagen de $f(x)$ en $\mathbb{Z}/p\mathbb{Z}[x]$) es irreducible en el anillo $\mathbb{F}_p[x]$.* □

Por ejemplo, cualquier libro de teoría de números contiene métodos para calcular que elementos de $\mathbb{Z}/p\mathbb{Z}$ son cuadrados, de este modo podemos encontrar fácilmente los primos de $\mathbb{Z}[\sqrt{n}]$ para $n \in \mathbb{Z}$. Como no todo anillo de la forma $\mathbb{Z}[\sqrt{n}]$ es in DIP, este método no permite determinar si un elemento dado es o no irreducible. Observese que si $(a + b\sqrt{n})(c + d\sqrt{n}) = e + f\sqrt{n}$, entonces $(a - b\sqrt{n})(c - d\sqrt{n}) = e - f\sqrt{n}$, y multiplicando ambas identidades, $(a - nb^2)(c - nd^2) = e - nf^2$. En particular, si $a + b\sqrt{n}$ divide a $e + f\sqrt{n}$, entonces $a - nb^2$ divide a $e - nf^2$ en $\mathbb{Z}$. De aquí, si $n < 0$, es fácil determinar por ensayo y error si un elemento de D es irreducible.

Ejemplo 9.22. El elemento $4 + \sqrt{-5}$ no es primo en $\mathbb{Z}[\sqrt{-5}]$, de hecho

$$\begin{aligned}
&\mathbb{Z}[\sqrt{-5}]/(4 + \sqrt{-5}) \cong \mathbb{Z}[x]/(x^2 + 5, 4 + x) \\
&\cong \mathbb{Z}[x]/(x^2 + 5 - (x - 4)(x + 4), 4 + x) \\
&\cong \mathbb{Z}[x]/(21, 4 + x) \cong \mathbb{Z}/21\mathbb{Z},
\end{aligned}$$

y 21 no es primo en $\mathbb{Z}$. Sin embargo es irreducible (ejercicio).

Con lo anterior, tenemos las herramientas para dar un ejemplo donde la descomposición en irreducibles no es única.

Ejemplo 9.23. Sea $D = \mathbb{Z}[\sqrt{-5}]$. En particular, $21 = 3 \cdot 7 = (4+\sqrt{-5})(4-\sqrt{-5})$ y cada uno de los elementos 3, 7, $4+\sqrt{-5}$ y $4-\sqrt{-5}$, es irreducible. No pueden ser todos primos, por la unicidad de la factorización. De hecho, 21 no puede ser producto de primos en este anillo. De hecho ninguno es primo ya que 3 no divide a $4+\sqrt{-5}$ ni a $4-\sqrt{-5}$, y así sucesivamente. También se puede determinar caso por caso como en el ejemplo precedente.

Ejercicios

1. Sea p un primo en $\mathbb{Z}$. Probar que (p) es primo en $\mathbb{Z}[\sqrt{n}]$ si y sólo si n es un cuadrado en $\mathbb{Z}/p\mathbb{Z}$.

Chapter 10

Criterios de irreducibilidad

Recordemos que si α es una raiz de un polinomio primo $f(x) \in k[x]$, el anillo cociente $k[x]/(f(x))$ es isomorfo al cuerpo $k[\alpha]$. Por esta razón, el estudio de los polinomios primos sobre un cuerpo dado es de gran importancia en teoría de cuerpos, en particular, en teoría de extensiones algebraicas. En este capítulo, estudiaremos algunos criterios que nos permiten probar fácilmente que un polinomio dado es primo.

Proposición 10.1. *Si k y L son cuerpos, con $k \subseteq L$, y si para alguna raiz α de $f(x)$ se tiene que $[k[\alpha] : k] = \deg f$, entonces $f(x)$ es irreducible.*

Demostración Esto es inmediato ya que $[k[\alpha] : k] = \deg p$ donde p es el polinomio irreducible de α. Se sigue que si $[k[\alpha] : k] = \deg f$, entonces $p = f$. □

Lema 10.2. *Si $\alpha \in k$, el polinomio $x - \alpha$ es irreducible.*

Demostración Sigue de la observación de que la identidad $f(x) = g(x)h(x)$ implica $\deg f = \deg g + \deg h$. □

Lema 10.3. *Un polinomio $f(x) \in k[x]$ es divisible por $x - \alpha$ si y sólo si $f(\alpha) = 0$.*

Demostración Utilizando el algoritmo de división, se tiene que $f(x) = q(x)(x - \alpha) + c$ donde c es una constante. Evaluando en α, se tiene $c = f(\alpha)$. □

Proposición 10.4. *Un polinomio de grado* 2 *o* 3 *es irreducible si y sólo si tiene una raiz.*

Demostración Sigue del lema anterior si observamos que la identidad $f(x) = g(x)h(x)$ implica $\deg f = \deg g + \deg h$, luego algún factor debe tener grado 1. □

Proposición 10.5. *Sean D y D' dominios de integridad. Sea $\phi : D \to D'$ un homomorfismo de anillos, y sea $\tilde{\phi} : D[x] \to D'[x]$ la extensión que lleva x en x. Sea $f(x)$ un polinomio tal que $\deg \tilde{\phi}(f) = \deg f$. Si $\tilde{\phi}(f)$ no es producto de polinomios no constantes, entonces tampoco lo es f.*

Demostración Observese que si $f(x) = g(x)h(x)$, entonces $\tilde{\phi}(f) = \tilde{\phi}(g)\tilde{\phi}(h)$. Además, $\deg \tilde{\phi}(r) \leq \deg r$ para todo polinomio $r(x)$. Se sigue que la condición $\deg \tilde{\phi}(f) = \deg f$ implica que se tiene $\deg \tilde{\phi}(g) = \deg g$ y $\deg \tilde{\phi}(h) = \deg h$. Luego g es no constante si y sólo si $\tilde{\phi}(g)$ es no constante, y lo mismo es cierto de h. □

Observación 10.6. La condición $\deg \tilde{\phi}(f) = \deg f$ quiere decir que si $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, entonces $\phi(a_n) \neq 0$.

Corolario 10.6.1. *Sean D y D' dominios de integridad, con $D \subseteq D'$. Entonces si $f(x)$ no es producto de polinomios no constantes en $D'[x]$, entonces tampoco los es en $D[x]$.* □

Corolario 10.6.2. *Sea D un dominio de integridad, y sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in D[x]$. Sea $\wp$ un ideal primo con $a_n \notin \wp$. Luego, si la reducción módulo $\wp$ de $f(x)$ es irreducible, entonces $f(x)$ no es producto de polinomios no constantes.* □

Corolario 10.6.3. *Sea D un DFU, y sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in D[x]$. Sea $\wp$ un ideal primo con $a_n \notin \wp$. Luego, si la reducción módulo $\wp$ de $f(x)$ es irreducible, entonces $f(x)$ es primo en $\mathfrak{Quot}(D)[x]$.*

Demostración Por el corolario anterior, $f(x)$ no es producto de polinomios no constantes en $D[x]$, pero esto implica que es primo en $\mathfrak{Quot}(D)[x]$. □

Observación 10.7. Nótese que este criterio no implica que $f(x)$ es primo en $D[x]$. Por ejemplo, la reducción módulo 7 del polinomio $8(x^2 - 3)$ es primo, pero este polinomio no es primo en $\mathbb{Z}[x]$.

Corolario 10.7.1. *Sea $f(x, y_1, \ldots, y_m) \in k[x, y_1, \ldots, y_m]$, y supongamos que existe $(a_1, \ldots, a_m) \in k^m$ tal que $f(x, a_1, \ldots, a_m)$ es irreducible, entonces si*

$$f(x, y_1, \ldots, y_m) = g(x, y_1, \ldots, y_m)h(x, y_1, \ldots, y_m),$$

y si $f(x, a_1, \ldots, a_m)$ tiene el mismo grado en x que $f(x, y_1, \ldots, y_m)$, entonces uno de los polinomios g o h no depende de x. □

Ejemplo 10.8. El polinomio $f(x, y) = y^3x^2 - x = (y^3x - 1)x$, pero $f(x, 0)$ es irreducible. Esto prueba que la condición de que $f(x, a_1, \ldots, a_m)$ tiene el mismo grado en x que $f(x, y_1, \ldots, y_m)$ es necesaria.

En lo que sigue, D es un DFU y $k = \mathfrak{Quot}(D)$.

Proposición 10.9 (Criterio de Eisenstein)**.** *Sea $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in D[x]$. Sea p un primo de D que divide a a_i para $0 \leq i \leq n-1$, que no divide a a_n, y tal que p^2 no divide a a_0. Entonces $f(x)$ es irreducible en $k[x]$.*

Demostración sea $f(x) = g(x)h(x)$ con g y h no constantes. Reduciendo módulo p se tiene $\overline{f(x)} = \overline{a_nx^n}$. Como $\overline{f(x)} = \overline{g(x)h(x)}$ en el dominio factorial $\mathfrak{Quot}\Big(D/(p)\Big)[x]$, se sigue que $\overline{g(x)} = \overline{b_tx^t}$ y $\overline{h(x)} = \overline{c_rx^r}$ donde $t + r = n$. Se sigue que $g(x) = b_tx^t + pg_1(x)$ y $h(x) = c_rx^r + ph_1(x)$, donde p no divide a b_t ni a c_r. Comparando grados $\deg g \geq t$ y $\deg h \geq r$. Como $f(x) = g(x)h(x)$, se tiene $\deg g = t$ y $\deg h = r$. En particular r y t son positivos, de donde al evaluar en 0 se tiene $a_0 = f(0) = g(0)h(0) = p^2g_1(0)h_1(0)$. Esto contradice la hipótesis. □

Ejemplo 10.10. Si $f(x)$ es libre de cuadrados y no constante, entonces $y^n - f(x)$ es irreducible (basta aplicar el criterio de Eisenstein a cualquier divisor primo de $f(x)$.

Observación 10.11. Las hipótesis del criterio de Eisenstein para un polinomio $f(x)$ con respecto a un primo p pueden reescribirse como sigue:

- $f(x) \equiv ax^n \pmod{p}$, donde $n = \deg f$ y p no divide a a.
- p^2 no divide a $f(0)$.

Ejemplo 10.12. Sea $p \in \mathbb{Z}$ un primo, y sea

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1}.$$

Entonces

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} \equiv x^{p-1} \pmod{p}.$$

Por otro lado $\Phi_p(0+1) = \Phi(1) = p$. Luego se puede aplicar el criterio de Eisenstein a p y se tiene que $\Phi_p(x+1)$ es irreducible, luego también lo es $\Phi_p(x)$.

Observación 10.13. Para probar que $\Phi_p(x)$ es irreducible, sabiendo que $\Phi_p(x+1)$ lo es, uno puede argumentar como sigue: Existe un homomorfismo de anillos que lleva a $D[x]$ en si mismo, que es la identidad en D y lleva a x en $x+1$. También existe un homomorfismo de anillos que lleva a $D[x]$ en si mismo, que es la identidad en D y lleva a x en $x-1$. Como ambas funciones son inversas, son isomorfismos. En particular $f(x)$ es irreducible si y sólo si $f(x+1)$ lo es. Otro modo es tomar una raiz α de $f(x+1)$ en algún cuerpo que contenga k (por ejemplo, $k[x]/(f(x+1))$), argumentar que $k[\alpha] = k[\alpha + 1]$ y utilizar 10.1.

Observación 10.14. La irreducibilidad que garantiza el criterio de Eisenstein es en $k[x]$ y no en $D[x]$. Por ejemplo, $2x^2 - 6 = 2(x^2 - 3)$ no es irreducible en $\mathbb{Z}[x]$.

Observación 10.15. El criterio de Eisenstein no se aplica a polinomios del tipo $x^n - p^2$. Para probar la irreducibilidad de estos polinomios, necesitamos otro criterio más general, que es lo que estudiaremos en la sección siguiente. Notemos sin embargo que la irreducibilidad del polinomio en dos variables $x^n - y^m$ con n y m relativamente primos si puede demostrarse con lo que ya sabemos como se vé en el próximo ejemplo.

Ejemplo 10.16. Probaremos ahora que $x^n - y^m$ es irreducible si n y m son relativamente primos. Usaremos inducción en $n + m$. Supongamos que $n > m$. Como $x^n - y^m$ es primitivo si lo consideramos como un polinomio es $K[x][y]$, basta ver que es irreducible en $K(x)[y]$. Esto es equivalente a que $x^n - (xy)^m = x^m(x^{n-m} - y^m)$ sea irreducible en $K(x)[y]$. Para esto basta ver que $x^{n-m} - y^m$ es irreducible en $K(x)[y]$. Para esto basta ver que $x^{n-m} - y^m$ es irreducible en $K[x, y]$ y la hipótesis de inducción se aplica.

Ejercicios

1. Probar que $x^n - y$ es primo en el anillo $k[x, y]$.

2. Probar que si $g(x)^r | f(x)$, entonces $g(x)^{r-1} | f'(x)$. En particular, si $f(x)$ y $f'(x)$ no tienen divisores comunes, entonces $f(x)$ es libre de cuadrados.

3. Probar que si $f(x)$ es libre de cuadrados, entonces $y^n - f(x)$ es irreducible en $k[x, y]$.

4. Probar que $x^n + y^n + 1$ es irreducible en $k[x, y]$ si la característica de k no divide a n.

5. Probar que $x^3 + y^3 + z^3$ es irreducible en $k[x, y, z]$, si la característica de k no es 3.

6. factorizar $48x^{12} + 48y^{12}$ en $\mathbb{Z}[x, y]$.

7. Probar que si la reducción módulo p de un polinomio $f(x) \in \mathbb{Z}[x]$ es irreducible y del mismo grado que $f(x)$, entonces f es irreducible sobre $\mathbb{Z}$ (y por lo tanto sobre $\mathbb{Q}$).

8. Probar que x^4+x+1 es irreducible en $\mathbb{Q}[x]$ (sugerencia: probar módulo 2).

9. Probar que $y^2 - (ax^3 + bx + c)$ es irreducible en $\mathbb{Q}[x, y]$ para cualquier valor de a, b, y c.

10. Probar que los siguientes polinomios son irreducibles sobre $\mathbb{Q}$.

$$X^3 - 2,\ X^7 + 8X - 2,\ X^3 + (2t + 1)X - (2s + 3),\ X^9 - 2^{10}.$$

11. Probar que el polinomio ciclotómico $\phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1}$ es irreducible.

12. Probar que si $a \in K^*$, el polinomio $f(X)$ es irreducible en $K[X]$ si y sólo sí $f(aX)$ es irreducible. Concluir que si m y n son relativamente primos entonces $X^n + Y^m$ es irreducible (Sugerencia: usar algoritmo de la división).

Chapter 11

Polígonos de Newton

Sea D un DFU, p un primo de D.

definición 11.1. Sea $v_p : D \to \mathbb{Z}_{\geq 0}$, la valuación p-ádica en D. Es decir, para todo $b \in D$, $v_p(b)$ es el único entero t tal que $b = p^t c$ con p y c relativamente primos.

Observación 11.2. La valuación p-ádica en D tiene las siguientes propiedades, cuya demostración se deja al lector:

- $v_p(m_1 m_2) = v_p(m_1) + v_p(m_2)$.
- $v_p(m_1 + m_2) \geq \min\{v_p(m_1), v_p(m_2)\}$.
- Si $v_p(m_1) \neq v_p(m_2)$, entonces $v_p(m_1 + m_2) = \min\{v_p(m_1), v_p(m_2)\}$.

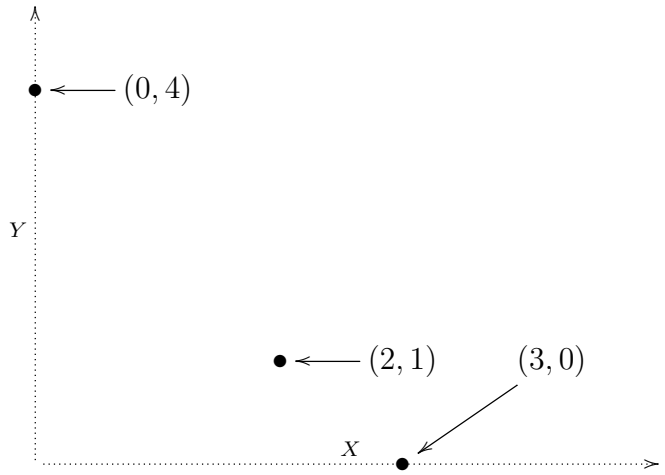
A cada monomio $ax^r \in D[x]$ le asociamos el punto del plano $\mathbb{R}^2$ dado por $z(ax^r) = (r, v_p(a))$. Sea

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in D[x].$$

Entonces, definimos $S_f = \{z(a_r x^r) | 0 \leq r \leq n\}$.

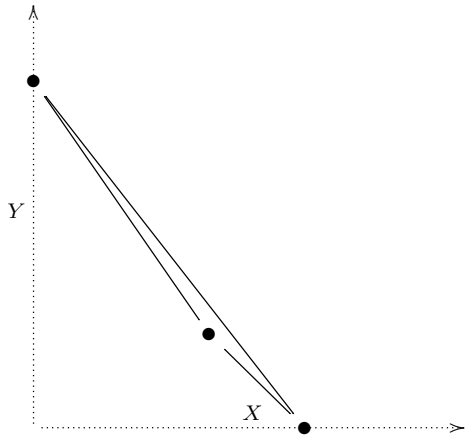
Ejemplo 11.3. Si $f(x) = x^3 + 4x + 16$ y $p = 2$, entonces S_f tiene 3 elementos.

De hecho $S_f = \{(0,4),(2,1),(3,0)\}$. En un diagrama:



definición 11.4. El polígono de Newton P_f de f se define como el menor polígono convexo que contiene a S_f.

En el ejemplo P_f es un triangulo:



definición 11.5. Sean α y β enteros, con $\beta > 0$, y sea $l(x,y) = \alpha x + \beta y$. Entonces, para todo monomio $ax^r \in D[x]$ le asociamos el peso

$$w(ax^r) = l(z(ax^r)) = \alpha r + \beta v_p(a).$$

Nótese que si μ_1 y μ_2 son monomios, se tiene $w(\mu_1\mu_2) = w(\mu_1) + w(\mu_2)$. Por otro lado si μ_1 y μ_2 son monomios del mismo grado entonces $w(\mu_1 + \mu_2) \geq \min(w(\mu_1), w(\mu_2))$. Además si $w(\mu_1) < w(\mu_2)$ entonces necesariamente $w(\mu_1 + \mu_2) = w(\mu_1)$, como se sigue de las propiedades de la valuación.

Sea ahora $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ un polinomio arbitrario. Nótese que para todo $(r, s) \in \mathbb{Z} \times \mathbb{Z}$, se tiene que $l(r, s) \in \mathbb{Z}$. Por lo tanto, los pesos de los monomios de f forman un conjunto finito de enteros, el cual debe tener un mínimo. Definimos

$$w(f) = \min_{(r,s)\in S_f} l(r, s) = \min_{r=1}^{n} w(a_r x^r).$$

Sea $E_-(f) = a_{e_-(f)}x^{e_-(f)}$ el monomio de menor grado cuyo peso es $w(f)$. Del mismo modo sea $E_+(f) = a_{e_+(f)}x^{e_+(f)}$ el monomio de mayor grado cuyo peso es $w(f)$.

Proposición 11.6. *Si $f(x) = g(x)h(x)$, entonces $w(f) = w(g) + w(h)$. Además se tiene $e_-(f) = e_-(g) + e_-(g)$ y $e_+(f) = e_+(g) + e_+(g)$.*

Consideremos los monomios $b_v x^v$ y $b_V x^V$ de g con $v = e_-(g)$ y $V = e_+(g)$. Del mismo modo, consideremos los monomios $c_u x^u$ y $c_U x^U$ con $u = e_-(h)$ y $U = e_+(h)$. En particular, $v \leq V$ y $u \leq U$.

Entonces $w(b_v c_u x^{v+u}) = w(b_v x^v) + w(c_u x^u) = w(g) + w(h)$. El monomio $a_{v+u}x^{v+u}$ de f satisface

$$a_{v+u} = c_{v+u}b_0 + c_{v+u-1}b_1 + \ldots + c_u b_v + \ldots + c_1 b_{v+u-1} + c_0 b_{v+u}. \qquad (11.1)$$

Para cada monomio $c_i x^i$ tenemos $w(c_i x^i) \geq w(h)$, o equivalentemente

$$v_p(c_i) \leq \beta^{-1}\Big(w(h) - i\alpha\Big),$$

y por la minimalidad de u, esta desigualdad es estricta cada vez que $i < u$. Del mismo modo, para cada monomio $b_j x^j$ tenemos

$$v_p(b_j) \leq \beta^{-1}\Big(w(g) - j\alpha\Big),$$

y esta desigualdad es estricta cada vez que $j < v$. Se sigue que

$$v_p(c_u b_v) = \beta^{-1}\Big(w(h) + w(g) - (u + v)\alpha\Big)$$

y cualquier otro sumando en (11.1) tiene una valuación mayor. Se concluye que $w(a_{v+u}x^{v+u}) = w(g) + w(h)$. Se sigue que $w(f) \leq w(g) + w(h)$.

Por otro lado, se demuestra $w(f) \leq w(g) + w(h)$ fácilmente de la correspondiente propiedad para monomios. Como además cada monomio de grado menor a $v + u$ es suma de monomios con grado mayor a $w(g) + w(h)$, por el mismo argumento usado arriba para probar que "cualquier otro sumando en (11.1) tiene una valuación mayor", se tiene que $e_-(f) = u+v = e_-(g)+e_-(h)$. La demostración de que $w(a_{V+U}x^{V+U}) = w(f)$ y de que este es el mayor monomio con esa propiedad es similar. Se concluye que $e_+(f) = U + V = e_+(g) + e_+(h)$. □

Elijamos α y β enteros, con $\beta > 0$, $(\alpha, \beta) = (1)$, y tales que l alcanza el mínimo en al menos dos puntos de S_f. En otras palabras, se escoge la recta $L = \{(x, y)|\alpha x + \beta y = \gamma\}$ de modo que al menos dos puntos de S_f estén en ella y el resto quede por encima. Otra manera de decir esto es que la recta L es un lado inferior de P_f. En particular se tiene que $w(f) = \gamma$, y que $e_-(f) < e_+(f)$. Por ejemplo, en el polinomio que corresponde a la Figura 12.4 se puede tomar $\alpha = 3$ y $\beta = 2$, lo que corresponde a la recta que pasa por $(0, 4)$ y $(2, 1)$, o bien $\alpha = \beta = 1$, lo que corresponde a la recta que pasa por $(2, 1)$ y $(3, 0)$.

Sea $t = e_-(f)$ y $T = e_+(f)$. Entonces los extremos de $L \cap S_f$ son $(t, \nu_p(a_t))$ y $(T, \nu_p(a_T))$. De la identidad $l(t, \nu_p(a_t)) = l(T, \nu_p(a_T)) = \gamma$ se obtiene que $\alpha(T - t) = -\beta(\nu_p(a_T) - \nu_p(a_t))$. Como α y β son relativamente primos, se tiene que $(T - t) = m\beta$, y $\nu_p(a_T) - \nu_p(a_t) = -m\alpha$. Además, m es el máximo común divisor de $(T - t)$ y $\nu_p(a_T) - \nu_p(a_t)$. En particular, $m \geq 1$.

Proposición 11.7 (Criterio de Dumas)**.** *Si $f(x) = g(x)h(x)$ en $D[x]$, con g y h no constantes, entonces existen enteros m_1, m_2, t_1, y t_2, tales que $m_1 + m_2 = m$, $t_1 + t_2 = n - m\beta$, $\deg(g) = m_1\beta + t_1$ y $\deg(h) = m_2\beta + t_2$.*

Demostración Supongamos que $f(x) = g(x)h(x)$ en $D[x]$. Sean $\gamma_1 = w(g)$ y $\gamma_2 = w(h)$. Entonces $w(f) = \gamma = \gamma_1 + \gamma_2$.

Sean $v = e_-(g)$, $V = e_+(g)$, $u = e_-(h)$ y $U = e_+(h)$. En las notaciones del parrafo previo se tiene $T = V + U$ y $t = v + u$. Se concluye que $m\beta = T - t = (V - v) + (U - u)$. Además, como $w(b_v x^v) = w(b_V x^V) = \gamma_1$, se tiene que

$$\alpha(V - v) = \beta(\nu_p(b_V) - \nu_p(b_v)).$$

Como α y β son relativamente primos, se tiene que $V - v = m_1\beta$. Del mismo modo, $U - u = m_2\beta$ con $m_1 + m_2 = m$. Además $V - v \leq \deg(g)$, luego

$\deg(g) = m_1\beta + t_1$ con $t_1 \geq 0$. Del mismo modo $\deg(h) = m_2\beta + t_2$ con $t_2 \geq 0$. Finalmente, $n = \deg(f) = \deg(g) + \deg(h) = m\beta + (t_1 + t_2)$. □

Corolario 11.7.1. *En lla situación anterior, se tiene que*

$$\max\{\deg(g), \deg(h)\} \geq \beta. \quad \square$$

Corolario 11.7.2. *Si puede elegirse $\beta = n$, entonces f es irreducible.* □

Ejemplo 11.8. Si $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in D[x]$, y si p un primo de D que divide a a_i para $0 \leq i \leq n-1$, que no divide a a_n, y tal que p^2 no divide a a_0, entonces podemos tomar $l(x, y) = x + ny$, luego $f(x)$ es irreducible en $k[x]$. Esto prueba que el criterio de Dumas implica el criterio de Eisenstein.

Ejemplo 11.9. Sea $x^n + a$ cor n y $v_p(a)$ relativamente primos. Entonces $S_f = \{(0, m), (n, 0)\}$. Luego, se puede tomas $l(x, y) = v_p(a)x + ny$, por lo que el polinomio es irreducible.

Ejemplo 11.10. Sea $f(x) = x^n + px + ap^2$, con $a \in D$, p primo. Entonces $S_f = \{(0, k), (1, 1), (n, 0)\}$, donde $k = 2 + v_p(a) \geq 2$. Entonces se puede tomar $\alpha = 1$, $\beta = n - 1$ (sugerimos dibujar el polígono en este caso). Luego, si $f(x)$ es reducible, debe tener una raiz.

Ejemplo 11.11. En el polinomio que corresponde a la Figura 12.4 se puede tomar $\alpha = 3$ y $\beta = 2$, como mencionamos mas arriba. En este caso, el criterio nos dice que al menos un polinomio debe tener grado 2 o mayor, lo que es evidente. En este caso no tenemos información nueva a partir del Corolario 11.7.1.

Chapter 12

Módulos

definición 12.1. Sea R un anillo. Un R-módulo (M, ϕ) es un grupo abeliano M, junto con un homomorfismo de anillos unitarios $\phi : R \to \mathrm{End}(M)$, donde $\mathrm{End}(M)$ es el anillo de endomorfismos de M (es decir homomorfismos de grupo de M en si mismo). Todo R-módulo define una operación de *multiplicación por escalares* que envía el par (r, m) en el elemento $r.m = \phi(r)(m)$. Además, esta operación satisface las propiedades siguientes:

- Ley distributiva izquierda: $(r_1 + r_2).m = r_1.m + r_2.m$.
- Ley distributiva derecha: $r.(m_1 + m_2) = r.m_1 + r.m_2$.
- Ley de identidad: $1_R.m = m \forall m \in M$.
- Ley asociativa mixta: $(r_1 r_2).m = r_1.(r_2.m)$ (donde la multiplicación dentro del primer paréntesis es la multiplicación del anillo).

Conversamente, toda operación de $R \times M$ en M que cumple estas condiciones define una estructura de R-módulo en el grupo abeliano M.

Ejemplo 12.2. Todo espacio vectorial sobre un cuerpo k es un k-módulo y conversamente.

Ejemplo 12.3. Si A es un grupo abeliano y $R \subseteq \mathrm{End}(A)$, donde $\mathrm{End}(A)$ es el anillo de endomorfismos (de grupos abelianos) de A, entonces A es un R-módulo.

Ejemplo 12.4. Si R es un anillo arbitrario, entonces R^n es un R-módulo y también un $\mathbb{M}_n(R)$-módulo con las operaciones usuales.

Ejemplo 12.5. Si C es un anillo conmutativo y B es una C-álgebra, entonces B es un C-módulo.

Ejemplo 12.6. Todo grupo abeliano es un $\mathbb{Z}$-módulo de manera única.

Ejemplo 12.7. Si V es un espacio vectorial sobre k, y si $T : V \to V$ es una función k-lineal, entonces V es un $k[x]$-módulo mediante $f(x).v = f(T)(v)$.

Ejemplo 12.8. Más generalmente, si R es un anillo conmutativo, y si (M, ϕ) es un R-módulo, entonces definimos el anillo de endomorfismos de R-módulo de M por

$$\mathrm{End}_R(M) = \{T \in \mathrm{End}(M) | r.T(m) = T(r.m)\ \forall r \in R,\ m \in M\}.$$

Este anillo es de hecho $C_{\mathrm{End}_{(M)}}(\phi(R))$, el anillo de endomorfismos de M que conmutan con $\phi(R)$. Entonces, para todo $T \in \mathrm{End}_R(M)$, la operación $f(x).m = f(T)(m)$ convierte a M en un $R[x]$-módulo.

Ejemplo 12.9. Si M y N son R-módulos, tambien lo es $M \times N$ con las operaciones por componente. Del mismo modo, si $\{M_i\}_{i\in I}$ es una familia arbitraria de R-módulos, también son R-módulos los grupos

$$\prod_{i\in I} M_i = \{(a_i)_{i\in I} | a_i \in M_i\},$$

y

$$\bigoplus_{i\in I} M_i = \left\{ (a_i)_{i\in I} \in \prod_{i\in I} M_i \Big| a_i = 0 \text{ para todo } i \text{ salvo un número finito} \right\}.$$

teoremas de isomorfía

definición 12.10. Sea M un R-módulo, y sea N un subgrupo de M. Diremos que N es un R-submódulo de M si es un R-módulo con respecto a la misma multiplicación escalar de M. En este caso, es fácil ver que el cociente de grupos M/N es también un R-módulo.

En teoría de R-módulos, tenemos los equivalentes a los tres teoremas de isomorfía de teoría de grupos, los cuales suiguen fácilmente de sus equivalentes para grupos abelianos.

Proposición 12.11. *Sea $\phi : M \to N$ un homomorfismo de R-módulos, entonces existe un isomorfismo*

$$\tilde{\phi} : M/\ker(\phi) \xrightarrow{\cong} \phi(M).$$

Demostración La existencia de $\tilde{\phi}$ sigue del resultado correspondiente en teoría de grupos. Falta probar que $\tilde{\phi}$ es un homomorfismo de R-módulos, pero esto es inmediato de

$$\tilde{\phi}(r.(m+\ker\phi)) = \tilde{\phi}(r.m+\ker\phi) = \phi(r.m)$$

$$= r.\phi(m) = \tilde{\phi}(m+\ker\phi). \quad \square$$

Corolario 12.11.1. *Sea M un R-módulo finitamente generado. Entonces M es isomorfo a un cociente de R^n para algún n.*

Demostración Por definición, M es la imagen de R^n por una función epiyectiva, luego el resultado sigue de el primer teorema de isomorfía. $\square$

Las demostraciones de los resultados siguientes son análogas a las del primer teorema de isomorfía y se dejan al lector.

Proposición 12.12. *Sea M un R-módulo. Sean N un submódulo. Entonces existe una correspondencia entre submódulos de M/N y submódulos de M que contienen a N dada por $P \leftrightarrow P/N$.*

Proposición 12.13. *Sea M un R-módulo. Sean $P \subseteq N$ submódulos, entonces entonces existe un isomorfismo*

$$\psi : M/N \xrightarrow{\cong} (M/P)/(N/P). \quad \square$$

Proposición 12.14. *Sea M un R-módulo. Sean P y N submódulos, entonces también lo son $P+N$ y $P \cap N$. Además existe un isomorfismo*

$$\rho : (P+N)/P \xrightarrow{\cong} N/(P \cap N). \quad \square$$

Módulos libres y generadores

definición 12.15. Un R-módulo es libre si es isomorfo a un módulo del tipo

$$R_I = \bigoplus_{i \in I} R,$$

Para algún conjunto de índices I.

Ejemplo 12.16. Tomando $I = \{1, \ldots, n\}$, vemos que R^n es un R-módulo libre para todo n.

definición 12.17. Sea M un R-módulo, y sea S un subconjunto de M. El submódulo generado por S es el submódulo mas pequeño que contiene a S. Este submódulo será denotado $R.S$ y se tiene que

$$R.S = \left\{ \sum_{i=i}^{t} r_i s_i \,\middle|\, r_i \in R, s_i \in S \right\}.$$

En particular, $N \subseteq M$ es un submódulo si y sólo si $R.N \subseteq N$.

definición 12.18. Diremos que S genera M si $R.S = M$. Si S puede escogerse finito, diremos que M es finitamente generado.

Ejemplo 12.19. El conjunto $S = \{e(i)\}_{i\in I} \subseteq R_I$ definidos por $e(i)_j = 1$ si $j = i$, $e(i)_j = 0$ si $j \neq i$, genera el R-módulo R_I. De hecho, para todo $a = (a_i)_i \in R_I$ podemos escribir

$$a = \sum_i a_i e(i) = \sum_{\substack{i \\ a_i \neq 0}} a_i e(i),$$

donde la última suma es finita por definición de R_I. El conjunto S se llama el conjunto de generadores canónicos de R^n.

definición 12.20. Sean (ϕ, M) y (ϕ', M') dos R-módulos. un homomorfismo de grupos abelianos $f : M \to M'$ es un homomorfismo de R-módulos si y sólo si para todo $r \in R$ y todo $m \in M$, se tiene $r.f(m) = f(r.m)$.

Proposición 12.21. *Sea M un R-módulo arbitrario. Sea $\psi : I \to M$ una función arbitraria. entonces existe un único homomorfismo de R-módulos $\phi : R_I \to M$ tal que $\phi(e(i)) = \psi(i)$.*

Demostración Si $a = (a_i)_i \in R_I$ se define un homomorfismo $\phi : R_I \to M$ por

$$\phi(a) = \sum_i a_i \psi(i) = \sum_{\substack{i \\ a_i \neq 0}} a_i \psi(i),$$

donde la suma es finita por definición de R_I. Dejamos al lector la rutinaria demostración de que esta función es un homomorfismo de módulos. □

definición 12.22. Un conjunto de generadores S del R-módulo F se llama un conjunto libre de generadores si toda función $\psi : S \to M$, para todo R-módulo M, se extiende a un único homomorfismo $\phi : F \to M$ tal que $\phi(s) = \psi(s)$ para todo $s \in S$. En particular, Un R-módulo libre R^I tiene un conjunto libre de generadores $S = \{e(i)|i \in I\}$. Por otro lado, si M tiene un conjunto libre de generadores S, entonces existen homomorfismos $\phi : R^S \to M$ y $\psi : M \to R^I$ tales que $\phi[e(s)] = s$ y $\psi(s) = e(s)$. Estos homomorfismos son inversos ya que $\phi \circ \psi(s) = s$ y $\psi \circ \phi[e(s)] = e(s)$ y por la unicidad se tiene $\phi \circ \psi = \mathrm{Id}_M$, $\psi \circ \phi = \mathrm{Id}_{R^I}$.

Observación 12.23. Para todo módulo M existe un homomorfismo epiyectivo de algún módulo libre en M. De hecho, existe un homomorfismo epiyectivo de R_M en M. Mas generalmente, Si S es un conjunto de generadores de M, existe un epimorfismo de R_S en M. En particular $M = R_S/K$ donde K es un submódulo llamado el submódulo de relaciones de M. Con estas definiciones es posible definir un módulo por generadores y relaciones tal como se hizo para álgebras. Un módulo es finitamente generado si y sólo si existe un homomorfismo epiyectivo de R^n en M.

Un homomorfismo de R^n en R^m está definido por una matriz cuyas filas corresponden a las coordenadas de las imagenes de los generadores canónicos de R^n. Por ejemplo, la matriz

$$\begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}$$

describe la función de R^3 en R^2 que envía $(1,0,0)$ en (a,b) y $(0,1,0)$ en (c,d), y a $(0,0,1)$ en (e,f). Las matrices operan por multiplicación por la derecha mientras los escalares multiplican por la izquierda del siguiente modo:

$$(1,0,0)\begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix} = (a,b), \qquad 3(1,0,0) = (3,0,0).$$

Con esta definición, composición de funciónes corresponde a multiplicación de matrices del siguiente modo: AB corresponde a la función lineal $T_B \circ T_A$. Con esta definición, R^n no es un $\mathbb{M}_n(R)$-módulo, sino un $\mathbb{M}_n(R)^c$-módulo, donde R^c es el anillo opuesto de R, es decir R con la multiplicación opuesta $a * b = ba$. Si R es conmutativo, se tiene la relación $(AB)^t = B^t A^t$,

donde A^t es la transpuesta de A. En particular, R^n es además un $\mathbb{M}_n(R)$-módulo, con la multiplicación $A.m = mA^t$.

Recordemos, como se probó en el capítulo 8, que si C es un anillo conmutativo y A es una matriz con coeficientes en C, entonces A es invertible si y sólo si su determinante lo es. Ahora, si A es una matriz de n filas y m columnas, con $n > m$, y si $AB = 1$ es la identidad de n por n, entonces puede completarse A y B a matrices cuadradas agragando columnas (o filas) de ceros y aun se tiene $AB = 1$. Pero una matriz con una columna de ceros debe tener determinante 0. Esta contradicción demuestra el siguiente resultado:

Proposición 12.24. *Sea C un anillo conmutativo. Entonces $C^n \cong C^m$ implica $n = m$.* □

Es posible, aunque no sencillo, construir ejemplos de anillos no conmutativos para los que esta propiedad es falsa. Por esta y otras razones, no parece posible extender la teoría de determinantes al caso no conmutativo.

Bimódulos

definición 12.25. Sean R y A anillos. Sea M un R-módulo que es a la vez un A^{op}-módulo. Entonces M se dice un (R, A)-bimódulo, si:

$$r.(a.m) = a.(r.m) \qquad \forall r \in R \forall a \in A \forall m \in M. \tag{12.1}$$

Por comodidad, si M es un (R, A)-bimódulo, se escribe $r.m.a$ o rma en vez de $r.(a.m)$. En cuyo caso, para $r, r' \in R$ y $a, a' \in A$ se tiene

$$(rr')m(aa') = r(r'ma)a'.$$

En términos de los homomorfismos $\phi : R \to \text{Hom}(M)$ y $\psi : A^{\text{op}} \to \text{Hom}(M)$, la condición (12.1) se reescribe $\phi(r)\psi(a) = \psi(a)\phi(r)$ para todo $r \in R$ y todo $a \in A$.

El principal ejemplo de bimódulo es R^n como un $\Big(R, \mathbb{M}_n(R)\Big)$-bimódulo. Mas generalmente, si I es un ideal bilátero de R, y si $\mathbb{M}_{n\times m}(I)$ es el grupo abeliano de matrices de n por m con coeficientes en I, entonces $\mathbb{M}_{n\times m}(I)$ es un $\Big(\mathbb{M}_n(R), \mathbb{M}_m(R)\Big)$-bimódulo con la operación de multiplicación de matrices. La demostración se deja como ejercicio al lector.

Producto tensorial de módulos

Otra construcción importante relacionada con módulos es la de producto tensorial. Sean A, B, y C tres anillos. Sea M un (A, B)-módulo y sea N un (B, C)-módulo. El producto tensorial $M \otimes_B N$ es el (A, C)-módulo generado por los elementos $m \otimes n$ con $m \in M$ y $n \in N$, y sujeto a las relaciones:

- $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$.
- $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$.
- $(mb) \otimes n = m \otimes (bn)$ for any $b \in B$.
- $(am) \otimes n = a(m \otimes n)$ for any $a \in A$.
- $m \otimes (nc) = (m \otimes n)c$ for any $c \in C$.

Con esta definición, se tiene que el producto tensorial satisface la siguiente propiedad universal: Si Z es un (A, C)-bimódulo y $\phi : M \times N \to Z$ es una función que satisface las propiedades siguientes:

- $\phi(m_1 + m_2, n) = \phi(m_1, n) + \phi(m_2, n)$.
- $\phi(m, n_1 + n_2) = \phi(m, n_1) + \phi(m, n_2)$.
- $\phi(mb, n) = \phi(m, bn)$ for any $b \in B$.
- $\phi(am, n) = a\phi(m, bn)$ for any $a \in A$.
- $\phi(m, nc) = \phi(m, n)c$ for any $c \in C$.

(a la que llamaremos una función central lineal) entonces existe un único homomorfismo $\psi : M \otimes_B N \to Z$ de grupos abelianos tal que

- $\psi\Big(am \otimes n\Big) = a\psi\Big(m \otimes n\Big)$ for any $a \in A$.
- $\psi\Big(m \otimes nc\Big) = a\psi\Big(m \otimes n\Big)c$ for any $c \in C$.

Ejemplo 12.26. Todo grupo abeliano es un $(\mathbb{Z}, \mathbb{Z})$-bimódulo con la multiplicación usual. Si $A = \mathbb{Z}/12\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/8\mathbb{Z}$, entonces

$$4(1 \otimes 1) = (12 - 8)(1 \otimes 1) = (12 \times 1) \otimes 1 - 1 \otimes (8 \times 1) = 0.$$

Por otro lado la función central lineal $\phi : \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ definida por $\phi(a + 12\mathbb{Z}, b + 8\mathbb{Z}) = ab + 4\mathbb{Z}$, prueba que de hecho $A \cong \mathbb{Z}/4\mathbb{Z}$.

Ejemplo 12.27. Si R es un anillo arbitrario, entonces R^n es un (R,R)-bimódulo con las operaciones

$$r(a_1,\ldots,a_n)t = (ra_1t,\ldots,ra_nt).$$

El (R,R)-bimódulo $R^n \otimes_R R^m$ está generado por los elementos $e_i \otimes e_j$ y se tiene $r(a\otimes b)s = (ra)\otimes(bs)$. Como R^m es de hecho un $\Big(R, \mathbb{M}_m(R)\Big)$-bimódulo, se tiene que $R^n \otimes_R R^m$ también lo es.

Ejemplo 12.28. Si R^{n*} denota el (R,R)-bimódulo de columnas

$$\begin{pmatrix} a_1 \\ \vdots a_n \end{pmatrix},$$

entonces R^{n*} es también un $\Big(\mathbb{M}_n(R), R\Big)$-bimódulo. Se sigue que $R^{n*} \otimes_R R^m$ es un $\Big(\mathbb{M}_n(R), \mathbb{M}_m(R)\Big)$-bimódulo. Está generado por los elementos $e_i^* \otimes e_j$, donde e_i^* es la columna con un 1 en la j-ésima fila y 0's en el resto. Podemos identificar R^m con $\mathbb{M}_{1\times m}(R)$ and R^{n*} con $\mathbb{M}_{n\times 1}(R)$, de donde la función $\phi(v,w) = vw$ dada por el producto matricial nos dá un homomorfismo $\psi : R^{n*} \otimes_R R^m \to \mathbb{M}_{n\times m}(R)$ que envía el elemento $e_i^* \otimes e_j$ en la matriz $E_{i,j}$. Este homomorfismo es epiyectivo (dado que cada $E_{i,j}$ está en la imágen), e inyectivo (ejercicio), luego es un isomorfismo de (R,R)-bimódulos. De hecho es también un isomorfismo de $\Big(\mathbb{M}_n(R), \mathbb{M}_m(R)\Big)$-bimódulos.

Por ejemplo, identificando los elementos de $R^{n*} \otimes_R R^m$ con los de $\mathbb{M}_{n\times m}(R)$ se tiene:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}.$$

Si

$$P = \begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix}, \qquad Q = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}, \qquad A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

entonces PAQ es la matriz que corresponde al tensor

$$\begin{pmatrix} 3 & 4 \\ 0 & 5 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} 3 & 4 \\ 0 & 5 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}.$$

Ejercicios

1. Demuestre las proposiciones 17.12, 17.13 y 17.14.

2. Sea M un R módulo y sea X un conjunto arbitrario. Demuestre que el conjunto M^X de todas las funciones de X en M es un R-módulo. Demuestre que R^X es un anillo y que M^X es un R^X-módulo con las operaciones por componente. Si M es un R-módulo finitamente generado, es M^X un R^X-módulo finitamente generado?

3. Sea R el anillo de polinomios en las variables $x_1, x_2, x_3, \ldots$. Cada elemento de R depende de un número finito pero no acotado de variables. Sea I el ideal de todos los polinomios sin término constante. Probar que I no es finitamente generado como ideal, es decir como R-módulo.

4. Puede un módulo finitamente generado tener un submódulo que no sea finitamente generado? (Sugerencia: utilizar el problema anterior).

5. Sea R un anillo con cuatro elementos a, b, c y d que satisfacen $ac = bd = 1$, $ad = bc = 0$ y $ca + db = 1$. Probar que R y R^2 son isomorfos como R-mdulos.

6. Sea R un anillo y sea M un R-mdulo. Probar que M^n es un $\mathbb{M}_n(R)$-módulo.

7. Sea $R \cong R_1 \times R_2$ un anillo y sea M un R-mdulo. Probar que existe un R_1-módulo M_1 y un R_2-módulo M_2 tal que $M \cong M_1 \times M_2$ con la multiplicación escalar $(r_1, r_2)(m_1, m_2) = (r_1 m_1, r_2 m_2)$.

8. Sea R un anillo y sea M' un R'-mdulo con $R = \mathbb{M}_n(R)$. Probar que $M' = M^n$ para angún R-módulo M (Sugerencia: R' tiene un subanillo isomorfo a R^n, por lo que puede aplicarse el ejercicio precedente).

9. Sea M un (R, R')-módulo. Probar que el conjunto de matrices de la forma $\begin{pmatrix} r & m \\ 0 & r' \end{pmatrix}$ con $r \in R$, $r' \in R'$ y $m \in M$ es un anillo.

Chapter 13

Módulos sobre DIPs

En este capítulo asumiremos que D es un DIP. Además, todos los D-módulos considerados serán finitamente generados.

Proposición 13.1. *Todo submódulo N de un D-módulo libre M en n generadores es libre en $m \leq n$ generadores.*

Demostración Sin pérdida de generalidad, asumimos que $M = D^n$. Utilizaremos inducción en n.

Escribiremos $a = (a_1, \ldots, a_n)$ para un elemento de D^n. Sea $J = \{a_1 | a \in N\}$. Entónces J es un ideal de D (ejercicio). Se sigue que $J = (b_1)$ para algún $b \in N$. Afirmamos que $N = D.b + N'$, donde N' es el submódulo de elementos que tienen la primera cordenada 0. De hecho, si c es un elemento arbitrario de N, entonces $c_1 = tb_1$ para algún $t \in D$, y por lo tanto la primera coordenada de $c - tb$ es nula, lo que demuestra la afirmación. supongamos ahora que $d.b + n' = 0$ con $d \in D$ y $n' \in N'$. Tomando la primera coordenada se tiene $db_1 = 0$. Como D es un dominio de integridad, esto implica $d = 0$. Se concluye que $N \cong D.b \times N'$. Como N' está contenido en $\{0\} \times D^{n-1}$, por inducción se obtiene el resultado. □

Lema 13.2. *Sea M un D-módulo finitamente generado. Entonces existe una función inyectiva $\phi : D^m \to D^n$, con $m \leq n$, tal que*

$$M \cong D^n / \phi(D^m).$$

Demostración Inmediata de 13.1 y del Corolario 12.11.1 □

Observación 13.3. El homomorfismo de D-módulos $\phi : D^m \to D^n$, tiene una representación matricial (en términos de los generadores canónicos de D^m y D^n). La matriz que representa la función ϕ en este sentido es la matriz con n filas y m columnas, tal que la j-ésima columna da las cordenadas en D^n de la imagen del elemento de D^m que tiene 1_D en la j-ésima cordenada y 0's en el resto. Por ejemplo, si $n = 3$ y $m = 2$, y si ϕ lleva los elementos $(1_D, 0_D)$ y $(0_D, 1_D)$ a (x, y, z) y (u, v, w), la matriz correspondiente es

$$\begin{pmatrix} x & y & z \\ u & v & w \end{pmatrix}.$$

definición 13.4. Si $M = D^n/\phi(D^m)$, diremos que M es el módulo definido por la matriz Φ correspondiente a ϕ. También diremos que la matriz Φ es la matriz de relaciones de M. Nótese que, matricialmente $\phi(v) = v\Phi$.

definición 13.5. Dos matrices de n filas y m columnas A y B se dicen equivalentes si existen elementos $P \in \mathbb{M}_n(D)^*$, y $Q \in \mathbb{M}_m(D)^*$, tales que $A = PBQ$.

Observación 13.6. Si P es invertible en $\mathbb{M}_n(D)$, la función $v \mapsto vP$ es un isomorfismo de D-módulos de D^n en si mismo, cuya inversa está dada por $v \mapsto vP^{-1}$.

Proposición 13.7. *Matrices equivalentes definen módulos isomorfos.*

Demostración Sea $\phi' : D^m \to D^n$ be the map $v \mapsto v\Phi'$ con $\phi' = P\Phi Q$. Observese que ya que P es invertible,

$$\phi(D^m.P) = (D^m.P)\Phi = D^m\Phi = \phi(D^m).$$

Luego, podemos suponer que P es la matriz identidad. Sea $N = \phi(D^m)$. Entonces multiplicación por Q define un isomorfismo

$$\tau : D^n/N \xrightarrow{\cong} (D^n.Q)/(N.Q) = D^n/N',$$

donde $N' = N.Q = (D^m)\Phi' = \phi'(D^m)$. □

Lema 13.8. *Sea $A = (a_{i,j})_{i,j}$ una matriz de n filas y m columnas con coeficientes en D. Sea* $\mathrm{mcd}(A)$ *el máximo común divisor de los $a_{i,j}$. Entonces, si $P \in \mathbb{M}_n(D)^*$ y $Q \in \mathbb{M}_m(D)^*$, entonces* $\mathrm{mcd}(A) = \mathrm{mcd}(PAQ)$.

Demostración Sea $I = (d)$ donde $d = \text{mcd}(A)$. Entonces $A \in \mathbb{M}_{n\times m}(I)$, el que es un $\Big(\mathbb{M}_n(D), \mathbb{M}_m(D)\Big)$-bimódulo. En particular $PAQ \in \mathbb{M}_{n\times m}(I)$, de donde $\text{mcd}(A)$ divide a $\text{mcd}(PAQ)$ y la conversa sigue de la identidad $A = P^{-1}(PAQ)Q^{-1}$ por simetría. □

Observación 13.9. Sea A una matriz con dos filas. Sea R la matriz

$$R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Entonces RA es la matriz que tiene las filas de A en el orden opuesto. No es dificil escribir matrices de dimensión arbitraria que tienen el mismo efecto de intercambiar dos filas dadas. De este modo, dos matrices que difieren solo en el orden de sus filas son equivalentes. Otro tanto se aplica a las columnas (multiplicando por la derecha). Del mismo modo, las matrices del tipo

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

nos permiten sumar un multiplo de una fila dada a una segunda fila. De modo tal que sumar un múltiplo de una fila (o columna) a otra fila (o columna) mantiene la equivalencia de matrices. En lo sucesivo, utilizaremos este hecho sin mayor explicación.

Observación 13.10. Recordemos que todo DIP es un anillo Noetheriano, en particular toda colección de ideales de D tiene un elemento maximal. Este hecho nos permitirá simplificar las demostraciones siguientes.

Lema 13.11. *Toda matriz de* 2 *por* 2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

es equivalente a una matriz de la forma

$$\begin{pmatrix} r & 0 \\ 0 & t \end{pmatrix}$$

donde r *es el máximo común divisor de* a*,* b*,* c*, y* d*.*

Demostración Por la observación anterior, si el lema no fuese cierto, podriamos escoger un contraejemplo

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

tal que el ideal (a) fuese maximal. Si a no divide a b, podemos tomar q y s tales que $r = ga + sb$ es el máximo común divisor de a y b y multiplicamos por la derecha por la matriz

$$\begin{pmatrix} g & -\frac{b}{r} \\ s & \frac{a}{r} \end{pmatrix},$$

cuyo determinante es 1_D y es por lo tanto invertible. Obtenemos así una matrix cuyo término superior izquierdo es (r), lo que contradice la maximalidad de (a). Se procede del mismo modo (intercambiando filas y columnas) si a no divide a c. Supondremos ahora que a divide a b y c. Restando un multiplo de la primera fila a la segunda, podemos suponer $c = 0$. Del mismo modo, suponemos $b = 0$. Sumando ahora la segunda fila a la primera, podemos suponer que la matriz tiene la forma

$$\begin{pmatrix} a & d \\ 0 & d \end{pmatrix}.$$

Repetimos ahora el procedimiento anterior para remplazar a por el máximo común divisor de a y d. □

Lema 13.12. *Toda matriz $A = (a_{i,j})_{i,j}$ de n por m es equivalente a una matriz de la forma*

$$\begin{pmatrix} r & O \\ O' & M \end{pmatrix}$$

donde r es el máximo común divisor de los $a_{i,j}$, O una fila de $m-1$ 0's, O' una columna de $n-1$ 0's, y M es una matriz de $n-1$ por $m-1$ (si $n-1$ o $m-1$ es 0, las matrices correspodientes se omiten).

Demostración Si el lema no fuese cierto, podriamos escoger un contraejemplo $A = (a_{i,j})_{i,j}$ tal que el ideal $(a_{1,1})$ fuese maximal. Es claro que $a_{1,1}$ no es igual a $\mathrm{mcd}(A)$, ya que en este caso tenemos la forma pedida restando múltiplos de la primera fila o columna. si algún $a_{i,j}$ no es divisible por $a_{1,1}$,

podemos suponer, intercambiando filas y columnas, que el par (i,j) está en el conjunto $\{(1,2),(2,1),(2,2)\}$. Multiplicando por matrices P y Q del tipo

$$P = \begin{pmatrix} P_0 & O \\ O' & I_{n-2} \end{pmatrix}, \qquad Q = \begin{pmatrix} Q_0 & O'' \\ O''' & I_{m-2} \end{pmatrix},$$

donde I_t es la identidad de t por t y $O, \ldots, O'''$ son bloques de 0's, podemos remplazar $a_{1,1}$ por el máximo común divisor de $a_{1,1}$, $a_{1,2}$, $a_{2,1}$, y $a_{2,2}$, como en el lema precedente. Esto contradice la elección de A. □

Lema 13.13. *Toda matriz $A = (a_{i,j})_{i,j}$ de n por m, es equivalente a una matriz de la forma*

$$\begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_m \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

o bien de la forma

$$\begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & d_n & 0 & \cdots & 0 \end{pmatrix},$$

donde d_1 es el máximo común divisor de los $a_{i,j}$, y cada d_i divide a d_{i+1}.

Demostración Usar inducción en el lema anterior. □

Proposición 13.14. *Todo D-módulo finitamente generado es isomorfo a un producto del tipo*

$$D^r \times \prod_{i=1}^{t} D/(d_i), \tag{13.1}$$

donde cada d_i divide a d_{i+1}.

Demostración Inmediato del primer caso del lema anterior. □

Observación 13.15. Si ϕ es inyectiva, como supusimos desde un comienzo, se tiene $m \leq n$, $t = m$, y $r = n - m$. Además, ningún d_i es 0, aunque si podrían ser uno, lo que dá factores triviales en la descomposición que pueden eliminarse. Sin embargo, podriamos partir con un conjunto cualquiera de relaciones entre los generadores, y obtener la forma dada por el lema 13.13. Si d_i es 0, el correspondiente factor es D y se agrega a D^r. Siempre puede escogerse la descomposición 13.1 de modo que ningún d_i sea 0 o 1. en este caso, el entero r se llama el rango de M y los elementos $d_1, \ldots, d_t$ se llaman los *factores invariantes* de M.

Corolario 13.15.1. *Todo grupo abeliano finitamente generado es isomorfo a un producto del tipo*

$$\mathbb{Z}^r \times \prod_{i=1}^{t} \mathbb{Z}/d_i\mathbb{Z},$$

donde cada d_i divide a d_{i+1} (con $d_1, \ldots, d_t \in \mathbb{Z}$).

Demostración Basta tomar $D = \mathbb{Z}$. □

definición 13.16. Un D-módulo M se dice de torsión si para todo $m \in M$ existe $d \in D$ tal que $dm = 0$.

Proposición 13.17. *Un D-módulo M finitamente generado es de torsión si y sólo si su rango es* 0.

Demostración Trivial. □

Supongamos en lo sucesivo que M es de torsión.

definición 13.18. Sean $p_1, \ldots, p_s$ los primos que dividen a d_t y sea $p_i^{e_{i,j}}$ la mayor potencia de p_i que divide a d_j, de modo que la descomposición en factores primos de d_j sea $d_j = up_1^{e_{1,j}} p_2^{e_{2,j}} \ldots p_s^{e_{s,j}}$. Entonces, los $s \times t$ elementos $p_i^{e_{i,j}}$, se llaman los divisores elementales de M. Nótese que como cada d_j divide a d_{j+1} se tiene $e_{i,1} \leq e_{i,2} \leq \ldots \leq e_{i,t}$.

El siguente resultado es una consecuencia inmediata del teorema chino de los restos:

Proposición 13.19. *Sea M un D-módulo finitamente generado de torsión. Sean $p_i^{e_{i,j}}$ los factores invariantes de M, entonces*

$$M \cong \prod_{i=1}^{t} \prod_{j=1}^{s} D/(p_i^{e_{i,j}}). \quad \square$$

Daremos ahora algunas aplicaciones del Teorema de descomposición primaria a formas canónicas de matrices. Para ello sea V un K-espacio vectorial de dimensión n y sea $T : V \to V$ una función lineal de modo que $f(x).v = f(T)(v)$ defina en V una estructura de $K[x]$-módulo como en el ejemplo 12.7. Denotaremos este módulo por M_T. Si $\{e_1, \ldots, e_n\}$ es una base de V, cada e_i satisface la relación $x.e_i = T(e_i)$. Si $B = (b_{i,j})_{i,j}$ es la matriz de T en la base $\{e_1, \ldots, e_n\}$, es decir $T(e_i) = \sum_{j=1}^{n} b_{i,j}e_j$ entonces $x.e_i - \sum_{j=1}^{n} b_{i,j}e_j = 0$ de donde M_T tiene como matriz de relaciones a $(xI - B)^t$ donde I es la matriz identidad. Por esta razón, los factores invariantes y los divisores elementales de una matriz B se calculan realizando operaciones por filas y columnas en la matriz $xI - B$. Estos no son sinó los factores invariantes de M_T donde T es una función lineal de matriz B. En lo que sigue denotaremos también este módulo por M_B. Se sigue que si $d_1(x), \ldots, d_r(x)$ son los factores invariantes de la matriz B entonces

$$M_B \cong K[x]/(d_1) \times \ldots \times K[x]/(d_r),$$

donde no hay ningún factor del tipo $K[x]$ ya que este tendría dimensión infinita sobre K. Además existen matrices invertibles P y Q con coeficientes en $K[x]$ tales que $P(xI - B)Q = \begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix}$ donde D es la matriz diagonal

$$\begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_m \end{pmatrix}.$$

La identidad en la esquina superior izquierda corresponde a los factores triviales $K[x]/(1)$ que se eliminan de la descomposición. En particular, el polinomio $C_B(x) = \det(xI - B)$, llamado también el polinomio característico de B satisface $C_B(x) = d_1(x)d_2(x)\ldots d_r(x)$. Como $C_B(x)$ es divisible por cada

d_i se tiene que $C_B(x)$ anula cada elemento de M_B, es decir $C_B(B) = 0$ como matriz. El polinomio mónico de menor grado que anula cada elemento de M_B es d_r el cual recibe el nombre de polinomio minimal de B y se denota también $m_B(x)$. Todo polinomio que satisface $f(B) = 0$ debe ser divisible por $m_B(x)$. Dado que cada d_i divide a d_{i+1} se obtiene también que los polinomios $C_B(x)$ y $m_B(x)$ tienen exactamente los mismos divisores primos.

Otra consecuencia de lo anterior es que para encontrar formas canónicas de matrices, es suficiente encontrarla para la acción de x en el módulo $K[x]/(f)$ donde $f(x)$ es un polinomio. Si $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, en el módulo $K[x]/(f)$ podemos tomar la base $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$. En esta base la múltiplicación por x tiene matriz $\begin{pmatrix} 0 & -a_0 \\ I & c \end{pmatrix}$ donde c es la columna

$$\begin{pmatrix} -a_1 \\ -a_2 \\ \vdots \\ -a_{n-1} \end{pmatrix}.$$

Esta matriz recibe el nombre de matriz compañera del polinomio f. Se concluye que toda matriz B puede llevarse a la forma

$$\begin{pmatrix} \Delta_1 & 0 & \cdots & 0 & 0 \\ 0 & \Delta_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \Delta_{r-1} & 0 \\ 0 & 0 & \cdots & 0 & \Delta_r \end{pmatrix}, \tag{13.2}$$

donde δ_i es la matriz compañera del polinomio $d_i(x)$. Esta se llama la forma canónica racional de la matriz B.

definición 13.20. Sea k un cuerpo, y sean $A, B \in \mathbb{M}_n(k)$. Se dice que A y B son conjugadas si existe $P \in \mathbb{M}_n(k)^*$ tal que $A = PBP^{-1}$. Dos matrices son conjugadas si y sólo si representan a la misma función lineal en (posiblemente) diferentes bases.

Se concluye que cada matriz es conjugada a una matriz de la forma (13.2). Descomponiendo cada $d_i(x)$ en sus divisores elementales $p_i(x)^{e_{i,j}}$, se obtiene

$$M_B \cong \prod_{i=1}^{t} \prod_{j=1}^{s} K[x]/(p_i(x)^{e_{i,j}}),$$

de donde se obtiene una forma canónica similar para estos polinomios. Otra forma canónica que utiliza la descomposición en divisores elementales es la *forma de Jordan*.

definición 13.21. Una *matriz de Jordan* es una matriz del tipo

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}.$$

Proposición 13.22. *Sea k un cuerpo algebraicamente cerrado. Toda matriz $B \in \mathbb{M}_n(k)$ es conjugada a una matriz del tipo*

$$\begin{pmatrix} \Lambda_1 & 0 & \cdots & 0 & 0 \\ 0 & \Lambda_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \Lambda_{K-1} & 0 \\ 0 & 0 & \cdots & 0 & \Lambda_K \end{pmatrix},$$

donde $\Lambda_1, \ldots, \Lambda_K$ son matrices de Jordan. Esta se denomina la forma de Jordan de B.

Demostración Basta con comprobar que la multiplicación por x en un módulo de la forma

$$M \cong K[x]/(p^\alpha)$$

donde $p(x)$ es un polinomio primo tiene como matriz a una matriz de Jordan en alguna base. Los únicos polinomios primos sobre un cuerpo algebraicamente cerrado son de la forma $x - \lambda$. Por lo tanto,

$$M \cong K[x]/(x - \lambda)^\alpha.$$

Si v es un generador de este módulo, entonces

$$v, (A - \lambda)v, \ldots, (A - \lambda)^{\alpha-1}v,$$

forman una base de M en la que A toma la forma requerida. □

Nótese que aunque la existencia de la forma de Jordan está garantizada para cualquier matriz sólo para un cuerpo algebraicamente cerrado, aún existe sobre cualquier cuerpo para matrices que tengan divisores elementales de la forma $(x-\lambda)^t$. Los elementos diagonales λ que aparecen en la forma de Jordan de B reciben el nombre de valores propios de B y son las raices de $\det(xI-B)=0$ en particular, la forma de Jordan existe para matrices con coeficientes en un cuerpo k arbitrario, a condición de que la matriz tenga a todos sus valores propios en el cuerpo k.

Ejercicios

1. Encuentre un conjunto libre de generadores para los siguientes subconjuntos de $\mathbb{Z}^3$:
   (a) $\{(x,y,z)\in\mathbb{Z}^3 | x+y+z$ es divisible por $3\}$.
   (b) El subgrupo generado por $(1,0,1)$, $(1,1,0)$, y $(0,1,1)$.
   (c) La intersección de los dos subgrupos anteriores.
   (d) La suma de dichos subgrupos.

2. Exprese cada uno de los siguientes grupos abelianos como un producto de grupos cíclicos:
   (a) $A=\langle x,y,z|23x+7y+9z=8x+12y+6z=x+33y+22z=0\rangle_{\text{ab}}$.
   (b) $A=\langle x,y|x=y\rangle_{\text{ab}}$.
   (c) $A=\langle x,y,z|3x=y,5z=y,9x+2y=0,11z+4x=0\rangle_{\text{ab}}$.

3. Probar que para todo entero n libre de cuadrados (es decir, no divisible por ningún cuadrado perfecto salvo 1), existe un único grupo abeliano con n elementos salvo isomorfismos.

4. Exprese el grupo abeliano $(\mathbb{Z}/16\mathbb{Z})^*$ como producto de grupos cíclicos.

5. Un grupo abeliano T se dice de torsión si y sólo si cada elemento tiene órden finito. Probar que para cada grupo abeliano de torsión se tiene
$$T=\bigoplus_p T_p,$$
donde para cada primo p, se define $T_p=\{t\in T|p^r t=0$ para algún $t\geq 0\}$.

6. Sea M el $\mathbb{Z}[i]$-módulo con matriz de relaciones $\begin{pmatrix} 1+i & 2 \\ 4 & 5+5i \end{pmatrix}$. Escriba M como un producto de módulos cíclicos.

7. Encuentre los factores invariantes y los divisores elementales de cada una de las matrices siguientes:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 56 & 105 \\ 0 & 2 & 22\sqrt{\pi} \\ 0 & 0 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -3 \\ 0 & 1 & -3 \end{pmatrix},$$

$$D = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 1\sqrt{\pi} \\ 0 & 0 & 2 \end{pmatrix}, \quad E = \begin{pmatrix} 4 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{pmatrix}, \quad E = \begin{pmatrix} 4 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

8. Busque un ejemplo de dos matrices que tengan el mismo polinomio minimal y el mismo polinomio característico, pero que no sean conjugadas.

9. Probar que dos matrices complejas de tres por tres con el mismo polinomio minimal y el mismo polinomio característico son conjugadas (puede asumir el teorema fundamental del álgebra si lo necesita).

10. Utilice la forma de Jordan para probar que cada matriz satisface su polinomio característico.

11. Demuestre o dé un contraejemplo de la siguiente afirmación:*Dos matrices con coeficientes reales que son conjugadas sobre* $\mathbb{C}$ *son también conjugadas sobre* $\mathbb{R}$.

12. Sea p un número primo y sea A la matriz de p por p con coeficientes en $\mathbb{F}_p$ que actúa en la base canónica mediante $Ae_i = e_{i+1}$ para $1 \leq i \leq n-1$ y $Ae_n = e_1$. Encuentre la matriz de Jordan B conjugada sobre $\overline{\mathbb{F}_p}$ a A. Comprobar que B tiene coeficientes en $\mathbb{F}_p$. Son A y B conjugadas sobre $\mathbb{F}_p$? Justifique.

Chapter 14

Anillos Noetherianos y Artinianos

definición 14.1. Una sucesión $I_1 \subseteq I_2 \subseteq I_2 \subseteq \ldots$ se *estabiliza* si para algún entero positivo N, $I_n = I_N$ para todo $n \leq N$. Un anillo C es *Noetheriano* si toda sucesión creciente de ideales de C se estabiliza. Tambien se dice que C satisface la condición de cadenas ascendentes (CCA).

La caracterización siguiente es muy útil:

Proposición 14.2. *Un anillo es Noetheriano si y sólo si cada ideal es finitamente generado.*

Demostración Si el ideal I no es finitamente generado, tomamos $I_1 = (0)$, y para todo $n \leq 2$, sea $I_n = I_{n-1} + (a_n)$ donde $a_n \in I - I_{n-1}$. Tal a_n existe por ser I_{n-1} finitamente generado. Entonces la sucesión $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ no se estabiliza.

Supongamos ahora que todo ideal es finitamente generado y sea $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ una sucesión creciente de ideales, entonces su union es un ideal I, y algún I_N contiene a todos los generadores. □

Corolario 14.2.1. *Todo DIP es Noetheriano.*

Demostración Todo ideal principal es finitamente generado. □

Proposición 14.3. *Sea J un ideal de D. Si D es un Noetheriano entonces D/J es Noetheriano.*

Demostración Por el teorema de la correspondencia, existe una biyección que preserva el orden entre los ideales de D/J y un subconjunto de los ideales de D. □

Proposición 14.4. *Sea S un subjunto mulptiplicativo de D. Si D es un Noetheriano entonces $S^{-1}D$ es Noetheriano.*

Demostración Similar a la anterior usando el Lema 18.10. □

Una de las principales propiedades de la CCA es que se preserva al tomar anillos de polinomios. Antes de probar este resultado necesitamos estudiar la teoría de módulos.

Módulos Noetherianos

En esta sección A es un anillo conmutativo.

definición 14.5. Una sucesión $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$ de A-módulos se estabiliza si para algún entero positivo N, se tiene $M_n = M_N$ para todo $n \leq N$. Un módulo M es Noetheriano si toda sucesión creciente de submódulos de M se estabiliza. Tambien se dice que M satisface la condición de cadenas ascendentes (CCA).

La demostración del resultado siguiente es identica al caso de anillos y se deja al lector.

Proposición 14.6. *Un módulo es Noetheriano si y sólo si cada submódulo es finitamente generado.* □

El siguiente resultado es inmediato de la definición:

Proposición 14.7. *Un submódulo de un módulo Noetheriano es Noetheriano.* □

El siguiente resultado es inmediato del Teorema de la correspondencia para módulos:

Proposición 14.8. *Un cociente de un módulo Noetheriano es Noetheriano.* □

El siguiente resultado será muy util en la demostración del teorema de la base de Hilbert en la sección siguiente:

Proposición 14.9. *Un módulo finitamente generado sobre un anillo Noetheriano es Noetheriano.*

Demostración Sea A un anillo Noetheriano. Como todo A-módulo finitamente generado es isomorfo a un cociente de A^n para algún n, podemos suponer $M = A^n$.

Si $n = 1$, la afirmación de que M es Noetheriano es equivalente a la afirmación de que A es Noetheriano como anillo. Supongamos demostrado que A^k es Noetheriano. Para $v \in A^{k+1}$, escribimos $v = (v[1], \ldots, v[k+1])$. Sea N un submódulo de A^{k+1}, y sea $J = \{v[k+1] | v \in N\}$. Observese que $(\alpha v + \beta w)[k+1] = \alpha v[k+1] + \beta w[k+1]$, así que J es un ideal. Se sigue que está generado por elementos $v_1[k+1], \ldots, v_r[k+1]$. Sea $\tilde{N}$ el submódulo generado por $v_1, \ldots, v_r$, y sea $N' = \{v \in N | v[k+1] = 0\}$. Afirmamos que $N = \tilde{N} + N'$. Como N' está contenido en $A^k \times 0$ que es isomorfo a A^k, el resultado sigue.

Para probar la afirmación, observamos que si v esta en N existen elementos $a_1, \ldots, a_r$ en A tales que $v[k+1] = \sum_i a_i v_i[k+1]$. de donde $v - \sum a_i v_i \in N'$. □

El Teorema de la Base de Hilbert

Proposición 14.10. *Si A es un anillo Noetheriano entonces también lo es el anillo de polinomios $A[X]$.*

Demostración Sea A un anillo Noetheriano y sea $I \subseteq A[X]$ un ideal. Para cualquier $f \in I$ no nulo, escribimos $f(X) = \sum_{i=0}^{n(f)} a_i(f) X^i$, donde $n(f)$ es el grado de f. En particular, $a_{n(f)}(f) \neq 0$. Sea $b(f) = a_{n(f)}(f)$. Afirmamos que el conjunto $J = \{b(f) | f \in I\} \cup \{0\}$ es un ideal de A. Es claro que para cualquier $a \in A$ y cualquier $f \in I$, tenemos $b(af) = ab(f)$. Ademas, si $b(f) + b(g) \neq 0$, entonces $b(f) + b(g) = b(X^{(N-n(f))} f + X^{(N-n(g))} g)$, para $N = \max\{n(f), n(g)\}$. Esto prueba la afirmación.

Sean $g'_1, \ldots, g'_M \in I$ tales que $b(g'_1), \ldots, b(g'_M)$ generen el ideal J. Sea $N = \max\{n(g'_1), \ldots, n(g'_M)\}$, y sea $g_i = X^{N-n(g'_i)} g'_i$. Sea I_N el conjunto de polinomios en I de grado menor que N. Afirmamos que $I = I_N + \sum_i A[X] g_i$. Como el conjunto de polinomios de grado menor o igual que N es un A-módulo finitamente generado como, y por lo tanto Noetheriano (ya que A es un anillo Noetheriano), el submódulo I_N es finitamente generado.

Ahora probamos la afirmación. Sea $f \in I$. Si f tiene grado menor a N, no hay nada que demostrar. De otro modo, $n(f) > N = n(g_i)$ para todo i. Además, dado que $b(g_i) = b(g'_i)$, entonces $b(g_1), \ldots, b(g_M)$ generan J y por lo tanto $b(f) = \sum_i a_i b(g_i)$ para ciertos elementos a_i. Se concluye que

$f - X^{n(f)-N}\sum_i a_i g_i$ tiene grado menor que f y la demostración concluye por inducción. □

Proposición 14.11. *Si A es un anillo Noetheriano entonces también lo es el anillo de series de potencia $A[[X]]$.*

Demostración Sea A un anillo Noetheriano y sea $I \subseteq A[[X]]$ un ideal. Para cualquier $f \in I$ no nulo, escribimos $f(X) = \sum_{n(f)}^{\infty} a_i(f)X^i$ con $a_{n(f)}(f) \neq 0$. Sea $b(f) = a_{n(f)}(f)$. Afirmamos que el conjunto $J = \{b(f)|f \in I\} \cup \{0\}$ es un ideal de A. La demostración de este hecho es identica a la que aparece en la proposición anterior y se deja al lector.

Sean $g'_1, \ldots, g'_M \in I$ tales que $b(g'_1), \ldots, b(g'_M)$ generen el ideal J. Sea $N = \max\{n(g'_1), \ldots, n(g'_M)\}$, y sea $g_i = X^{N-n(g'_i)}g'_i$. Sea $I(N)$ un A-submódulo finitamente generado de I tal que $I(N) + (X^N) = I + (X^N)$. Tal $I(N)$ siempre existe ya que $A[[X]]/(X^N)$ es finitamente generado como A-módulo. Afirmamos que $I = I(N) + \sum_i A[X]g_i$. Esto concluirá la demostración. Sea $f \in I$. Sea $g \in I(N)$ tal que $f - g \in (X^N)$. Escribimos

$$b(g - f) = \sum_j a_{1,j} b(g_j),$$

y definimos el polinomio h_1 por

$$h_1 = \sum_j a_{1,j} X^{n(g-f)-n(g_j)} g_j.$$

Sea $f_1 = f - g - h_1$, entonces $n(f_1) > n(f - g)$. Iterando, para cada $i > 1$ definimos inductivamente una combinación h_{i+1} de los vectores g_j's de la forma

$$h_{i+1} = \sum_{j=1}^{M} a_{i+1,j} X^{n(f_i)-n(g_j)} g_j,$$

y tal que $f_{i+1} = f_i - h_{i+1}$ satisface $n(f_{i+1}) > n(f_i)$. se sigue que f_i converge a 0 y por lo tanto

$$f = g + \sum_{i=1}^{\infty} h_i = g + \sum_{j=1}^{M} \left(\sum_{i=1}^{\infty} a_{i,j} X^{n(f_{i-1})-n(g_j)} \right) g_j,$$

donde $f_0 = f - g$. Como cada suma en paréntesis converge, esto termina la demostración. □

Anillos Artinianos

El concepto opuesto de anillo Noetheriano es el de anillo artiniano:

definición 14.12. Un anillo C es *artiniano* si toda sucesión decreciente de ideales de C se estabiliza. Tambien se dice que C satisface la condición de cadenas descendentes (CCD).

Ejemplo 14.13. Todo anillo finito es Artiniano. También lo es toda algebra de dimensión finita sobre un cuerpo.

Los resultados siguientes son análogos a los correspondientes resultados para anillos Noetherianos:

Proposición 14.14. *Sea J un ideal de D. Si D es un Noetheriano entonces D/J es Noetheriano.* □

Proposición 14.15. *Sea S un subjunto mulptiplicativo de D. Si D es un Noetheriano entonces $S^{-1}D$ es Noetheriano.* □

Proposición 14.16. *Todo dominio de integridad artiniano es un cuerpo.*

Demostración Si $a \neq 0$ en D, la sucesión $(a) \supseteq (a^2) \supseteq \ldots$ es decreciente, luego para algún n, se tiene que $(a^n) = (a^{n+1})$. En particular, existe t tal que $a^n = ta^{n+1}$, pero entonces $ta = 1$. □

Corolario 14.16.1. *En un anillo Artiniano todo ideal primo es maximal.* □

Proposición 14.17. *En un anillo Artiniano hay una cantidad finita de ideales maximales.*

Demostración Sea $\wp_1, \wp_2, \wp_3, \ldots$ una sucesión de ideales maximales distintos. Se define una cadena descendente

$$\wp_1 \supseteq \wp_1 \cap \wp_2 \supseteq \wp_1 \cap \wp_2 \cap \wp_3 \supseteq \ldots.$$

Por definición de anillo Artiniano, esta sucesión se estabiliza. En particular existe $n+1$ tal que $\wp_{n+1} \supseteq \wp_1 \cap \ldots \cap \wp_n$. Por otro lado, como cada $\wp_i$ es comaximal con $\wp_{n+1}$, se tiene que $\wp_{n+1}$ y $\wp_1 \cap \ldots \cap \wp_n$ son comaximales. □

Proposición 14.18. *Un anillo Artiniano A sin elementos nilpotentes no triviales es un producto de cuerpos.*

Demostración Sean $\wp_1, \wp_2, \ldots, \wp_n$ los ideales maximales distintos de A. Por el Teorema Chino de los Restos, se tiene que

$$A/\wp_1 \cap \ldots \cap \wp_n \cong \prod_i A/\wp_i.$$

Como $\wp_1, \wp_2, \ldots, \wp_n$ son los ideales primos distintos de A, $\wp_1 \cap \ldots \cap \wp_n = \mathfrak{N}(A) = \{0\}$. □

Corolario 14.18.1. *Un anillo finito es producto de cuerpos si y sólo si no tiene elementos nilpotentes.*

Corolario 14.18.2. *Un álgebra conmutativa y de dimensión finita sobre un cuerpos es producto de cuerpos si y sólo si no tiene elementos nilpotentes.*

Ejercicios

1. Probar que un anillo conmutativo C es Noetheriano si y sólo si cada cada C-módulo finitamente generado es Noetheriano.

2. Sea M un C-módulo y sea N un submódulo. Probar que las siguientes afirmaciones son equivalentes:

   (a) M es Noetheriano.

   (b) N y M/N son ambos Noetherianos.

3. Utilice el resultado precedente para dar una segunda demostración de la Proposición 18.9.

4. Probar que todo anillo de polinomios de la forma $K[X_1, \ldots, X_n]$, donde K es un cuerpo, es Noetheriano.

5. Probar que todo anillo de la forma $K[a_1, \ldots, a_n]$, donde $K \subseteq L$ son cuerpos, mientras $a_1, \ldots, a_n \in L$ son elementos arbitrarios, es Noetheriano.

6. Probar que el anillo de todos los números complejos que son raiz de un polinomio mónico con coeficientes enteros no es Noetheriano.

7. Probar que el anillo de todas las funciones continuas del intervalo $[0, 1]$ a $\mathbb{R}$ no es Noetheriano.

8. Sea D un dominio noetheriano en el que para cada par de elementos (a, b) existe un elemento d que satisface $(a, b) = (d)$. Probar que D es un DIP.

9. Probar, mediante un ejemplo, que la condición de que D sea Noetheriano en el problema precedente es necesaria (Sugerencia: considere polinomios en $X^{1/n}$ para n arbitrariamente grande).

Chapter 15

Anillos completos y series de potencias

El anillo de series de potencia posee una propiedad universal similar a la del anillo de polinomios que vimos en el capítulo anterior, pero antes de enunciarla con el suficiente grado de generalidad es necesario definir el concepto de anillo completo.

Sea A un anillo, y sea I un ideal bilátero de A. Sea

$$I^\infty = \bigcap_{i=1}^{\infty} I^i.$$

En lo que sigue asumiremos que $I^\infty = \{0\}$. Ejemplo de ideal que no satisface esta condición es PA donde P es un idempotente central.

definición 15.1. Una sucesión $\{a_n\}_{n=1}^\infty$ se dice converger a un límite a (en simbolos $a_n \xrightarrow{I} a$) si para todo M positivo, existe $N = N(M)$ tal que, para $n > N$, $a - a_n \in I^M$.

definición 15.2. Una sucesión $\{a_n\}_{n=1}^\infty$ se dice de cauchy (respecto de I) si para todo M positivo, existe $N = N(M)$ tal que, para $n, m > N$, se tiene que $a_m - a_n \in I^M$.

definición 15.3. Un anillo A se dice completo respecto de un ideal bilátero I, si toda sucesion de Cauchy respecto de I converge.

Con estas definiciones, es posible introducir una métrica en el anillo A que define la convergencia con respecto al ideal J, pero no lo haremos aquí.

También es posible definir, para todo anillo A y todo ideal bilátero J que satisface $J^\infty = 0$, el *completado* de A con respecto al ideal J. Este es un anillo $\tilde{A}$ que contiene a A, y con un ideal $\tilde{J}$, tal que $A \cap \tilde{J} = J$ y $\tilde{A}$ es completo con respecto a $\tilde{J}$. Por ejemplo, el anillo de enteros p-ádicos $\mathbb{Z}_p$ se define como el completado de $\mathbb{Z}$ respecto de $p\mathbb{Z}$.

El anillo $C[[x]]$ es completo con respecto al ideal (x). De hecho, $C[[x]]$ es el completado del anillo de polinomios $C[x]$ con respecto al ideal (x). La serie de potencias $f(x)$ es invertible si y sólo si a_0 es invertible, y su inverso $g(x) = f(x)^{-1}$ se obtiene resolviendo las ecuaciones sucesivas:

$$\begin{aligned} a_0b_0 &= 1 \\ a_1b_0 + a_0b_1 &= 0 \\ a_2b_0 + a_1b_1 + a_0b_2 &= 0 \\ a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 &= 0 \\ \vdots \quad \vdots &\quad \vdots, \end{aligned}$$

en las incógnitas $b_0, b_1, \ldots$.

Si B es una $\mathbb{Q}$-álgebra, ejemplos de series de potencia con coeficientes en B son las conocidas expresiones (donde $\lambda \in B$):

$$\begin{aligned} (1+x)^\lambda &= 1 + \lambda x + \tbinom{\lambda}{2}x^2 + \tbinom{\lambda}{3}x^3 + \ldots \\ \cos(x) &= 1 - \tfrac{x^2}{2!} + \tfrac{x^4}{4!} - \tfrac{x^6}{6!} + \ldots \\ \operatorname{sen}(x) &= x - \tfrac{x^3}{3!} + \tfrac{x^5}{5!} - \tfrac{x^7}{7!} + \ldots \\ e^x &= 1 + x + \tfrac{x^2}{2!} + \tfrac{x^3}{3!} + \tfrac{x^4}{4!} + \ldots \\ \ln(1+x) &= x - \tfrac{x^2}{2} + \tfrac{x^3}{3} - \tfrac{x^4}{4} + \ldots \\ \operatorname{Arctan}(x) &= x - \tfrac{x^3}{3} + \tfrac{x^5}{5} - \tfrac{x^7}{7} + \ldots \end{aligned}$$

En particular, $\cos(x)$ es invertible y puede definirse la serie de potencias $\tan(x) = \operatorname{sen}(x)/\cos(x)$.

La serie de potencias $(1+x)^n$ definida para valores enteros de n, es un elemento de $\mathbb{Z}[[x]]$, ya que $\binom{n}{k}$ es siempre un entero.

La propiedad universal del algebra de series de potencias es la siguiente:

Proposición 15.4. *Sea (B, ϕ) es un C-algebra, y sea J un ideal bilátero de B. Supongamos además que $J^\infty = \{0\}$ y que B es completo respecto de J. Entonces, dado cualquier $u \in J$, existe un homomorfismo de anillos $\phi : C[[x]] \to B$ que lleva a x en u. La imagen de la serie $f(x)$ se denota $f(u)$. Mas generalmente, si los elementos $u_1, \ldots, u_n \in J$ conmutan, entonces existe un homomorfismo de anillos $\phi : C[[x_1, \ldots, x_n]] \to B$ que lleva a x_i en u_i.*

definición 15.5. La imagen de la serie $f(x_1, \ldots, x_n)$ se denota $f(u_1, \ldots, u_n)$. En particular, Si $u(x) \in (x)$ y $f(x) \in K[[x]]$ entonces $f(u(x))$ es una serie de potencias que se denomina la composición de f y u.

Ejemplo 15.6. Si $f(x) = 1+x+x^2+\ldots$, y si $u(x) = x^3$, entonces $f(u(x)) = 1 + x^3 + x^6 + \ldots$.

Expresiones como $e^{\text{sen}x}$ y $\cos(e^x - 1)$ tienen sentido en este contexto. Nótese, sin embargo, que $e^{\cos x}$ no está definida como elemento de $\mathbb{Q}[[x]]$, ya que $\cos x$ no está en el ideal (x). Esto se traduce en el hecho de que la expansión de Taylor de la función real $g(x) = e^{\cos x}$ podría no tener coeficientes racionales (como de hecho ocurre).

Cálculos mediante congruencias

Si A es un anillo e I un ideal bilátero, se dice que a, b son congruentes módulo I si $a - b \in I$. En simbolos, se escribe

$$a \equiv b \pmod{I}.$$

Si $I = (t)$ se escribe

$$a \equiv b \pmod{t}.$$

Observemos que si $u \in I$, entonces $u^n \in I^n$. Esta observación permite calcular composiciones de expansiones en serie de potencias módulo cualquier potencia I^n predeterminada, como se observa en el siguiente ejemplo:

Ejemplo 15.7.

$$\begin{aligned} e^{\text{sen}x} &\equiv 1 + (\text{sen}x) + \tfrac{1}{2}(\text{sen}x)^2 + \tfrac{1}{6}(\text{sen}x)^3 \pmod{x^4} \\ &\equiv 1 + (x - \tfrac{1}{6}x^3) + \tfrac{1}{2}(x - \tfrac{1}{6}x^3)^2 + \tfrac{1}{6}(x - \tfrac{1}{6}x^3)^3 \pmod{x^4} \\ &\equiv 1 + x + \tfrac{1}{2}x^2 \pmod{x^4}. \end{aligned}$$

Identidades entre series de potencias

Sea A un anillo conmutativo, completo con respecto al ideal I (con $I^\infty = \{0\}$). Sean $u_1, \ldots, u_n \in I$. Entonces, existe un único homomorfismo continuo de anillos

$$\Phi : \mathbb{Z}[[x_1, \ldots, x_n]] \longrightarrow A,$$

tal que $\Phi(x_i) = u_i$. En particular, cualquier identidad que sea cierta en $\mathbb{Z}[[x_1, \ldots, x_n]]$ lo será también en un anillo conmutativo arbitrario. En general, no lo será en anillos no conmutativos, pero si los elementos en cuestión conmutan, uno puede restringirse al subanillo mas pequeño que contiene a estos elementos y trabajar allí (en un capitulo posterior desarrollaremos esta idea de *anillo generado* en mas detalle).

Por ejemplo, sea $m \in \mathbb{Z}$ y consideremos las series de potencias

$$(1 + x_1)^m = \sum_{i=0}^{\infty} \binom{m}{i} x^i.$$

Estas series corresponden a funciones analíticas de variable real. Una función analítica determina completamente su serie de potencias. Esto significa que la conocida identidad

$$(1 + x_1)^{m_1}(1 + x_1)^{m_2} = (1 + x_1)^{m_1+m_2},$$

entre las correspondientes funciones analíticas, es una identidad en el anillo $\mathbb{Z}[[x_1, \ldots, x_n]]$. Ella es, por lo tanto, válida sobre cualquier anillo completo. En particular, si $u \in I$ entonces $(1 + u)^m$ es invertible para todo $m \in \mathbb{Z}$.

Nuevas identidades de este tipo se obtienen considerando el anillo de series de potencias con coeficientes racionales $\mathbb{Q}[[X_1, \ldots, X_n]]$. Si A es un anillo conmutativo, completo respecto de I (con $I^\infty = \{0\}$), que es a la vez una $\mathbb{Q}$-álgebra, y si $u_1, \ldots, u_n \in I$, entonces existe un único homomorfismo continuo de anillos

$$\Psi : \mathbb{Q}[X_1, \ldots, X_n]] \longrightarrow A$$

tal que $\Psi(X_i) = u_i$. Esto significa que todas las identidades usuales entre series de potencia con coeficientes racionales son válidas también sobre cualquier anillo A con las propiedades mencionadas. Ellas son, en particular, válidas en el anillo de series de potencia sobre cualquier cuerpo de característica 0.

Como ejemplos de estas identidades, podemos citar.

$$\begin{aligned} e^{X_1}e^{X_2} &= e^{X_1+X_2}, \\ \operatorname{sen}(X_1+X_2) &= \operatorname{sen}(X_1)\cos(X_2)+\cos(X_1)\operatorname{sen}(X_2), \\ \ln(1+[e^{X_1}-1]) &= X_1, \\ \operatorname{Arctan}(\tan(X_1)) &= X_1. \end{aligned}$$

Ideales nilpotentes Sea A un anillo e I un ideal bilátero. Si $I^n = 0$ para algún entero n, se dice que I es nilpotente. Entonces A es completo respecto del anillo I. En particular, todo anillo es completo respecto del ideal 0, aunque este ejemplo no es muy interesante.

Si A es un anillo conmutativo y $u \in A$ es nilpotente, entonces $1-u$ es invertible y su inverso puede calcularse mediante $(1-u)^{-1} = 1+u+u^2+\ldots$.

Otra aplicación, es el siguiente resultado:

Proposición 15.8. *Si A es un $\mathbb{Q}$-álgebra conmutativo e I es nilpotente, entonces el grupo abeliano multiplicativo $1+I$ es isomorfo al grupo aditivo I.*

Demostración. El isomorfismo entre ambos grupos está dado por las funciones exponencial y logarítmica. □

Ejercicios

1. Probar que si J es un ideal de C entonces $J[[x]]$ (series de potencias con coeficientes en J) es un ideal de $C[[x]]$ y que $C/J[[x]]$ es isomorfo a $C[[x]]/J[[x]]$. Probar el resultado correspondiente para anillos de polinomios.

2. Sea C un anillo conmutativo. Probar que $\mathfrak{R}(C[[x]]) = (x) + \mathfrak{R}(C)$ y que $\mathfrak{N}(C[[x]]) \subseteq \mathfrak{N}(C)[[x]]$. Probar que si existe n tal que $\mathfrak{N}(C)^n = 0$, entonces $\mathfrak{N}(C[[x]]) = \mathfrak{N}(C)[[x]]$ (este ejercicio prueba que, en general, el radical de Jacobson y el nilradical no coinciden).

3. Probar que Si C es un dominio de integridad, entonces $C[[x]]$ es un dominio de integridad.

4. Sea K un cuerpo. Calcule el radical de Jacobson y el nilradical de los siguientes anillos: $\mathbb{Z}$, K, $\mathbb{Z}[X]$, $K[X]$, $\mathbb{Z}[[X]]$, $K[[X]]$, $\mathbb{Z}/108\mathbb{Z}$, $\mathbb{Z}/108\mathbb{Z}[[X]]$, $K[X]/(X^3 - X^2)$, $K[[X,Y]]/(X^3 - X^2)$.

5. Probar que $(C \times C')[[x]] \cong (C[[x]]) \times (C'[[x]])$. Probar el resultado correspondiente para anillos de polinomios.

6. a)Sea (B, ϕ) una C-algebra conmutativa. Suponga que J es un ideal de B tal que $J^\infty = (0)$ y B es completo respecto de J. Demostrar que si $u \in J$ y $a \in B$, entonces existe una única función $\tilde{\phi} : C[X][[Y]] \to B$. Tal que $\tilde{\phi}|_C = \phi$, $\tilde{\phi}(X) = a$, y $\tilde{\phi}(Y) = u$.

   b) Generalice a $C[X_1, \ldots, X_n][[Y_1, \ldots, Y_m]]$.

7. a) Sea $(1+x)^y \in \mathbb{Q}[y][[x]]$ la serie de potencias definida por

$$(1+x)^y = \sum_{n=0}^{\infty} \binom{y}{n} x^n.$$

   (Nótese que $\binom{y}{n} \in \mathbb{Q}[y]$). Entonces en el anillo de series de potencia $\mathbb{Q}[y,z][[x]]$ se satisface

$$(1+x)^y(1+x)^z = (1+x)^{y+z}.$$

   b) Concluir que si (B, ϕ) una $\mathbb{Q}$-algebra conmutativa, entonces para todo $\alpha, \beta \in B$, las series de potencia en $B[[x]]$,

$$(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n \text{ y } (1+x)^\beta = \sum_{n=0}^{\infty} \binom{\beta}{n} x^n$$

   satisfacen

$$(1+x)^\alpha(1+x)^\beta = (1+x)^{\alpha+\beta}.$$

   (Sugerencia: Usar problema anterior).

8. Sea R un anillo unitario arbitrario, $a, B \in R$. Probar que si $1 + AB$ es invertible entonces $1 + BA$ es invertible (sugerencia, Suponer primero que R es completo con respecto al ideal I y que $A \in I$, de modo que $(1 + AB)$ tiene un desarrollo en serie, luego despejar $(1 + BA)^{-1}$ en términos de $(1 + AB)^{-1}$, A y B, y probar que esta fórmula funciona en general).

Chapter 16

Derivadas formales

Sea C un anillo conmutativo. Sea $f(x) \in C[[x]]$. Entonces, $f(x+y)$ es un elemento del anillo de series de potencia en 2 variables $C[[x,y]]$. Podemos escribir

$$f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + f_3(x)y^3 + \dots.$$

Evaluando en $y = 0$ se tiene $f_0(x) = f(x)$. Definimos $\frac{d}{dx}(f(x)) = f'(x) = f_1(x)$. En otras palabras $f'(x)$ es la única serie de potencias en x tal que

$$f(x+y) \equiv f(x) + yf'(x) \pmod{y^2}.$$

Ejemplo 16.1. Si $f(x) = x^n$, el teorema del binomio nos dá $(x+y)^n \equiv x^n + nx^{n-1}y \pmod{y^2}$. Se concluye que $f'(x) = nx^{n-1}$.

Con esta definición, no es dificil comprobar las propiedades

$$\frac{d}{dx}[f(x)+g(x)] = f'(x)+g'(x), \qquad \frac{d}{dx}[f(x)g(x)] = f'(x)g(x)+f(x)g'(x),$$

Por ejemplo, probaremos la última.

$$\begin{aligned} f(x+y)g(x+y) &\equiv (f(x)+yf'(x))(g(x)+yg'(x)) \\ &\equiv f(x)g(x) + (f'(x)g(x)+f(x)g'(x))y \pmod{y^2}. \end{aligned}$$

Ejemplo 16.2. Si $f(x) = \sum_{i=0}^{n} a_i x^i$ es un polinomio, entonces $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

Proposición 16.3. *Para toda $f(x) \in (x)^n$, se tiene $\frac{d}{dx}(f(x)) \in (x)^{n-1}$.*

Demostración. Basta ver que si $f(x) \in (x^n)$, entonces podemos escribir $f(x) = x^n g(x)$ de donde $f'(x) = nx^{n-1}g(x) + x^n g'(x)$. □

Este resultado tiene la siguiente consecuencia:

Corolario 16.3.1. *Si $f_n(x) \to f(x)$ entonces $f_n'(x) \to f'(x)$.* □

Donde la convergencia en $C[[x]]$ debe entenderse en el sentido definido en el capítulo anterior. El lector con conocimientos básicos de topología interpretará este resultado diciendo que el operador $\frac{d}{dx}$ es continuo con respecto a la topología definida por (x).

Ejemplo 16.4. La continuidad nos permite generalizar el ejemplo anterior a series de potencia arbitrarias. En otras palabras, si $f(x) = \sum_{i=0}^{\infty} a_i x^i$, entonces $f'(x) = \sum_{i=1}^{\infty} i a_i x^{i-1}$.

Otra consecuencia de la definición y de la propiedad universal del anillo $C[[x]]$ es la siguiente:

Proposición 16.5 (Expansión de Taylor a primer orden)**.** *Sea B una C-álgebra conmutativa completa con respecto a un ideal I. Sea $f(x) \in C[[x]]$, y sean $u, \epsilon \in I$. Entonces se tiene que*

$$f(u+\epsilon) \equiv f(u) + f'(u)\epsilon \pmod{\epsilon^2}. \quad \square$$

Este resultado nos permite demostrar fácilmente la regla de la cadena.

Proposición 16.6 (Regla de la cadena)**.** *Si $f(x) \in C[[x]]$ y $w(x) \in (x)$, entonces $\frac{d}{dx}(f(w(x)) = f'(w(x))w'(x)$.*

Demostración. Observese que $w(x+y) \equiv w(x) + yw'(x) \pmod{y^2}$. Sea $h = w(x+y) - w(x)$. Entonces, y divide a h. Ahora escribimos

$$\begin{aligned} f(w(x+y)) &= f(w(x)+h) \\ &\equiv f(w(x)) + hf'(w(x)) && \pmod{h^2} \\ &\equiv f(w(x)) + (w'(x)y)f'(w(x)) && \pmod{y^2}. \quad \square \end{aligned}$$

Para polinomios existe una versión más sencilla que sigue inmediatamente de la propiedad universal de $C[x]$:

Proposición 16.7 (Expansión de Taylor a primer orden)**.** *Sea B una C-álgebra conmutativa. Para cualesquiera $f(x) \in C[x]$, $u, \epsilon \in B$ se tiene que*

$$f(u+\epsilon) \equiv f(u) + f'(u)\epsilon \pmod{\epsilon^2}. \quad \square$$

Ejemplo 16.8. Mostraremos ahora como la fórmula de Taylor puede utilizarse para resolver ecuaciones de congruencias. Tomemos por ejemplo la ecuación $x^2 \equiv 14 \pmod{13^2}$. Claramente la ecuación $x^2 \equiv 14 \pmod{13}$ tiene las soluciones 1 y -1, luego basta buscar soluciones del tipo $1+13t$ o $-1+13t$. Ahora bien, si $f(x) = x^2$, se tiene $f(1+13t) \equiv f(1) + 13tf'(1) \pmod{13^2}$, de donde necesitamos encontrar t tal que $14 \equiv f(1) + 13tf'(1) \equiv 1 + 13t \times 2 \pmod{13^2}$. Dividiendo por 13 se tiene $1 \equiv 2t \pmod{13}$, luego $t \equiv 7 \pmod{13}$ o $x \equiv 1 + 7 \times 13 \pmod{13^2}$. Del mismo modo se obtiene la solución $x \equiv -1 + 6 \times 13 \pmod{13^2}$.

Otra consecuencia de la expansión de Taylor a primer orden es la siguiente: Si C es un dominio de integridad, entonces para toda sucesión $\{\epsilon_n\}_n$ tal que $\epsilon \overset{n\to\infty}{\longrightarrow} 0$, y $\epsilon_n \neq 0$ para todo n, se tiene

$$f'(u) = \lim_{n\longrightarrow\infty} \frac{f(u+\epsilon_n) - f(u)}{\epsilon_n}. \tag{16.1}$$

donde la división tiene sentido, ya que el numerador es divisible por ϵ_n. Si $I = 0$ no existe una tal sucesión. Por otro lado, si $I \neq 0$ podemos tomar $x \in I$ con $x \neq 0$ y definir $\epsilon_n = x^n$, el que no se anula por ser C un dominio de integridad.

Una vez que se ha definido la derivada, podemos definir las derivadas sucesivas por inducción mediante $f^{(n+1)}(x) = \frac{d}{dx} f^{(n)}(x)$. Nótese que en la relación

$$f(x+y) = f(x) + f'(x)y + f_2(x)y^2 + f_3(x)y^3 + \dots$$

podemos considerar ambos lados como series de potencias en y con coeficientes en $C[[x]]$ de modo que al derivar ambos lados se tiene

$$f'(x+y) = f'(x) + 2f_2(x)y + 3f_3(x)y^2 + \dots,$$

y al evaluar en $y = 0$ se tiene $2f_2(x) = f''(x)$. Iterando este procedimiento se obtiene la relación $n!f_n(x) = f^{(n)}(x)$.

Observación 16.9. La relación $n!f_n(x) = f^{(n)}(x)$ puede demostrarse también considerando los coeficientes de la serie de potencias $f(x)$ como variables independientes y utilizando la propiedad universal de las series de potencia con coeficientes enteros, ya que es sabido que estas relaciones se satisfacen para series de potencias con coeficientes complejos. Nótese sin embargo que esa demostración requiere el uso de series de potencia en una cantidad numerable de variables.

Supongamos ahora que C es un $\mathbb{Q}$-álgebra (por ejemplo un cuerpo de caracteristica 0). Entonces tenemos la fórmula

$$f(x+y) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x)}{n!} y^n.$$

Esta fórmula recibe el nombre de fórmula de Taylor. Más generalmente, se tiene el siguiente resultado:

Proposición 16.10. *Sea C una $\mathbb{Q}$-álgebra conmutativa. Sea $f \in C[[x]]$. Sea A una C-álgebra conmutativa y completa respecto del ideal I. Sean $u, v \in I$. Entonces*

$$f(u+v) = \sum_{n=0}^{\infty} \frac{f^{(n)}(u)}{n!} v^n. \quad \square$$

Como antes, la fórmula de Taylor tiene una versión más general para polinomios:

Proposición 16.11. *Sea C una $\mathbb{Q}$-álgebra conmutativa. Sea $f(x)$ un polinomio con coeficientes en C. Para todo C-algebra conmutativa A, y todo par de elementos u y v en A, se tiene la fórmula*

$$f(u+v) = \sum_{n=0}^{\infty} \frac{f^{(n)}(u)}{n!} v^n.$$

Demostración. Esta es una aplicación directa de la propiedad universal de $C[x]$. $\square$

Observación 16.12. Nótese que la suma mencionada mas arriba es en realidad una suma finita, ya que alguna derivada de $f(x)$ es 0. Es por esta razón que la suma esta definida. Este no es el caso para una serie de potencias arbitraria, recuerdese que $f(x+1)$ no está definida si f no es un polinomio.

El teorema de la función inversa.

Proposición 16.13 (Lema de Hensel)**.** *Sea $f(x) \in C[[x]]$, $w(x) \in C[[x]]$, $u(x) \in (x)$ que satisfacen*

$$w(x) \equiv f(u(x)) \pmod{x^n}, \ f'(0) \in C^*.$$

Entonces existe una única solución $u'(x) \in (x)$ de la ecuación $w(x) = f(u'(x))$, que satisface $u(x) \equiv u'(x) \pmod{x^n}$.

Demostración. La condición $f'(0) \in C^*$ implica que $f'(t)$ es una unidad para todo $t \in (x)$. Del mismo modo, la condición $w(x) \equiv f(u(x)) \pmod{x}$ implica que $f(t) - w(x) \in (x)$ para todo $t \in (x)$. Sea $u_0 = u$. Si $u_n \in (x)$ está definido, definimos u_{n+1} mediante

$$u_{n+1} = u_n - \frac{f(u_n) - w}{f'(u_n)}.$$

Observese que $u_{n+1} \in (x)$. Además se tiene:

(1) $(u_n - u_{n+1}) = (f(u_n) - w)$.

(2) $(f(u_{n+1}) - w) \subseteq (f(u_n) - w)^2$.

La afirmación (1) es inmediata. Para demostrar (2), aplicamos la proposición 16.7 con $\epsilon = (f(u_n) - w)/f'(u_n)$. Se tiene

$$\begin{aligned} f(u_{n+1}) - w &= f(u_n - \epsilon) - w \\ &\equiv (f(u_n) - w) - f'(u_n)\epsilon \pmod{\epsilon^2} \\ &\equiv 0 \pmod{\epsilon^2}. \end{aligned}$$

Ahora, como $f'(u_n)$ es invertible, $(\epsilon) = (f(u_n) - w)$. Esto termina de probar (2). De (1) y (2) se obtiene fácilmente que la sucesión $\{u_n\}_{n=1}^{\infty}$ converge a un elemento u_∞ de (x) y se satisface $f(u_\infty) = 0$. De (1)y (2) se obtiene también por inducción que $u_n(x) \equiv u(x) \pmod{x^n}$ para todo n, luego $u_\infty(x) \equiv u(x) \pmod{x^n}$ □

Una consecuencia es el siguiente resultado:

Proposición 16.14 (teorema de la función inversa)**.** *Si $f(x) \in (x)$, satisface $f'(0) \in C^*$, entonces existe $g(x) \in (x)$ tal que $f(g(x)) = g(f(x)) = x$.*

Demostración. Dado que $f(x) \in I = (x)$ implica que $f(x) \equiv x \pmod{x}$, existe $g(x) \in I$ tal que $f(g(x)) = x$. En particular, por la regla de la cadena, se tiene que $f'(0)g'(0) = 1$. En particular, $g'(0) \neq 0$. Luego, repitiendo el argumento para g, se tiene que $g(h(x)) = x$ para algun $h(x) \in I$.

Con la composición de series de potencia, el elemento $f(x) \in I$ define una función $\tilde{f} : I \longrightarrow I$, definida por $u(x) \mapsto f(u(x))$. Análogamente se definen $\tilde{g}$, y $\tilde{h}$. La función $\tilde{f}$ es inversa por la izquierda de $\tilde{g}$, y $\tilde{h}$ es su inversa por la derecha. Se tiene que $\tilde{f} = \tilde{h}$ y, evaluando en x, $f(x) = h(x)$. □

Observación 16.15. Una función de la forma $\tilde{f}$ con $f(x) \in (x)$, $f'(0) \in C^*$ recibe el nombre de cambio de coordenadas.

Ejemplo 16.16. Si la característica de k no es 2, entonces existe una serie de potencias $w(x)$ tal que $w(x)^2 + 2w(x) = x$. En particular, $1 + x$ es un cuadrado. Si la característica de k fuese 0 entonces basta tomar $w(x) = e^{\frac{1}{2}\ln(1+x)} - 1$.

Ejercicios

1. Sea $V = \mathbb{Q}[x]_n$ el espacio de polinomios de grado no mayor a n. Sean $\Delta, D : V \to V$, definidos por $Df(x) = f'(x)$, $\Delta f(x) = f(x+1) - f(x)$.

   a) Probar que D y Δ son nilpotentes en $\mathrm{End}_{\mathbb{Q}}(V)$.

   b) Sea $\mathbb{Q}[D]$ la imagen de $\mathbb{Q}[x]$ bajo el homomorfismo que envía x a D. Probar que $\mathbb{Q}[D]$ es completo respecto de (D).

   c) Probar que $1+\Delta = e^D$ (puede asumir la fórmula de Taylor). Concluir que $D = \ln(1 + \Delta)$.

   d) Probar que $\Delta\binom{x}{n} = \binom{x}{n-1}$. Concluir que

   $$\frac{d}{dx}\binom{x}{n} = \sum_{k=0}^{n} \frac{1}{k}\binom{x}{n-k}.$$

   e) Usar la expansión binomial de $(1 + \Delta)^k$ para probar que

   $$\binom{x+k}{n} = \sum_{m=0}^{n} \binom{k}{m}\binom{x}{n-m}.$$

   Concluir que $\binom{2n}{n} = \sum_{m=0}^{n} \binom{n}{m}^2$.

2. Sea $C = \mathbb{Z}/2\mathbb{Z}$. Probar que el polinomio $f(x) \in C[x]$ satisface $f'(x) = 0$ si y sólo si existe $g(x)$ tal que $f(x) = g(x)^2$.

3. Sea C un anillo conmutativo, y sean $f(x), g(x) \in C[[x]]$. Probar que si $g(0) \in C^*$, entonces

   $$\left(\frac{f(x)}{g(x)}\right)' = \frac{f'(x)g(x) - f(x)g'(x)}{g(x)^2}.$$

4. Considerese el anillo completo (no conmutativo) $\mathbb{M}_2(\mathbb{R}[[x]])$. Cada elemento de este anillo puede escribirse como una serie de potencias con coeficientes matriciales.

   a) Probar que $e^{Ax}e^{Bx} = e^{(A+B)x}$ si y sólo si $AB = BA$.

   b) Probar que si $A(0)$ es invertible, entonces $(A(x)^{-1})' = A(x)^{-1}A'(x)A(x)^{-1}$.

   c) La matriz $B(x) = e^{Ax}$ satisface $B'(x) = A \cdot B(x)$.

5. Sea $f(x) = \cos(\text{sen}(e^x - 1))$. Probar que $f^{(n)}(0) \in \mathbb{Q}$ para todo n. Puede decirse lo mismo de $g(x) = \cos(\text{sen}(e^x))$?.

Chapter 17

Generadores y relaciones

En este capítulo formalizaremos el proceso de definir un anillo en terminos de generadores y relaciones.

Una *palabra* en los simbolos $\{x_1, \ldots, x_n\}$ es cualquer sucesión finita de elementos de $\{x_1, \ldots, x_n\}$. Como es costumbre, utilizaremos exponentes para denotar la precencia repetida de un mismo elemento, por ejemplo escribiremos $x_1x_3^5x_4^2$ en vez de $x_1x_3x_3x_3x_3x_3x_4x_4$. Sea C un anillo conmutativo. La *C-algebra libre* en los generadores $\{x_1, \ldots, x_n\}$ es el anillo $C\langle x_1, \ldots, x_n\rangle$, formado por todas las expresiones del tipo

$$\sum_{\sigma\in\Sigma} a_\sigma\sigma,$$

donde Σ es un conjunto finito de palabras en $\{x_1, \ldots, x_n\}$. La suma y producto en $C\langle x_1, \ldots, x_n\rangle$ se definen por las fórmulas

$$\sum_{\sigma\in\Sigma} a_\sigma\sigma + \sum_{\sigma\in\Sigma} b_\sigma\sigma = \sum_{\sigma\in\Sigma}(a_\sigma + b_\sigma)\sigma$$

y

$$\left(\sum_{\sigma\in\Sigma} a_\sigma\sigma\right)\left(\sum_{\sigma\in\Sigma} b_\sigma\sigma\right) = \sum_{\sigma\in\Sigma} c_\sigma\sigma,$$

donde

$$c_\sigma = \sum_{\tau\lambda=\sigma} a_\tau b_\lambda.$$

Aqui, $\tau\lambda$ denota la palabra obtenida escribiendo τ y luego λ con las convenciones mencionadas mas arriba, es decir $(x_1^2x_2^3)(x_2^2x_1^4) = x_1^2x_2^5x_1^4$. Dejamos

al lector comprobar que $C\langle x_1, \ldots, x_n\rangle$ es un anillo (de hecho un C-álgebra) unitario no conmutativo (salvo para $n = 1$).

Mas generalmente, si $\{x_i\}_{i\in I}$ es cualquier familia de simbolos, podemos definir análogamente el anillo $C\langle\{x_i\}_{i\in I}\rangle$. Los detalles se dejan al lector.

Si R es una colección de elementos de $C\langle\{x_i\}_{i\in I}\rangle$, y si J es el ideal mas pequeño que contiene a R (el ideal generado por R), el anillo $C\langle\{x_i\}_{i\in I}|R\rangle$ es por definición el anillo $C\langle\{x_i\}_{i\in I}\rangle/J$.

Ejemplo 17.1. Sea K un cuerpo, y sean $a, b \in K$. El anillo de cuaterniones $\left(\frac{a,b}{K}\right)$ se define por

$$\left(\frac{a,b}{K}\right) = K\langle i, j|\{i^2 - a, j^2 - b, ij + ji\}\rangle.$$

Escribiremos también

$$\left(\frac{a,b}{K}\right) = K\langle i, j|i^2 = a, j^2 = b, ij = -ji\rangle.$$

Por ejemplo, $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$. Tambien se comprueba fácilmente que $\left(\frac{1,a}{K}\right) \cong \mathbb{M}_2(K)$, con el isomorfismo ϕ definido por

$$\phi(i) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \phi(j) = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}.$$

definición 17.2. Un monoide es un conjunto M con una operación $\cdot$ que satisface

a) $(mn)p = m(np)$ para todo $m, n, p \in M$.

b) Existe $1 \in M$ tal que $1m = m1 = m$ para todo $m \in M$.

Si $(M, \cdot)$ es un monoide, definimos

$$C[M] = C\langle\{x_m\}_{m\in M}|\{x_m x_n - x_{mn}\}_{m,n\in M}\rangle.$$

Si M es un grupo, $C[M]$ se llama el algebra de grupo de M con coeficientes en C.

Ejemplo 17.3. El anillo $C[\mathbb{N}_0]$, donde $\mathbb{N}_0$ es el monoide de enteros no negativos, es el anillo de polinomios en una variable con coeficientes en C. El anillo $C[\mathbb{N}_0^n]$, es el anillo de polinomios en n variables.

Ejemplo 17.4. El anillo $C[\mathbb{Z}]$ se llama el anillo de polinomios de Laurent con coeficientes en C, por ejemplo, $x^{-2} + x^4 \in C[\mathbb{Z}]$. Este anillo se denota también $C[x, x^{-1}]$.

Ejemplo 17.5. El anillo $C[\mathbb{Q}_{\geq 0}]$ de polinomios con exponentes racionales no negativos, tiene un ideal maximal $\mathfrak{m}$ generado por las potencias x^r con $r > 0$. Este ideal satisface $\mathfrak{m}^2 = \mathfrak{m}$, pero este ideal no está generado por un idempotente.

Ejemplo 17.6. Considerese el algebra de grupo $\mathbb{C}[C_2]$, donde $\mathbb{C}$ es el cuerpo de números complejos, y C_2 es el grupo con 2 elementos. El lector puede demostrar fácilmente que

$$\mathbb{C}[C_2] \cong \mathbb{C}[x]/(x^2 - 1).$$

Si σ es el generador de C_2, entonces $P = \frac{1}{2}(1 + x_\sigma)$ es un idempotente central, y cada uno de los anillos $P\mathbb{C}$ y $(1 - P)\mathbb{C}$ es isomorfo a $\mathbb{C}$, de donde $\mathbb{C}[C_2] \cong \mathbb{C} \times \mathbb{C}$. Mas generalmente, para todo grupo finito G, el elemento

$$N = \frac{1}{|G|} \sum_{g \in G} x_g \in \mathbb{C}[G]$$

es un idempotente central.

Ejemplo 17.7. El anillo $\mathbb{C}[\mathbb{N}]$, donde $\mathbb{N}$ es el monoide *multiplicativo* de enteros positivos es útil para el estudio de funciones aritméticas, es decir funciones complejas definidas en $\mathbb{N}$. Es posible definir un anillo $\mathbb{C}[[\mathbb{N}]]$, de series de dirichlet que extiende $\mathbb{C}[\mathbb{N}]$. los elementos de $\mathbb{C}[[\mathbb{N}]]$ son sumas formales del tipo

$$f = \sum_{n \in \mathbb{N}} a_n[n], \qquad g = \sum_{n \in \mathbb{N}} b_n[n].$$

La suma y el producto se definen mediante

$$f + g = \sum_{n \in \mathbb{N}} (a_n + b_n)[n],$$

y

$$fg = \sum_{n \in \mathbb{N}} c_n[n], \qquad c_n = \sum_{d|n} a_d b_{n/d}.$$

Una importante aplicación de este anillo es la fórmula de inversión de möbius

$$f(n) = \sum_{d|n} g(d) \Rightarrow g(n) = \sum_{d|n} f(d)\mu(n/d),$$

donde μ es la función definida por

$$\mu(n) = \left\{ \begin{array}{ccl} 0 & \text{if} & n \text{ es divisible por un cuadrado} \\ 1 & \text{if} & n = 1 \\ (-1)^t & \text{if} & n = p_1 \dots p_t \text{ donde } p_1, \dots, p_t \text{ son primos distintos} \end{array} \right|$$

Esta fórmula se deduce de la identidad

$$\left(\sum_{n \in \mathbb{N}} [n] \right) \left(\sum_{n \in \mathbb{N}} \mu(n)[n] \right) = 1.$$

Los detalles se dejan al lector.

Ejercicios

1. Probar que $\mathbb{C}[C_n] \cong \underbrace{\mathbb{C} \times \ldots \times \mathbb{C}}_{n}$, donde C_n es el grupo cíclico con n elementos.
2. Probar que $\left(\frac{a^2b, c^2d}{K}\right) \cong \left(\frac{b,d}{K}\right)$ y que $\left(\frac{a,1}{K}\right) \cong \left(\frac{a,-a}{K}\right) \cong \mathbb{M}_2(K)$.
3. Probar que $\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{M}_2(\mathbb{C})$ (sugerencia, considere las matrices

   $$\left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right), \qquad \left(\begin{array}{cc} \omega & 0 \\ 0 & \omega^{-1} \end{array} \right)$$

   donde omega es una raiz cúbica de la unidad y los elementos

   $$P_1 = \sum_{\sigma \in S_3} \sigma, \ P_2 = \sum_{\sigma \in S_3} \text{sign}(\sigma)\sigma$$

).

Chapter 18

Localización

Sea C un anillo conmutativo. Un conjunto multiplicativo es un subconjunto no vacío $S \subseteq C$ tal que:

- $0 \notin S$.
- Para todo $s_1, s_2 \in S$, $s_1 s_2 \in S$.

Nótese que S puede tener divisores de 0, pero si $ab = 0$, S no contiene *simultaneamente* a a y b.

La *localización* de C por S es el anillo

$$S^{-1}C = \{(a, b) | a \in C, b \in S\} / \equiv,$$

donde la relación de equivalencia $\equiv$ se define por

$$(a, b) \equiv (a', b') \Leftrightarrow s(ab' - a'b) = 0 \text{ para algún } s \in S.$$

La clase de equivalencia de (a, b) se denota $\frac{a}{b}$. La suma y la multiplicación en $S^{-1}C$ se definen por

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'},$$

$$\frac{a}{b} \times \frac{a'}{b'} = \frac{aa'}{bb'}.$$

Con estas operaciones, $S^{-1}C$ es un anillo con la unidad $1_{S^{-1}C} = \frac{s}{s}$. La comprobación de todas las propiedades de anillo se deja al lector. Existe un homomorfismo $\phi_S : C \to S^{-1}C$ dado por $\phi_S(c) = \frac{sc}{s}$. El núcleo de este homomorfismo es el ideal

$$I_S = \{c \in C | sc = 0 \text{ para algún } s \in S\}.$$

Si S no contiene divisores de 0, entonces ϕ es inyectiva. En este caso, la unidad de la localización bebe escribirse como una fracción del tipo $\frac{s}{s}$. En general, la unidad de la localización puede escribirse también en la forma $\frac{s+j}{s}$, donde $j \in I_S$ para $s \in S$.

Un conjunto multiplicativo S no necesita contener a 1_C, pero $S_1 = S \cup \{1_C\}$ es también un conjunto multiplicativo y se tiene que $S^{-1}C \cong S_1^{-1}C$, dado que la fracción $\frac{c}{1}$ es igual a $\frac{sc}{s}$ para cualquier $s \in S$, y si la identidad $s(ab' - a'b) = 0$ se cumple con $s = s_2 \in S_1$ se cumple tambien para algún $s = s_2 \in S$ (lo que es obvio exepto si $s_1 = 1$, en cuyo caso *cualquier* s_2 sirve). Por esta razón puede suponerse siempre que $1 \in S$, como haremos en lo sucesivo. Mas generalmente, se tiene el siguiente resultado:

Proposición 18.1. *Si $ab \in S$ para algún $b \in C$, y si definimos S_a como el conjunto multiplicativo mas pequeño que contiene a a y S, entonces $S^{-1}C \cong S_a^{-1}C$.*

Demostración Con la definición dada S_a es el conjunto $\bigcup_{n=0}^{\infty} a^n S$. Este conjunto es claramente cerrado bajo productos y si $a^n s = 0$ entonces también se anula $(ab)^n s \in S$. En particular, como $S \subseteq S_a$, toda fracción $\frac{t}{s}$ en $S^{-1}C$ es también una fracción en $S_a^{-1}C$. Llamaremos ϕ a la función que lleva la fracción $\frac{t}{s}$ en $S^{-1}C$ a la correspondiente fracción en $S_a^{-1}C$. Esta función está bien definida (ejercicio). Toda fracción en $S^{-1}C$ es de la forma $\frac{t}{a^n s}$, la cual es igual a $\frac{tb^n}{(ab)^n s}$. Por lo tanto ϕ es epiyectiva. por otro lado, si las fracciones $\frac{x}{y}$ y $\frac{x'}{y'}$ coinciden como elementos de $S_a^{-1}C$ entonces $a^r s(xy' - x'y) = 0$ para algún $s \in S$ y $r \in \mathbb{N}_0$. Esto implica $(ab)^r s(xy' - x'y) = 0$ donde $(ab)^r s \in S$, por lo que la función $S^{-1}C \to S_a^{-1}C$ es inyectiva. Es inmediato ahora de la definición de suma y multiplicación de $S^{-1}C$ que ϕ es un isomorfismo de anillos. □

En particular, sienpre se puede suponer que si $ab \in S$ entonces a y b pertenecen a S. Un conjunto multiplicativo con esta propiedad se dice saturado.

Ejemplo 18.2. Si D es un dominio de integridad, y $S = D - \{0\}$, entonces $S^{-1}D$ es un cuerpo, llamado el cuerpo de cocientes de D, y se denota $\mathfrak{Quot}(D)$. Por ejemplo, $\mathfrak{Quot}(\mathbb{Z}) = \mathbb{Q}$. El cuerpo $k(x) = \mathfrak{Quot}(k[x])$ se llama el cuerpo de funciones racionales sobre k. El cuerpo $k((x)) = \mathfrak{Quot}(k[[x]])$ se llama el cuerpo de series de Laurent sobre k. Cada elemento de $k((x))$ puede

escribirse en la forma

$$a_n x^n + a_{n+1}x^{n+1} + a_{n+2}x^{n+2} + a_{n+3}x^{n+3} + \ldots,$$

con $n \in \mathbb{Z}$.

Ejemplo 18.3. Mas generalmente, si C es un anillo conmutativo arbitrario y S es el conjunto de elementos de C que no son divisores de 0, entonces S es el mayor subconjunto multiplicativo de C tal que el homomorfismo canónico de C en $S^{-1}C$ es inyectivo. Este anillo recibe el nombre de anillo completo de fracciones de C.

Ejemplo 18.4. Si $\wp \subseteq C$ es un ideal primo, $S_\wp = C - \wp$ es un conjunto multiplicativo. El anillo $S_\wp^{-1}C$ se denota $C_\wp$, y se llama la localización de C en el *lugar* $\wp$. Nótese que todo elemento de C que no está en $\wp$ es invertible en $C_\wp$.

Ejemplo 18.5. Si $C = C_1 \times C_2$, y si S contiene un elemento de la forma $(a, 0)$ entonces la imagen de $(0, 1)$ en $S^{-1}C$ es trivial. Si S_1 es el conjunto de primeras coordenadas de elementos de S, se tiene que S_1 es un conjunto multiplicativo (que no contiene al 0, ya que $(0, r) \in S$ implica $(a, 0)(0, r) = (0, 0) \in S$) y se tiene $S^{-1}C \cong S_1^{-1}C_1$. El lector puede demostrar esto directamente como ejercicio, aunque es un caso particular de la proposición 18.15 mas abajo. Por ejemplo si $C = \mathbb{Z}/6\mathbb{Z}$ y $S = \{\overline{3}\}$, se tiene $S^{-1}C \cong \mathbb{Z}/2\mathbb{Z}$.

Ejemplo 18.6. Si S_1 es un conjunto multiplicativo de C_1 y S_2 es un conjunto multiplicativo de C_2, entonces $S = S_1 \times S_2$ es un conjunto multiplicativo de $C = C_1 \times C_2$ y se tiene $S^{-1}C \cong S_1^{-1}C_1 \times S_2^{-1}C_2$.

Observación 18.7. En general, si $\phi : C \to C'$ es un homomorfismo, el ideal $\phi_*(I)$ se define como el ideal mas pequeo de C' que contiene a la imagen $\phi(I)$. De hecho

$$\phi_*(I) = \left\{ \sum_n a_n \phi(j_n) | a_n \in C', j_n \in I \right\}.$$

Si $\phi C \to S^{-1}C$ es el homomorfismo canónico, el ideal $\phi_*(I)$ se denota $S^{-1}I$. Tomando denominador común en una suma del tipo

$$\sum_n \frac{j_n}{1}\frac{a_n}{s_n}$$

se prueba que

$$S^{-1}I = \left\{ \frac{i}{s} \in S^{-1}C | i \in I \right\}$$

es un ideal de $S^{-1}C$. Nótese, sin embargo, que si I no es primo, $\frac{c}{s} \in S^{-1}I$ no implica $c \in I$.

Proposición 18.8. *Sea I un ideal de C. Sea*

$$I' = \{c \in C | cs \in I \text{ para algún } s \in S\}.$$

Entonces $\frac{c}{s} \in S^{-1}C$ si y sólo si $c \in I'$. En particular, la preimagen en C de $S^{-1}I$ es el ideal I'.

Demostración Si $c \in I'$ entonces $cs' \in I$ para algún $s' \in I$ luego $\frac{c}{s} = \frac{s'c}{s's} \in S^{-1}I$. Por otro lado, si $\frac{c}{s} = \frac{i}{s}'$ con $i \in I$, entonces $s''(cs' - is) = 0$ para algún $s'' \in S$, luego $cs's'' \in I$. La última observación es el caso particular $\frac{c}{s} = \frac{c}{1}$. □

La siguiente propiedad es inmediata de lo precedente.

Proposición 18.9. *Si S es un conjunto multiplicativo en C, y I es un ideal de C, entonces $S^{-1}I$ es un ideal propio de $S^{-1}C$ si y sólo si $I \cap S = \emptyset$.* □

De hecho es posible caracterizar de esta forma todos los ideales de la localización:

Lema 18.10. *Sea C un anillo conmutativo, y sea S un subconjunto multiplicativo. Todo ideal de $S^{-1}C$ es de la forma $S^{-1}I$, donde I es un ideal de C.*

Demostración Sea I' un ideal de $S^{-1}C$. Entonces

$$I = \phi_S^{-1}(I') = \left\{ i \in C \Big| \frac{i}{1} \in I' \right\}$$

es un ideal de C. Sea $I'' = S^{-1}I$. Entonces $I'' \subseteq I'$, ya que $\frac{i}{s} = \frac{i}{1} \times \frac{1}{s}$. Por otro lado, si $\frac{m}{s} \in I'$, entonces $\frac{m}{1} = \frac{s}{1} \times \frac{m}{s} \in I'$, luego $m \in I$ y $\frac{m}{1} \in I''$, luego $I' = I''$. □

Observación 18.11. De hecho, los ideales de $S^{-1}C$ están en correspondencia con los ideales I de C que satisfacen $I = \{a \in C | as \in I \text{ para algún } s \in S\}$.

Proposición 18.12. *Sea S un subjunto mulptiplicativo de D. Si D es un DIP entonces $S^{-1}D$ es un DIP.*

Demostración inmediata del lemma 18.10. □

Ejemplo 18.13. El anillo $\mathbb{Z}[\frac{1}{2}]$ en un DIP, ya que es una localización de $\mathbb{Z}$.

Ejemplo 18.14. El anillo $\mathbb{Z}[i, \frac{1}{3}]$ es un DIP, ya que es una localización de $\mathbb{Z}[i]$.

Otra importante propiedad de la localización es que "conmuta" con la operación de tomar cuociente, en el sentido siguiente:

Proposición 18.15. *Sea S un conjunto multiplicativo en C, y sea I un ideal tal que $I \cap S = \emptyset$. Si S' es la imagen de S en C/I, entonces*

$$(S')^{-1}[C/I] \cong S^{-1}C/S^{-1}I.$$

Demostración La función $\frac{a}{s} \to \frac{a+I}{s+I}$ es un homomorfismo epiyectivo bien definido entre $S^{-1}C$ y $(S')^{-1}[C/I]$ (Ejercicio). Un elemento $\frac{a}{s} \in S^{-1}C$ está en el núcleo sí y sólo si $(a + I)(s' + I) = 0 + I$ para algún $s' \in I$, es decir $as' \in I$ para algún $s' \in I$. Esto último equivale a $a \in I'$ lo que a su vez equivale a $\frac{a}{s} \in S^{-1}I$. □

Corolario 18.15.1. *Si $\wp$ es un ideal primo (maximal) tal que $\wp \cap S = \emptyset$, entonces $S^{-1}\wp$ es primo (maximal).* □

Proposición 18.16. *Todo ideal primo de $S^{-1}C$ es de la forma $S^{-1}\wp$ con $\wp$ primo.*

Demostración Si $\wp'$ es un ideal primo de $S^{-1}C$, entonces $\wp = \phi_S^{-1}(\wp')$ es primo en C (ejercicio), y $\wp \cap S = \emptyset$. Si $\frac{p}{s} \in \wp'$, se tiene que $ps \in \wp$, luego $p \in \wp$. Se concluye que$\wp' = S^{-1}\wp$. □

Observación 18.17. No todo ideal maximal de $S^{-1}C$ es de la forma $S^{-1}I$ con I maximal.

Observación 18.18. El ideal $\wp C_\wp$ es maximal en $C_\wp$, de hecho, ya que todo elemento fuera de este ideal es invertible, $\wp C_\wp$ es el único ideal maximal en $C_\wp$.

definición 18.19. Un anillo A se dice local si tiene un único ideal bilátero maximal $\mathfrak{m}_A$. El ideal $\mathfrak{m}_A$ es el conjunto de elementos no-invertibles de A.

Ejemplo 18.20. El anillo $k[[x]]$ es local. Su único ideal maximal es (x).

Ejemplo 18.21. El anillo $\mathbb{Z}/p^n\mathbb{Z}$ es un anillo local para todo primo p.

Ejemplo 18.22. El anillo $C_\wp$ es un anillo local.

Ejemplo 18.23. El anillo local $\mathbb{Z}_{(p)}$ está formado por los racionales cuyo denominador no es divisible por p. Nótese que $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$. Es por esta razón que al trabajar con congruencias módulo p *no hace daño* suponer que estas fracciones están en $\mathbb{Z}/p\mathbb{Z}$.

Localización y factorización única

Primero estudiaremos el comportamiento de los primos bajo localización.

Proposición 18.24. *Sea C un anillo conmutativo, y sea S un subconjunto multiplicativo (sin 0). Si p es un primo de C, y si p no divide a ningún elemento de S, entonces p es un primo de $S^{-1}C$. Si p divide a algún elemento de S, entonces $\frac{p}{1} \in (S^{-1}C)^*$.*

Demostración Se sabe que si el ideal primo $\wp$ satisface $\wp \cap S = \emptyset$, entonces $\wp S^{-1}C$ es primo (ver el capítulo sobre localización). Por otro lado, si $pt = s \in S$, entonces

$$\frac{p}{1}\left(\frac{t}{s}\right) = \frac{1}{1}. \quad \square$$

Proposición 18.25. *Sea D un DFU y sea S un subjunto mulptiplicativo de D. Entonces $S^{-1}D$ es un DFU.*

Demostración Sea $\frac{m}{s} \in S^{-1}D$. Entonces m es producto de primos (y unidades) en D, y $\frac{1}{s}$ es una unidad. Ahora aplicamos el resultado anterior. $\square$

Chapter 19

Introducción a la Teoría de Cuerpos II

El Teorema de Extensión de Homomorfismos

Recordemos que se probó en el capítulo 6 la existencia de la clausura algebraica. En este capítulo probaremos la unicidad. Para ello, probaremos una importante propiedad de los homomorfismos de cuerpos.

Lema 19.1. *Sean K y L cuerpos, sea $F = K[\alpha]$ una extensión de K y sea $\phi : K \to L$ un homomorfismo. Sea $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ el polinomio irreducible de α, y sea $\phi(f) = x^n + \phi(a_{n-1})x^{n-1} + \ldots + \phi(a_1)x + \phi(a_0)$ su imagen bajo ϕ. Si $\beta \in L$ es una raiz de $\phi(f)$ entonces existe una único homomorfismo $\tilde{\phi} : F \to L$ tal que $\tilde{\phi}(\alpha) = \beta$ y $\tilde{\phi}|_K = \phi$.*

Demostración Por la propiedad universal de los polinomios, la evaluación en β define un homomorfismo $\psi : K[x] \to L$ definido por $g(x) \mapsto \phi(g)(\beta)$. Como $\phi(f)[\beta] = 0$ por definición, el polinomio f está en el núcleo de este homomorfismo. Como el ideal (f) es maximal en $K[x]$ se tiene que $(f) = \ker(\psi)$. El resultado sigue ahora del primer teorema de isomorfía. □

Proposición 19.2. *Si F/K es una extensión algebraica y $\phi : K \to L$ es un homomorfismo con L algebraicamente cerrado, entonces existe un homomorfismo $\tilde{\phi} : F \to L$ tal que $\tilde{\phi}|_K = \phi$.*

Demostración Sea Σ la colección de pares (E, ψ) donde E es un cuerpo con $K \subseteq E \subseteq F$ y ψ es una extensión de ϕ a E. Definimos el orden en Σ por

$(E, \psi) < (E', \psi')$ si $E \subseteq E'$ y ψ' extiende ψ. Como (K, ϕ) está en Σ, este no es vacio. Si $\{(E_\lambda, \psi_\lambda)\}_{\lambda \in \Lambda}$ es una cadena en Σ se define un homomorfismo ψ en $E = \bigcup_\lambda E_\lambda$ tal que si $a \in E_\lambda \subseteq E$ entonces $\psi(a) = \psi_\lambda(a)$. Con esta definición (E, ψ) es una cota superior de la cadena. Por lema de zorn, Σ tiene un elemento maximal (Γ, τ). Si $\alpha \notin \Gamma$ el lemma anterior prueba que τ puede extenderse a $\Gamma[\alpha]$ lo que contradice la maximalidad. Se concluye que $\Gamma = F$. □

Proposición 19.3. *Dos clausuras algebraicas sobre el mismo cuerpo son isomorfas.*

Demostración Sean L y L' dos clausuras algebraicas de K. Por la proposición anterior, la inclusión $i : K \to L'$ se extiende a un homomorfismo $\phi : L \to L'$. Como L es algebraicamente cerrado tambien lo es su imagen $\phi(L) \subseteq L'$. Afirmamos que $\phi(L) = L'$. Para esto observamos que si $\alpha \in L'$ su polinomio irreducible sobre $\phi(L)$ debe ser lineal ya que estos son los únicos polinomios irreducibles sobre un cuerpo algebraicamente cerrado, pero entonces $\alpha \in \phi(L)$. Como α era arbitrario se obtiene lo pedido. □

Nótese sin embargo que la extensión de homomorfismos y por lo tanto el isomorfismo entre las clausuras algebraicas no es canónico. en particular, si L es una extensión algebraica de K, siempre puede identificarse L con un subcuerpo de $\overline{K}$ pero no de manera única.

Extensiones Separables e inseparables

Sea L/K una extensión algebraica. Un elemento α de L se dice separable si y sólo si el polinomio irreducible $m_\alpha(x)$ de α tiene raices distintas en $\overline{K}$, es decir

$$m_\alpha(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

donde $\alpha_1, \ldots, \alpha_n$ son distintos. En caso contrario se dice que α es inseparable sobre K.

El lema siguiente es un cálculo directo usando la regla del producto:

Lema 19.4. *Si $g(x)^2$ divide a $f(x)$ entonces $g(x)$ divide a su derivada $f'(x)$.* □

Proposición 19.5. *α es separable sobre K si y sólo si su polinomio irreducible satisface $m'_\alpha(x) \neq 0$.*

Demostración Si $m'_\alpha(x) \neq 0$ entonces como $m_\alpha(x)$ es irreducible en $K[x]$ y su derivada es de grado menor, necesariamente $m_\alpha(x)$ y $m_\alpha(x)$ son relativamente primos. Se deduce que existen $t(x)$ y $s(x)$ en $K[x]$ tales que

$$t(x)m_\alpha(x) + s(x)m'_\alpha(x) = 1$$

en $K[x]$ y por lo tanto también en $\overline{K}[x]$. Se concluye que $m_\alpha(x)$ y su derivada son relativamente primos en $\overline{K}[x]$ por lo que no puede haber una raiz doble por el lema precedente. Por otro lado, si $m'_\alpha(x) = 0$ entonces para toda raiz u de $m_\alpha(x)$ se tiene que $x - u$ divide a $m_\alpha(x)$ (en $\overline{K}[x]$), es decir $m_\alpha(x) = g(x)(x - u)$ para algún polinomio $g(x) \in \overline{K}[x]$. Derivando se tiene $0 = m'_\alpha(x) = g'(x)(x-u) + g(x)$, de donde al evaluar en u se tiene $g(u) = 0$, por lo que u es una raiz múltiple. □

En particular se concluye de la demostración que si α no es separable *cada* raiz de su polinomio irreducible es una raiz múltiple.

Ejemplo 19.6. Si K tiene característica 0 cada elemento α algebraico sobre K es separable.

Ejemplo 19.7. Si L es el cuerpo de funciones racionales en la variable y sobre el cuerpo $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, es decir $L = \mathbb{F}_2(y)$ y si K es el subcuerpo $K = \mathbb{F}_2(y^2)$, entonces el polinomio minimal de y sobre K es $x^2 - y^2 \in K[x]$. En este caso su derivada es 0, luego y no es separable sobre K.

Proposición 19.8. *Si α es inseparable sobre K entonces existe un polinomio $g(x)$ tal que $m_\alpha(x) = g(x^p)$ donde p es la característica de K.*

Demostración Sea

$$m_\alpha(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

Entonces

$$m'_\alpha(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-1} + \ldots + 2a_2 x + a_1.$$

Se concluye que si $m'_\alpha(x) = 0$, entonces $ka_k = 0$ para todo k, y por lo tanto a_k puede ser no nulo si y sólo sí p divide a k. Se concluye que

$$m_\alpha(x) = a_{pr}x^{pr} + a_{p(r-1)}x^{p(r-1)} + \ldots + a_p x^p + a_0.$$

Basta ahora tomar

$$g(x) = a_{pr}x^r + a_{p(r-1)}x^{r-1} + \ldots + a_p x + a_0.$$

□

definición 19.9. Un cuerpo K se dice perfecto si todo elemento de $\overline{K}$ es separable sobre K.

Se sigue de la definición que todo cuerpo de característica 0 es perfecto.

Proposición 19.10. *Un cuerpo de característica p es perfecto si y sólo si todo elemento de K es una p-potencia.*

Demostración Si algún $a \in K$ no es una p-potencia y si b es una raiz en $\overline{K}$ de $x^p - a = 0$, entonces b no es separable sobre K. Por otro lado, si todo elemento de K es una p-potencia y si α es un elemento inseparable con polinomio irreducible

$$m_\alpha(x) = a_r x^{pr} + a_{r-1}x^{p(r-1)} + \ldots + a_1 x^p + a_0,$$

tomamos elementos $b_i \in K$ que satisfacen $b_i^p = a_i$, y definimos

$$h(x) = b_r x^r + b_{r-1}x^{r-1} + \ldots + b_1 x + b_0,$$

y se obtiene que $h(x)^p = m_\alpha(x)$ lo que contradice la irreducibilidad de m_α. □

Proposición 19.11. *Todos los cuerpos finitos son perfectos.*

Demostración Basta ver que todo elemento es una p-potencia, donde p es la característica, pero si $x^p = y^p$ entonces $(x-y)^p = x^p - y^p = 0$, por lo que $x = y$. Se concluye que la función $x \mapsto x^p$ en inyectiva y por lo tanto epiyectiva. □

Lema 19.12. *Sea $\phi : K \to E$ un homopmorfismo de cuerpos con E algebraicamente cerrado. Sea $\alpha \in \overline{K}$. Entonces existe exactamente una extensión de ϕ a $K[\alpha]$ por cada raiz de* $\mathrm{irr}_K(\alpha, x)$ *en $\overline{K}$.*

Demostración Sea $f(x) = \mathrm{irr}_K(\alpha, x) \in K[x]$. Si $\psi : K[\alpha] \to E$ es una tal extensión, entonces $\psi(\alpha)$ es raiz del polinomio $\phi(f) \in \phi(K)[x]$. Por otro lado si β es raiz de $\phi(f)$ en E, entonces por el lema [**?**] existe un homomorfismo $\widetilde{?}K[\alpha] \to E$ que satisface $\widetilde{\psi}(\bar{x}) = \beta$. Observamos ahora si $f(x) = h(x^{p^t})$ con t maximal, entonces h es irreducible y tiene por lo tanto raices distintas, de donde el número de raices de f es el grado de h. En particular, el número de raices de f es igual al número de raices de $\phi(f)$. □

Lema 19.13. *Sea $F = K[\alpha]$ y sea $f(x) = \mathrm{irr}_K(\alpha, x)$. Sea n el grado de f. Entonces para todo cuerpo algebraicamente cerrado L y cada homomorfismo $\psi : K \to L$, existen a lo más n homomorfismos $\phi : F \to L$ que extienden ψ con igualdad si y sólo si α es separable sobre K.*

Demostración La primera afirmación sigue de que ϕ está totalmente determinado por $\phi(\alpha)$ que es una raiz de $\psi(f)$. Por otro lado, el Lemma 19.12 implica que existe exactamente un homomorfismo ϕ por cada raiz de $\psi(f)$. Como f tiene raices distintas si y sólo si $f' = 0$, se sigue que f tiene raices distintas si y sólo si $\psi(f)$ tiene raices distintas, de donde se obtiene la segunda afirmación. □

Proposición 19.14. *Sea F/K una extensión finita de grado n. Entonces para todo cuerpo algebraicamente cerrado L y cada homomorfismo $\psi : K \to L$, existen a lo más n homomorfismos $\phi : F \to L$ que extienden ψ.*

Demostración Sea $F = K[\alpha_1, \ldots, \alpha_r]$. Utilizaremos inducción en r. El caso $r = 1$ es el lema previo. Sea $F' = K[\alpha_1, \ldots, \alpha_{r-1}]$, y sea $m = [F' : K]$. Por hipótesis de inducción existen a lo más m extensiones de ψ a F' y cada una puede extenderse a $F = F'[\alpha_r]$ de $n/m = [F : F']$ maneras. □

Proposición 19.15. *Sea $F = K[\alpha_1, \ldots, \alpha_r]$ una extensión finita de K. Las siguientes afirmaciones son equivalentes:*

1. *Todo $\alpha \in F$ es separable sobre K.*
2. *Cada α_i es separable sobre K.*
3. *Para todo cuerpo algebraicamente cerrado L y cada homomorfismo $\psi : K \to L$, existen exactamente $[F : K]$ homomorfismos $\phi : F \to L$ que extienden ψ.*
4. *P Existen exactamente $[F : K]$ homomorfismos $\phi : F \to \overline{K}$ que extienden la contención $K \hookrightarrow \overline{K}$.*

Demostración (1) $\Rightarrow$ (2) y (3) $\Rightarrow$ (4) son triviales. Para (4) $\Rightarrow$ (1) observamos que cada homomorfismo $\phi : K[\alpha] \to \overline{K}$ puede extenderse a F de a lo más $[F : K[\alpha]]$ maneras, luego la identidad se extiende a $K[\alpha]$ de al menos $[F : K]/[F : K[\alpha]] = [K[\alpha] : K]$ maneras y aplicamos el lema 19.13. Finalmente, para (2) $\Rightarrow$ (3) utilizamos inducción en el lema 19.13. □

Una extensión algebraica F/K se dice separable si todo elemento α en F es separable sobre K. Se sigue que para extensiones finitas la separabilidad es equivalente a cualquiera de las condiciones $(1)-(4)$. Nótese que si F/K es separable entonces F es separable sobre cualquier subcuerpo que contenga a K.

Extensiones totalmente inseparables

En este capítulo estudiaremos el concepto opuesto al de extensiones separables. El de extensiones totalmente inseparables. En una extensión algebraica L/K, un elemento α de L se dice totalmente inseparable sobre K si su polinomio irreducible sobre K tiene una única raiz en $\overline{K}$. Una extensión algebraica L/K se dice totalmente inseparable si cada elemento de L es totalmente inseparable sobre K.

Ejemplo 19.16. Si K es un cuerpo de característica p, y si a es un elemento de K que no está en K^p, entonces la (única) raiz α de $X^p - a$ es totalmente inseparable sobre K ya que en $\overline{K}[X]$ se tiene $X^p - a = (X-\alpha)^p$.

Recordemos que por la proposición 19.8, un polinomio irreducible $f(x)$ tiene raices distintas sí y sólo si $f(x) = g(x^p)$ para algún polinomio g. Si f tiene una única raiz α, se sigue que g tiene también una única raiz, a saber α^p, por lo que este proceso puede iterarse hasta obtener $f(x) = x^{p^t} - a$. Se sigue que un elemento α es totalmente inseparable sobre un cuerpo K sí y sólo si α^{p^t} está en K para algún $t \geq 0$, y en dicho caso se tiene $\mathrm{irr}_K(\alpha, x) = x^{p^t} - \alpha^{p^t}$.

Una extensión algebraica L/K se dice totalmente inseparable sí y sólo si cada elemento de L es totalmente inseparable sobre K. Nótese que si F/K es totalmente inseparable entonces F es totalmente inseparable sobre cualquier subcuerpo que contenga a K. Se tiene una caracterización para dichas extensiones similar a la que obtuvimos previamente para las extensiones separables.

Proposición 19.17. *Sea $F = K[\alpha_1, \ldots, \alpha_r]$ una extensión finita de K. Suponga que F se identifica a un subcuerpo de $\overline{K}$. Las siguientes afirmaciones son equivalentes:*

1. *F/K es totalmente inseparrable.*
2. *Cada α_i es totalmente inseparable sobre K.*

3. *Para todo cuerpo algebraicamente cerrado L y cada homomorfismo $\psi : K \to L$, existen exactamente un homomorfismo $\phi : F \to L$ que extiende ψ.*

4. *Si $\phi : F \to \overline{K}$ es un homomorfismo cuya restricción a K es la contención $K \hookrightarrow \overline{K}$ entonces ϕ es la contención $F \hookrightarrow \overline{K}$.*

Demostración (1) $\Rightarrow$ (2) y (3) $\Rightarrow$ (4) son triviales. Para (4) $\Rightarrow$ (1) observamos que cada homomorfismo $\phi : K[\alpha] \to \overline{K}$ puede extenderse a F y dicha extensión debe coincidir con la identidad, luego ϕ es la identidad. Finalmente, para (2) $\Rightarrow$ (3) utilizamos inducción en el Lema 19.12. □

En particular, si α y β son totalmente inseparables sobre K, entonces también lo es cada elemento de $K(\alpha, \beta)$.

Corolario 19.17.1. *Si α y β son totalmente inseparables sobre K, también lo son $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$, y α/β (si $\beta \neq 0$).* □

Corolario 19.17.2. *Si L/K es una extensión algebraica, entonces el subconjunto*

$$L_{\text{T.I.}} = \{\alpha \in L | \alpha \text{ es totalmente inseparable sobre } K\}$$

es un subcuerpo de L que contiene a K. □

Similarmente, utilizando la Proposición 19.15 se demuestran los resultados equivalentes para extensiones separables.

Lema 19.18. *Si α y β son separables sobre K, también lo son $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$, y α/β (si $\beta \neq 0$).* □

Proposición 19.19. *Si L/K es una extensión algebraica, entonces el subconjunto*

$$L_{\text{Sep}} = \{\alpha \in L | \alpha \text{ es separable sobre } K\}$$

es un subcuerpo de L que contiene a K. □

Si α es algebraico sobre K, y si el polinomio $f(x) = \text{irr}_K(\alpha, x)$ satisface $f(x) = h(x^{p^t})$ con t maximal, entonces α^{p^t} es separable sobre K y α es totalmente inseparable sobre $K[\alpha^{p^t}]$. El siguiente resultado sigue:

Proposición 19.20. *Sea L/K una extensión algebraica. Entonces L es totalmente inseparable sobre L_{Sep}.* □

Sin embargo, no es siempre el caso que $L/L_{\text{T.I.}}$ sea separable, como lo demuestra el siguiente ejemplo:

Ejemplo 19.21. Sea F un cuerpo arbitrario, sea $L = F(x^{1/2}, y)$, y sea $K = F(\sigma, \tau)$ donde $\sigma = x + y$ y $\tau = xy$. Como σ y τ son las funciones simétricas elementales de x e y, es fácil ver que $L_{\text{Sep}} = F(x, y)$. Sin embargo, si u una función racional en $x^{1/2}$ e y, entonces u^{2^t} es una función racional de $x^{2^{t-1}}$ e y^{2^t}. Si u^{2^t} es simétrica en x e y se tiene que u^{2^t} es realmente una función racional de x^{2^t} e y^{2^t}, de donde u es una función racional simétrica de x e y. Se concluye que $L_{\text{T.I.}} = K$, pero L/K no es separable.

Existe, sin embargo, un caso en el que se puede garantizar que $L/L_{\text{T.I.}}$ sea separable.

Proposición 19.22. *Si L/K es normal, entonces $L/L_{\text{T.I.}}$ es separable.*

Demostración Obsérvese que si L/K es normal, entonces también lo es L_{Sep}/K, ya que si una raiz de un polinomio irreducible es separable también lo son todas las otras. En particular L_{Sep}/K es Galoisiana.

Supongamos primero que L/K es finita. Cada elemento $\sigma \in \text{Gal}(L_{\text{Sep}}/K)$ se extiende de manera única a $\widetilde{\sigma} : L \to \overline{K}$. Como L/K es normal, se tiene además $\widetilde{\sigma}(L) = L$ para todo tal $\widetilde{\sigma}$. En particular, el grupo $G = \text{Gal}(L/K)$ es isomorfo a $\text{Gal}(L_{\text{Sep}}/K)$ mediante $\sigma \mapsto \widetilde{\sigma}$. Afirmamos que el cuerpo fijo L^G de G es $L_{\text{T.I.}}$. Esto termina la demostración, ya que L/L^G es Galoisiana. Como todo homomorfismo $\phi : L_{\text{T.I.}} \to \overline{K}$ que es la identidad en K es la identidad en $L_{\text{T.I.}}$, la contención $L_{\text{T.I.}} \subseteq L^G$ es inmediata. Por otro lado si $\alpha \notin L_{\text{T.I.}}$, entonces existe una raiz α del polinomio $\text{irr}_K(\alpha, x)$ distinta de α. Existe por lo tanto un homomorfismo $\phi_0 : K[\alpha] \to \overline{K}$ que satisface $\phi_0(\alpha) = \beta$. Podemos extender ϕ_0 a un homomorfismo $\phi : L \to \overline{K}$, que necesariamente satisface $\phi(L) = L$ por la condición de normalidad, y aún satisface $\phi(\alpha) = \beta$. Dicho ϕ es un elemento de G que no fija a α.

Consideremos ahora el caso general. Sea sea $\alpha \in L$ y sea Σ/K una subextensión normal y finita de L/K. Entonces por lo ya demostrado, α es separable sobre $\Sigma_{\text{T.I.}} \subseteq L_{\text{T.I.}}$. □

Nótese que si bién L/K normal implica L_{Sep}/K Galoisiana, no es cierto que L_{Sep}/K Galoisiana implique L/K normal, como lo muestra el contraejemplo 19.21.

Ejercicios

Chapter 20

Teoría de Galois

Proposición 20.1. *Sea $F = K[\alpha_1, \ldots, \alpha_r] \subseteq \overline{K}$ una extensión finita de K. Las siguientes afirmaciones son equivalentes:*

1. *Para todo $\alpha \in F$ cada raiz en $\overline{K}$ del polinomio minimal de α sobre K está en F.*
2. *Para todo $i = 1, \ldots, r$ cada raiz en $\overline{K}$ del polinomio minimal de α_i sobre K está en F.*
3. *P Para cada homomorfismo $\phi : F \to \overline{K}$ que extiende la identidad en K se tiene que $\phi(F) = F$.*

Demostración (1) $\Rightarrow$ (2) es trivial. Para (3) $\Rightarrow$ (1) observamos que para cada raiz β del polinomio minimal de α existe un homomorfismo $\psi : K[\alpha] \to K[\beta]$ tal que $\psi(\alpha) = \beta$ y que este puede extenderse a un homomorfismo $\psi : F \to \overline{K}$. Se concluye que $\beta = \psi(\alpha) = \phi(\alpha) \in \phi(F) = F$. Para (2) $\Rightarrow$ (3) observamos que $\psi(F) = K[\psi(\alpha_1), \ldots, \psi(\alpha_r)]$ y cada $\psi(\alpha_i)$ es alguna raiz del polinomio minimal de α_i. □

Una extensión algebraica F/K (que podemos asumir contenida en $\overline{K}$) se dice normal si para todo elemento α en F cada raiz en $\overline{K}$ del polinomio minimal de α sobre K está en F. Se sigue que para extensiones finitas la separabilidad es equivalente a cualquiera de las condiciones $(1) - (3)$. nótese que si F/K es normal, F es normal sobre cualquier subcuerpo que contenga a K.

Ejemplo 20.2. Sea $f(x) \in K[x]$ un polinomio con raices $\alpha_1, \ldots, \alpha_n$ en $\overline{K}$. El cuerpo $F = K[\alpha_1, \ldots, \alpha_n]$ se llama el cuerpo de descomposición de $f(x)$.

Como F está generado por *Todas* las raices de cada divisor primo de f, se tiene que F/K es normal. Afirmamos que $[F : K] \leq n!$. De hecho si $E = K[\alpha]$ para alguna raiz α de f, entonces $f(x) = (x - \alpha)g(x)$ con $g(x) \in E[x]$ de grado $n - 1$ y el resultado sigue por inducción.

definición 20.3. Una extesión algebraica se dice *Galoisiana* si es normal y separable. Para una extensión Galoisiana F/K de grado n existen n automorfismos $\phi : F \to F$ que extienden la identidad de K. Estos forman un grupo llamado el grupo de Galois de F/K. Se denota $\mathrm{Gal}(F/K)$. Si E es un subcuerpo de F que contiene a K entonces F/E es también Galoisiana y $\mathrm{Gal}(F/E)$ es el subgrupo de automorfismos que son la identidad en E.

Ejemplo 20.4. Sea $f(x) \in K[x]$ un polinomio sin raices repetidas (es decir f y f' son relativamente primos). Sean $\alpha_1, \ldots, \alpha_n$ las raices de f en $\overline{K}$. Sea $F = K[\alpha_1, \ldots, \alpha_n]$ el cuerpo de descomposición de f. Entonces F/K es Galoisiana. Como un automorfismo τ que fija K está totalmente determinado por las imágenes $\tau(\alpha_i)$ y como τ debe llevar raices de f en raices de f, el automorfismo τ puede identificarse con la permutación $\tilde{\tau}$ en el grupo simétrico S_n que satisface $\tau(\alpha_i) = \alpha_{\tilde{\tau}(i)}$. Por lo tanto, el grupo $\mathrm{Gal}(F/K)$ se identifica a un subgrupo de S_n.

Los siguientes lemas serviran para demostrar los teoremas fundamentales de la teoría de Galois:

Lema 20.5. *Si L/K es una extensión Galoisisana y F/K es una extensión finita con $F \subseteq L$. Entonces existe $L' \subseteq L$ tal que $L' \supseteq F$ y L'/K es Galoisiana y finita. En particular, si L/K es infinita, entonces contiene subextensiones Galoisianas finitas de grado arbitrariamente grande.*

Demostración Sea $F = K[\alpha_1, \ldots, \alpha_t]$ y sea $\beta_1, \ldots, \beta_r$ la lista de todas las raices de los polinomios minimales de $\alpha_1, \ldots, \alpha_t$ en L (incluidos $\alpha_1, \ldots, \alpha_t$). Entonces $L' = K[\beta_1, \ldots, \beta_r] \supseteq F$ es una extensión normal de K y es separable ya que L lo es. □

Lema 20.6. *Sea D un dominio de integridad infinito. Sea $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ un polinomio tal que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in D^n$. Entonces f es el polinomio 0.*

Demostración Utilizaremos inducción sobre n. Si $n = 1$ un polinomio no nulo puede tener sólo una cantidad finita de raices en el cuerpo de cocientes de D. Supongamos ahora que el lema es cierto para $n = k$ y sea $n = k + 1$. Escribamos $f(x_1, \ldots, x_k, x_{k+1}) = g_m x_{k+1}^m + \ldots + g_1 x_{k+1} + g_0$ donde cada g_i es un polinomio en $x_1, \ldots, x_k$. Entonces si f se anula en cada punto de D^{k+1}, para cada $(a_1, \ldots, a_k) \in D^k$ el polinomio

$$g_m(a_1, \ldots, a_k)x_{k+1}^m + \ldots + g_1(a_1, \ldots, a_k)x_{k+1} + g_0(a_1, \ldots, a_k)$$

tiene infinitas raices, luego es el polinomio 0 y se tiene $g_i(a_1, \ldots, a_k) = 0$ para todo i. Por hypótesis de inducción cada g_i es el polinomio 0 y el resultado sigue. □

Necesitamos ahora algunos resultados del algebra lineal:

Lema 20.7. *Sea K un cuerpo. Si W es un subespacio propio de K^n entonces existe una forma lineal $l(x_1, \ldots, x_n) = a_1x_1 + \ldots + a_nx_n$ que se anula en cada elemento de W.*

Demostración Si $v = (a_1, \ldots, a_n)$ y $w = (b_1, \ldots, b_n)$ son elementos de K^n definimos $v \cdot w$ por $v \cdot w = a_1b_1 + \ldots + a_nb_n$. Claramente $v \mapsto v \cdot w$ es lineal para cada w fijo. Si $w_1, \ldots, w_r$ es una base de W, se tiene que $\psi : K^n \to K^r$ definida por $\psi(v) = (v \cdot w_1, v \cdot w_2, \ldots, v \cdot w_r)$ es lineal. Como $r = \dim W < n$ el núcleo de ϕ es no trivial, de donde existe v tal que $v \cdot w_i = 0$ para todo i. Como los w_i generan W se tiene $v \cdot w = 0$ para todo $w \in W$. □

Lema 20.8. *Sea K un cuerpo infinito sea V un espacio vectorial sobre K de dimensión finita. Si $V = \bigcup_{i=1}^N V_i$ donde cada V_i es un subespacio de V entonces $V = V_i$ para algún i.*

Demostración Podemos suponer $V = K^n$. Si $V_i \neq V$, existe una función lineal l_i no nula que se anula en V_i. Supongamos que ningún V_i es todo V. Sea $f(v) = \prod_i l_i(v)$. Para cada $v \in V$ existe i tal que $v \in V_i$, luego $l_i(v) = 0$ luego $f(v) = 0$. Se concluye que f es el polinomio 0. Como $K[x_1, \ldots, x_n]$ es un dominio de integridad se tiene $l_i = 0$ para algún i ($\Rightarrow\Leftarrow$). □

Proposición 20.9. *Supongamos que un grupo finito G actúa fielmente en un cuerpo L por automorfismos. Sea $K = \{x \in L | \sigma(x) = x \ \forall \sigma \in G\}$. Entonces K es un subcuerpo de L tal que L/K es una extensión finita Galoisiana y* $\mathrm{Gal}(L/K) = G$.

Demostración Sea $\alpha \in L$ y sea $\{\alpha_1, \ldots, \alpha^t\}$ su órbita bajo G. Sea $f(x) = \prod_{i=1}^{t}(x - \alpha_i)$. Claramente $f(\alpha) = 0$. Como G actúa en $K[x]$ por automorfismos mediante

$$\sigma(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0) = \sigma(a_n)x^n + \sigma(a_{n-1})x^{n-1} + \ldots + \sigma(a_1)x + \sigma(a_0),$$

se tiene que $f(x)$ es invariante y por lo tanto tiene sus coeficientes en K. Se concluye que L/K es algebraica y Galoisiana (pues f se descompone totalmente en L y tiene raices distintas). Sea L'/K una subextensión Galoisiana y finita de L/K que, si L/K fuese infinito, por el Lema 20.5 podríamos suponer de grado arbitrariamente grande. Por otro lado si L/K fuese finito podríamos tomar $L = L'$. Afirmamos que existe $\tau \in G$ tal que $\sigma(\alpha) = \tau(\alpha)$ para todo $\alpha \in L$. Esto demuestra que $|\mathrm{Gal}(L'/K)| < |G|$ lo que termina la demostración.

Supondremos primero que K es infinito. Entonces para todo $\alpha \in L'$ se tiene que $\sigma(\alpha)$ es una raiz del polinomio $f(x)$ definido en el parrafo precedente, luego es un elemento de la órbita de α. Se sigue que si para todo $\tau \in G$ definimos

$$V_\tau = \{x \in L' | \sigma(x) = \tau(x)\},$$

se tiene $L' = \bigcup_{\tau \in G} V_\tau$ y por el lema 20.8 se tiene $L' = V_\tau$ para algún τ lo que termina la demostración.

Supongamos ahora que $K = \mathbb{F}_{p^n}$ es un cuerpo finito. Entonces $L' = \mathbb{F}_{p^{ns}}$ para algún s. Sea x un generador de $\mathbb{F}^*_{p^{ns}}$. Entonces existe un $\tau \in G$ tal que $\tau(x) = \sigma(x)$. Como τ y σ son automorfismos se tiene $\tau(x^m) = \sigma(x^m)$ para todo m, y todo elemento de L' es una potencia de x. □

Ejemplo 20.10. Sea F un cuerpo arbitrario y sea $G \subseteq S_n$ donde S_n es el grupo simétrico. Entonces S_n actúa en $L = F(x_1, \ldots, x_n)$ mediante $\tau(x_i) = x_{\tau(i)}$. Por ejemplo si $\tau = (1234)$ entonces

$$\tau\left(\frac{x_1x_2 + x_3}{x_3^2x_4 + x_1}\right) = \frac{x_2x_3 + x_4}{x_4^2x_1 + x_2}.$$

En este caso L es una extensión Galoisiana del cuerpo invariante $K = L^G$. Por ejemplo si $G = S_n$, entonces $[L : K] = |G| = n!$. Como los coeficientes $\sigma_1, \ldots, \sigma_n$ del polinomio

$$\prod_{i=1}^{n}(T - x_i)^n = T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} - \ldots + (-1)^{n-1}\sigma_{n-1} + (-1)^n\sigma_n$$

pertenecen al cuerpo fijo de donde si $K' = F(\sigma_1, \ldots, \sigma_n)$ se tiene $K' \subseteq K$. Por otro lado L es el cuerpo de descomposición de $\prod_{i=1}^{n}(T - x_i)^n$ sobre K', de donde $[L : K'] \leq n! = [L : K]$. Se concluye que $K = K'$. Se concluye que toda función racional en $x_1, \ldots, x_n$ es una función racional de $\sigma_1, \ldots, \sigma_n$. Este resultado es una primera versión del teorema de las funciones simétricas. Las funciones $\sigma_1, \ldots, \sigma_n$ reciben el nombre de funciones simétricas elementales.

Proposición 20.11. *Sea L/K una extensión Galoisiana finita. Sea $G = \mathrm{Gal}(L/K)$. Entonces existe una biyección entre cuerpos F con $K \subseteq F \subseteq L$ y subgrupos H de G dada por $F \mapsto \mathrm{Gal}(L/F)$. La biyección inversa está dada por $H \mapsto L^H = \{x \in L | h(x) = x \ \forall h \in H\}$.*

Demostración Basta probar que $\mathrm{Gal}(L/L^H) = H$ y que $L^{\mathrm{Gal}(L/F)} = F$. La primera igualdad es inmediata de la Proposición 20.9. Es claro de las definiciones que $L^{\mathrm{Gal}(L/F)} \supseteq F$. Probaremos la inclusión contraria. Como L/F es Galoisiana, se tiene $[L : F] = |\mathrm{Gal}(L/F)|$. Se sigue de la Proposición 20.9 que $L/L^{\mathrm{Gal}(L/F)}$ es Galoisiana y $[L : L^{\mathrm{Gal}(L/F)}] = |\mathrm{Gal}(L/F)|$ de donde sigue la segunda igualdad. □

Proposición 20.12. *Sea L/K una extensión Galoisiana finita. Sea F un cuerpo con $K \subseteq F \subseteq L$. La extensión F/K es Galoisiana si y sólo si $\mathrm{Gal}(L/F)$ es normal en $\mathrm{Gal}(L/K)$ y en tal caso*

$$\mathrm{Gal}(F/K) \cong \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)}.$$

Demostración Si $\sigma \in \mathrm{Gal}(L/F)$, $\tau \in \mathrm{Gal}(L/K)$, para todo $x \in F$ se tiene $\tau\sigma\tau^{-1}[\tau(x)] = \tau(x)$. Se xoncluye que

$$\tau\mathrm{Gal}(L/F)\tau^{-1} = \mathrm{Gal}\Big(L/\tau(F)\Big).$$

Como si $\tau \in \mathrm{Gal}(L/K)$, se tiene $\tau(F) = F$, la primera afirmación es ahora inmediata. Para la segunda observemos que si F/K es Galoisiana entonces la restricción a F define un homomorfismo $\psi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ que es epiyectivo (ya que todo automorfismo se extiende) y su núcleo es $\mathrm{Gal}(L/F)$. □

Ejemplo 20.13. Sea K un cuerpo de característica distinta de 2. Si $L = K[\sqrt{a_1}, \ldots, \sqrt{a_n}]$ con cada a_i en K, todo elemento τ de $\mathrm{Gal}(L/K)$ está determinado por un vector $(\epsilon_1, \ldots, \epsilon_n) \in \mathbb{F}_2^n$ que satisface $\tau(\sqrt{a_i}) = (-1)^{\epsilon_i}\sqrt{a_i}$.

Supongamos que los a_i han sido escogidos de modo tal que $[L:K] = 2^n$ con lo que $\mathrm{Gal}(L/K) \cong \mathbb{F}_2^n$. Entonces toda extensión cuadrática de K contenida en L está determinada por un hiperplano de $\mathbb{F}_2^n$. Es decir $H = \{(\epsilon_1, \ldots, \epsilon_n) | \sum_i \beta_i \epsilon_i = 0\}$ para algún vector $(\beta_1, \ldots, \beta_n) \in \mathbb{F}_p^n$. Observemos que si $b = a_1^{\beta^1} \ldots a_n^{\beta_n} \in K$, entonces $\sqrt{b}$ está en L y es invariante por cualquier elemento de H. Se concluye que las únicas extensiones cuadráticas contenidas en L son de la forma $K[\sqrt{b}]$ para algún b como arriba. En particular, un sencillo argumento por inducción demuestra ahora que si ningún a_i es una combinación de los anteriores entonces de hecho $[L:K] = 2^n$.

Ejemplo 20.14. Sea F un cuerpo arbitrario. Sean $L = F(x_1, \ldots, x_n)$ y el subcuerpo de funciones simétricas, de modo que $\mathrm{Gal}(L/K) = S_n$. Si $n \leq 5$ el único subgrupo normal de S_n es A_n, de modo que el único coerpo F con $K \subseteq F \subseteq L$ y F/K normal es $F = L^{A_n}$. Este es la única extensión cuadrática de K contenida en L. Si $\delta = \prod_{i<j}(x_i - x_j)$ es fácil ver que $\tau(\delta) = \mathrm{sgn}(\tau)\delta$, de modo que de hecho $L^{A_n} = K(\delta)$.

Ejemplo 20.15. Sea $L/\mathbb{R}$ una extensión algebraica finita. Agregando raices si es necesario podemos asumir que $L/\mathbb{R}$ es Galoisiana y $\mathbb{C} \subseteq L$. Sea $G = \mathrm{Gal}(L/\mathbb{R})$. Si H es un 2-subgrupo de Sylow de G la extensión $L^H/\mathbb{R}$ tiene grado impar. Como todo polinomio de grado impar con coeficientes reales tiene una raiz real (lo que puede demostrarse utilizando métodos de Cálculo elemental), se concluye que $L^H = \mathbb{R}$ por lo que G debe ser un 2-grupo. Utilizando el hecho de que los p-grupos son solubles se concluye que si $[L : \mathbb{R}] > 2$ debe existir una extensión cuadrática no trivial $E/\mathbb{C}$ pero es fácil ver (utilizando por ejemplo la representación polar de los números complejos) que cada complejo tiene una raiz cuadrada. Se concluye que $\mathbb{C}$ es algebraicamente cerrado.

Independencia de los automorfismos

Proposición 20.16. *Sea L/K una extensión Galoisiana con grupo de Galois $G = \mathrm{Gal}(L/K)$. Si las constantes $\lambda_\sigma \in L$, donde σ recorre G, satisfacen*

$$\sum_{\sigma \in G} \lambda_\sigma \sigma(a) = 0, \ \forall a \in L,$$

entonces $\lambda_\sigma = 0$ para todo $\sigma \in G$.

Demostración Supongamos que se ha escogido una solución no trivial $\{\lambda_\sigma | \sigma \in G\}$ de

$$\sum_{\sigma \in G} \lambda_\sigma \sigma(a) = 0, \ \forall a \in L,$$

con el mínimo número de coeficientes no nulos. Observese que si

$$\sum_{\sigma \in G} \lambda_\sigma \sigma(a) = 0, \ \forall a \in L,$$

entonces en particular

$$\sum_{\sigma \in G} \lambda_\sigma \sigma\Big(\tau^{-1}(a)\Big) = 0, \ \forall a \in L.$$

Realizando el cambio de variables $\sigma = \xi\tau$, se tiene

$$\sum_{\xi \in G} \lambda_{\xi\tau} \xi(a) = 0, \ \forall a \in L.$$

Se concluye que si existe tal solución no trivial, puede suponerse que $\lambda_e \neq 0$, donde e es la identidad de G. Supongamos ahora que este es el caso. Entonces λ_e y al menos algún otro coeficiente λ_ρ son no nulos. Sea $t \in L$ con $\rho(t) \neq t$. Entonces, de la ecuación

$$\sum_{\sigma \in G} \lambda_\sigma \sigma(a) = 0, \ \forall a \in L,$$

se tiene en particular, remplazando a por ta,

$$\sum_{\sigma \in G} \lambda_\sigma \sigma(t)\sigma(a) = 0, \ \forall a \in L.$$

Restando t veces la primera identidad de la segunda, se tiene

$$\sum_{\sigma \in G} \lambda_\sigma \Big(t - \sigma(t)\Big)\sigma(a) = 0, \ \forall a \in L.$$

Esto dá una nueva solución no trivial con un número menor de coeficientes no nulos contradiciendo la elección de la solución inicial. □

Este resultado se puede interpretar como la independencia lineal de los automorfismos con respecto a L.

Corolario 20.16.1. *ea L/K una extensión Galoisiana. Sea $a_1, \ldots, a_n$ una K-base de L y sea* $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. *Entonces la matriz*

$$\begin{pmatrix} \sigma_1(a_1) & \sigma_1(a_2) & \sigma_1(a_3) & \cdots & \sigma_1(a_n) \\ \sigma_2(a_1) & \sigma_2(a_2) & \sigma_2(a_3) & \cdots & \sigma_2(a_n) \\ \sigma_3(a_1) & \sigma_3(a_2) & \sigma_3(a_3) & \cdots & \sigma_3(a_n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n(a_1) & \sigma_n(a_2) & \sigma_n(a_3) & \cdots & \sigma_n(a_n) \end{pmatrix}.$$

es invertible. □

El siguiente resultado nos dice que los automorfismos son mucho más que linealmente independientes. Antes de probarlo necesitamos cierta preparación sobre cuerpos de funciones racionales.

Lema 20.17. *Sea L/K una extensión finita. Sean*

$$L' = L(x_1, ..., x_n), \qquad K' = K(x_1, ..., x_n),$$

los cuerpos de funciones racionales respectivos. Entonces

$$[L : K] = [L' : K'].$$

Demostración Podemos suponer primero que $L = K[\alpha]$ ya que el caso general sigue de este por la multiplicatividad del grado. Basta ver que el polinomio irreducible $m_{\alpha,K}(T)$ es irreducible en el anillo $K'[T]$. De hecho basta ver que es irreducible en el anillo de polinomios $K[x_1, \ldots, x_n, T]$ y aplicar el Lemma de Gauss. Esta ultima afirmación sigue de que siendo $m_{\alpha,K}(T)$ un polinomio de grado 0 en cada variable x_i, lo mismo se aplica a cada uno de sus factores. □

Si L/K es Galoisiana. Su grupo de Galois $G = \mathrm{Gal}(L/K)$ actúa en el cuerpo $L' = L(x_1, ..., x_n)$ como sigue:

1. Si
$$p(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x^{i_1} \cdots x_n^{i_n}$$
es un polinomio, entonces
$$\sigma[p(x)] = \sum_{i_1,\ldots,i_n} \sigma(a_{i_1,\ldots,i_n}) x^{i_1} \cdots x_n^{i_n}.$$

2. Si $f = \frac{p}{q}$ es una fracción racional, definimos $\sigma f = \frac{\sigma(p)}{\sigma(q)}$.

Nótese que dado que $[L : K] = [L' : K']$, esta acción define un isomorfismo entre los grupos de Galois de las extensiones L/K y L'/K'.

El siguiente resultado refina lo anterior. No lo usaremos aqu pero lo incluimos por completitud.

Lema 20.18. *Sea L/K una extensión finita. Si $S = \{s_1, \ldots, s_d\}$ es base de L/K entonces S es también base de L'/K'.*

Demostración Basta ver que los elementos de S son linealmente independientes. Supongamos que

$$\sum_{i=1}^{d} h_i(x_1, \ldots, x_n)s_i = 0, \qquad h_i \in L'. \tag{20.1}$$

Multiplicando por el denominador común puede suponerse que cada h_i es un polinomio y no todos son nulos. Supongamos por fijar ideas que h_1 no es el polinomio 0. Consideremos dos casos:

1. Si K es un cuerpo infinito se sigue del Lemma 20.6 que existe $a = (a_1, \ldots, a_n) \in K^n$ tal que $h_1(a) \neq 0$. Por lo que los elementos de S son linealmente dependientes sobre K.

2. Si K es un cuerpo finito, entonces elevando la identidad (20.1) a potencias sucesivas de q se tiene

$$\sum_{i=1}^{d} h_i^{q^r}(x_1, \ldots, x_n)s_i^{q^r} = 0.$$

Como cada elemento de K es invariante por el automorfismo $u \mapsto u^{q^r}$, se tiene

$$\sum_{i=1}^{d} h_i(x_1^{q^r}, \ldots, x_n^{q^r})s_i^{q^r} = 0.$$

Esta última expresión puede evaluarse en $x_1^{1/q^r}, \ldots, x_n^{1/q^r} \in \overline{K'}$ para obtener

$$\sum_{i=1}^{d} h_i(x_1, \ldots, x_n)s_i^{q^r} = 0,$$

y esto implica que los elementos de S son linealmente dependientes sobre $\mathbb{F}_q$ por el ejercicio (Kuotar).

□

Corolario 20.18.1. *Sea L/K una extensión finita. Si $f \in L[x_1, \ldots, x_n]$ es un polinomio que se anula en cada elemento de K^n entonces f es el polinomio* 0.

Demostración Basta escribir $f = \sum_{i=1}^{d} f_i s_i$ donde cada f_i es un polinomio con coeficientes en K. Si f se anula en K^n lo mismo sucede con cada polinomio f_i y utilizamos el Lemma 20.6. □

Si $\{a_1, \ldots, a_n\}$ es una base de L/K, el elemento $x = \sum_{i=1}^{n} x_i a_i$ se dice un elemento genérico de L. Depende por cierto de la elección de una base.

Proposición 20.19. *Sea L/K una extensión Galoisiana con grupo de Galois $G = \{\sigma_1, \ldots, \sigma_n\}$. Sea $f(x_1, \ldots, x_n) \in L[x_1, \ldots, x_n]$ un polinomio en n variables tal que $f\Big(\sigma_1(a), \ldots, \sigma_n(a)\Big) = 0$ para todo elemento a en L. Entonces $f = 0$.*

Demostración Sea $g(x_1, \ldots, x_n) = f\Big(\sigma_1(x), \ldots, \sigma_n(x)\Big)$, where $x = \sum_{i=1}^{n} x_i a_i$ es un elemento genérico de L. Como g se anula en cada elemento de K^n se sigue que g debe ser el polinomio 0. Se concluye que g se anula también en cada elemento de L. Como para cada $u_1, \ldots, u_n \in L$, existen $v_1, \ldots, v_n \in L$ tales que $u_j = \sum_{i=1}^{n} v_i \sigma_j(a_i)$ por el corolario 20.16.1, se tiene que $f(u_1, \ldots, u_n) = g(v_1, \ldots, v_n) = 0$. Como $u_1, \ldots, u_n \in L$ son arbitrarios, se tiene $f = 0$. □

Normas y trazas

Si la extensión L/K es finita y $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$ son todas las incrustaciones de L en la clausura algebraica de K, la traza y la norma definida en el capítulo 6 puede definirse mediante las incrustaciones σ_i de acuerdo al siguiente resultado.

Proposición 20.20. *Para toda extensión finita L/K, se tiene*

$$\mathrm{Tr}_{L/K}(a) = t \sum_{i=1}^{n} \sigma_i(a), \qquad N_{L/K}(a) = \left(\prod_{i=1}^{n} \sigma_i(a) \right)^t,$$

donde $t = [L : L_{\mathrm{Sep}}]$ es el grado de inseparabilidad de L/K.

Demostración Supongamos primero que $L = K[a]$. Basta ver que si

$$m_{K,a}(X) = X^N + a_{N-1}X^{N-1} + \ldots + a_1X + a_0$$

es el polinomio irreducible de a entonces

$$N_{L/K}(a) = (-1)^N a_0, \qquad \mathrm{Tr}_{L/K}(a) = -a_{N-1}.$$

En el caso general, el resultado sigue de

$$\mathrm{Tr}_{L/K}(a) = \Big[L : K[a]\Big]\mathrm{Tr}_{K[a]/K}(a),$$

dado que $\Big[L : K[a]\Big]$ es también el producto entre el grado de inseparabilidad de $L/K[a]$ y el número de incrustaciones σ_i con la misma restricción a $K[a]$. □

Proposición 20.21. *Si $K \subseteq L \subseteq E$ con E/K separable y finita, se tiene*

$$\mathrm{Tr}_{E/K}(a) = \mathrm{Tr}_{L/K}[\mathrm{Tr}_{E/L}(a)], \qquad N_{E/K}(a) = N_{L/K}[N_{E/L}(a)].$$

Demostración Sean $\sigma_1, \ldots, \sigma_n$ las incrustaciones distintas de L en $\overline{K}$. Identificamos L con $\sigma_1(L)$. Recordemos que cada incrustación σ_i de L en $\overline{K}$ tiene m extensiones $\sigma_{i,1}, \ldots, \sigma_{i,m}$ a E, donde m es el grado separable de E/L. Identificamos también E con $\sigma_{1,1}(E)$. Se sigue que

$$N_{E/K}(a) = \left(\prod_{i=1}^{n}\prod_{j=1}^{m}\sigma_{i,j}(a)\right)^t,$$

donde t es el grado inseparable de E/K. De hecho $t = sr$ donde s es el grado inseparable de E/L y r el de L/K, Luego lo anterior es igual a

$$\left(\prod_{i=1}^{n}\left(\prod_{j=1}^{m}\sigma_{i,j}(a)\right)^r\right)^s.$$

Denotemos por

$$b_{i,j} = N_{\sigma_{i,j}(E)/\sigma_{i,j}(L)}\Big(\sigma_{i,j}(a)\Big) \in \sigma_{i,j}(L) = \sigma_i(L).$$

Entonces basta observar que

$$b_{i,j} = \left(\prod_{j=1}^{m} \sigma_{i,j}(a) \right)^r,$$

ya que los homomorfismos $\sigma_{i,j}$ son todas las extensiones de σ_i a E. De este modo $b_i = b_{i,j}$ no depende de j. Afirmamos ahora que si $b = b_1 \in L$, entonces $b_i = \sigma_i(b)$ para todo i. Se sigue que $N_{L/K}(b) = N_{E/K}(a)$, lo que concluye la demostración.

Para probar la afirmación, tomamos el polinomio irreducible

$$p_i(X) = X^u + c_{i,u-1}X^{u-1} + \ldots + c_{i,1}X + c_{i,0}$$

de $\sigma_{i,j}(a)$ para algún (todo) j, y observamos que

$$b_i = (-1)^u c_{i,0} = \sigma_i\Big((-1)^u c_{1,0}\Big) = \sigma_i(b_1).$$

La demostración para las trazas es análoga. □

La teoría desarrollada hasta aqui nos permite dar la siguiente caracterización de las extensiones separables.

Proposición 20.22. *Una extensión finita L/K es separable si y sólo si existe $\alpha \in L$ tal que $\mathrm{Tr}_{L/K}(\alpha) \neq 0$.*

Demostración Si L/K es inseparable, basta tomar $\alpha \notin L_{\mathrm{Sep}}$ y se tiene que

$$\mathrm{Tr}_{L/L_{\mathrm{Sep}}}(\alpha) = 0,$$

ya que el polinomio irreducible de α sobre L_{Sep} tiene una única raiz y su multiplicidad es necesariamente una potencia de p. Se sigue que

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{L_{\mathrm{Sep}}/K}(0) = 0.$$

Supongamos ahora que L/K es separable. Si L/K es una extensión Galoisiana y si $\mathrm{Tr}_{L/K}(\alpha) = 0$ para todo $\alpha \in L$, se tiene

$$\sigma_1(\alpha) + \cdots + \sigma_n(\alpha) = 0 \qquad \forall \alpha \in L,$$

lo que contradice la proposición 20.16. En el caso general, sea E la clausura Galoisiana de L/K. ciertamente existe un elemento $\alpha \in E$ tal que $\mathrm{Tr}_{E/K}(a) \neq 0$ por lo que el elemento $b = \mathrm{Tr}_{E/L}(a)$ satisface $\mathrm{Tr}_{L/K}(b) \neq 0$. □

Ejercicios

Chapter 21

Ecuaciones resolubles por radicales

Se sabe que si λ es una raiz de la ecuación $x^2 + ax + b = 0$, en un cuerpo de característica distinta de 2, entonces se tiene $\lambda = \frac{1}{2}(-a \pm \sqrt{a^2 - 4b})$ y que si μ es una raiz de la ecuación $x^3 + ax + b = 0$, en un cuerpo de característica distinta de 2 y 3, entonces

$$\mu = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}},$$

para una elección apropiada de las raices cúbicas. Estos son casos particulares de un proceso mas general denominado resolución de ecuaciones por radicales. Un radical es para nosotros una expresión del tipo $\sqrt[n]{a}$ o $\wp^{-1}(a)$ donde $\wp(a) = a^p - a$ (si la característica del cuerpo es p). La consideración de este último caso se justifica porque, como veremos, estos son los dos tipos básicos de extensiones cíclicas. Para fijar ideas consideremos la siguiente definición:

definición 21.1. Sea L/K una extensión algebraica. Un elemento a de L se dice expresable por radicales sobre K si existe una una cadena de extensiones $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_n = L$ tal que $L_{i+1} = L_i(\sqrt[n]{a})$ con $a \in L_i$ o bien $L_{i+1} = L_i(\wp^{-1}a)$ con $a \in L_i$. Una ecuacin $f(x) = 0$, donde $f(x) \in K[x]$ se dice resoluble por radicales si cada una de sus raices es expresable por radicales. Si $f(x)$ es irreducible en $K[x]$ y si una de sus raices es expresable por radicales entonces $f(x)$ es resoluble por radicales ya que el grupo de Galois del cuerpo de descomposición de f sobre K acta transitivamente en las raices de f.

Las extensiones de la forma $K(\sqrt[n]{a})/K$ se conocen como extensiones de Kummer, y las extensiones de la forma $K(\wp^{-1}a)/K$ se conocen como extensiones de Artin-Schreier.

Extensiones de Artin Schreier

Observemos primero que el polinomio $\wp$ es aditivo es decir

$$\wp(a+b) = (a+b)^p - (a+b) = (a^p - a) + (b^p - b) = \wp(a) + \wp(b).$$

Por otro lado, las raices de $\wp(x) = 0$ son los elementos del cuerpo primo $\mathbb{F}_p$. Se concluye que si α es una raiz de $\wp(x) = a$, las restantes raices son $\alpha + 1, \ldots, \alpha + (p-1)$. En particular, toda extensión de Artin-Schreier es separable, normal, y por lo tanto Galoisiana. Además si $\alpha \notin K$ entonces un elemento no trivial σ de $\mathrm{Gal}(K(\alpha)/K)$ debe satisfacer $\sigma(\alpha) = \alpha + t$ con $t \in \mathbb{F}_p^*$, por lo que tiene orden p. Se concluye que $\mathrm{Gal}(K(\alpha)/K)$ es un grupo cíclico de orden p. En particular $\wp(x) - a$ es irreducible.

Ejemplo 21.2. Sea $K = \mathbb{F}_2$ y sea $L = \mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ entonces $\alpha^2 = \alpha + 1$ por lo que $\mathrm{irr}_K(\alpha, x) = \wp(x) - 1$. Se sigue que $\mathbb{F}_4/\mathbb{F}_2$ es una extensión de Artin-Schreier.

Extensiones de Kummer

Supondremos ahora que K contiene el conjunto μ_n de raices n-ésimas de la unidad. Bajo esta condición, si α es una raiz del polinomio $x^n - a$ entonces las restantes raices son $\rho\alpha, \ldots, \rho^{n-1}\alpha$. Se concluye que toda extensión de Kummer sobre un cuerpo que contiene a las raices n-ésimas de la unidad es Galoisiana. Además todo elemento no trivial σ de $\mathrm{Gal}(K(\alpha)/K)$ debe satisfacer $\sigma(\alpha) = \rho^{\Gamma(\sigma)}\alpha$ para algún $\Gamma(\sigma) \in \mathbb{Z}$. Como $\rho^n = 1$, podemos ver a $\Gamma(\sigma)$ como un elemento de $\mathbb{Z}/n\mathbb{Z}$. La correspondencia $\sigma \mapsto \Gamma(\sigma)$ define un homomorfismo inyectivo de grupos $\Gamma : \mathrm{Gal}(K(\alpha)/K) \to \mathbb{Z}/n\mathbb{Z}$ que recibe el nombre de Homomorfismo de Kummer. En particular se sigue que $\mathrm{Gal}(K(\alpha)/K)$ es un grupo cíclico cuyo orden divide a n. Además, se tiene que si $[K[\alpha] : K] = n/t$, entonces un generador σ de $\mathrm{Gal}(K(\alpha)/K)$ satisface $\sigma(\alpha) = \rho^{st}\alpha$ para algún entero s relativamente primo con n/t, en particular $\sigma(\alpha^{n/t}) = \alpha^{n/t}$ por lo que $\alpha^{n/t} \in K$.

Extensiones Ciclotómicas

Sea ahora K un cuerpo cuya característica sea relativamente prima con n y sea $\rho \in \overline{K}$ una raiz n-ésima primitiva de la unidad (es decir que su orden es exactamente n). En particular, ρ es raiz del polinomio $x^n - 1 \in K[x]$. Las restantes raices de este polinomio son $\rho^2, \rho^3, \ldots, \rho^{n-1}, \rho^n = 1$. Se deduce que la extensión $K(\rho)/K$ es Galoisiana. Además todo elemento no trivial σ de $\mathrm{Gal}(K(\rho)/K)$ debe satisfacer $\sigma(\rho) = \rho^{\Delta(\sigma)}$ para algún $\Delta(\sigma) \in \mathbb{Z}/n\mathbb{Z}$. Como ρ es de hecho un generador del grupo μ_n de raices de la unidad, se tiene que $\Delta(\sigma)$ debe ser relativamente primo con n. La correspondencia $\sigma \mapsto \Delta(\sigma)$ define un homomorfismo inyectivo de grupos $\Gamma : \mathrm{Gal}(K(\rho)/K) \to (\mathbb{Z}/n\mathbb{Z})^*$, ya que

$$\rho^{\Delta(\sigma\tau)} = \sigma \circ \tau(\rho) = \sigma\Big(\tau(\rho)\Big) = \sigma(\rho^{\Delta(\tau)}) = (\rho^{\Delta(\sigma)})^{\Delta(\tau)} = \rho^{\Delta(\sigma)\Delta(\tau)}.$$

Se concluye que $\mathrm{Gal}(K(\rho)/K)$ es un grupo abeliano.

Irreducibilidad de la ecuación de quinto grado

Con lo anterior podemos demostrar el siguiente resultado:

Proposición 21.3. *Si $f(x) = 0$ es soluble por radicales para un polinomio $f(x) \in K[x]$, y si L es el cuerpo de descomposición de f sobre K entonces* $\mathrm{Gal}(L/K)$ *es Soluble.*

Demostración Basta con demostrar que existe una extensión Galoisiana E/K tal que $L \subseteq E$ y tal que $\mathrm{Gal}(E/K)$ sea soluble. Sea $[L : K] = n$, sea m el producto de los primos que dividen a n y no son la característica de K, y sea ρ una raiz m-ésima primitiva de la unidad. Entonces $K[\rho]/K$ es una extesión ciclotómica y por lo tanto es Galoisiana con grupo de Galois abeliano. Además, si E/K es Galoisiana y finita, digamos $E = K[\alpha_1, \ldots, \alpha_n]$, entonces $E[\rho] = K[\rho, \alpha_1, \ldots, \alpha_n]$ es tambien Galoisiano sobre K. Se concluye que para toda extensión Galoisiana E/K el grupo $\mathrm{Gal}(E[\rho]/K[\rho])$ es normal en $\mathrm{Gal}(E[\rho]/K)$ y su cociente es abeliano, de donde $\mathrm{Gal}(E[\rho]/K)$ es soluble si y sólo si $\mathrm{Gal}(E[\rho]/K[\rho])$ es soluble. Por otro lado

$$\mathrm{Gal}(E/K) = \phi[\mathrm{Gal}(E[\rho]/K)],$$

donde ϕ denota la restricción de $E[\rho]$ a E. Luego si $\mathrm{Gal}(E[\rho]/K)$ es soluble también lo es $\mathrm{Gal}(E/K)$. En particular, podemos suponer que K contiene las raices m-ésimas de la unidad. Supondremos esto en todo lo que sigue.

Sea E el cuerpo de descomposición de f sobre K. Por definición de *soluble por radicales* existe una cadena de subcuerpos $K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n$ con $E \subseteq L_n$ y tal que L_{i+1}/L_i es una extensión de Kummer o de Artin-Schreier para cada i, de modo que el grupo $\mathrm{Gal}(L_{i+1}/L_i)$ es abeliano. Sea $E_i = L_i \cap E$. Entonces $\mathrm{Gal}(E_{i+1}/E_i) = \phi_i[\mathrm{Gal}(L_{i+1}/L_i)]$, donde ϕ_i es la restricción de L_{i+1} a E_{i+1}, es también abeliano. Sea $G_i = \mathrm{Gal}(E/E_i)$. Entonces G_{i+1} es normal en G_i para cada i y $G_i/G_{i+1} = \mathrm{Gal}(E_{i+1}/E_i)$ es abeliano, de donde $\mathrm{Gal}(E/K)$ es soluble. □

Proposición 21.4. *Existen ecuaciones de quinto grado que no son solubles por radicales.*

Demostración Basta con encontrar una ecuación de quinto grado cuyo grupo de Galois sea S_5 y por lo tanto no soluble. Si $\sigma_1, \ldots, \sigma_5$ son las funciones simétricas elementales en las variables $x_1, \ldots, x_5$, de modo que

$$\begin{aligned} f(T) &= (T - x_1)(T - x_2)(T - x_3)(T - x_4)(T - x_5) \\ &= T^5 - \sigma_1 T^4 + \sigma_2 T^3 - \sigma_3 T^2 + \sigma_4 T - \sigma_5, \end{aligned}$$

el cuerpo $K(x_1, \ldots, x_5)$ es el cuerpo de descomposición sobre $K(\sigma_1, \ldots, \sigma_5)$ de $f(T)$ y su grupo de Galois es S_5. □

La existencia de este tipo de extensiones demuestra que es imposible escribir una fórmula para las soluciones de una ecuación de quinto grado similar a las mencionadas al comienzo de este capítulo, ya que de haberla debería ser aplicable en este caso. Mas adelante veremos que la existencia de soluciones implica en particular la existencia de formulas. Sin embargo, sería concebible que aún sin una fórmula general se pudiese resolver individualmente cada ecuación con coeficientes racionales. De hecho esto tampoco es posible como lo demuestra el siguiente resultado.

Proposición 21.5. *Existen ecuaciones de quinto grado sobre los racionales que no son solubles por radicales.*

Demostración Sea $f(x)$ un polinomio irreducible en $\mathbb{Q}[x]$ con exactamente tres raices reales α_1, α_2, y α_3. Entonces las raices complejas α_4 y α_5 deben ser conjugadas. En particular, Si K es el cuerpo de descomposición de f sobre $\mathbb{Q}$, la conjugación compleja es un elemento del grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$ que corresponde a la trasposición (45). Como $\mathbb{Q}[\alpha_i]/\mathbb{Q}$ tiene grado 5 para cada i se concluye que $[K : \mathbb{Q}]$ es divisible por 5, de donde

$\mathrm{Gal}(K/\mathbb{Q})$ debe contener un elemento ρ de orden 5. Remplazando ρ por una potencia si es necesario podemos suponer que $\rho(\alpha_4) = \alpha_5$, y reenumerando α_1, α_2, y α_3, podemos suponer que ρ corresponde al ciclo (12345). Se concluye que $\mathrm{Gal}(K/\mathbb{Q})$ contiene homomorfismos correspondientes a las transposiciones (45), $(34) = (12345)^{-1}(45)(12345)$, $(23) = (12345)^{-2}(45)(12345)^2$, y $(12) = (12345)^{-3}(45)(12345)^3$, las que claramente general S_5. Para concluir la demostración basta con exhibir un polinomio con dichas propiedades.

Sea

$$f(x) = x(x-2)(x+2)(x-8) = x^4 - 8x^3 - 4x^2 + 32x.$$

este polinomio es la derivada de $g(x) = \frac{1}{5}x^5 - 2x^4 - \frac{4}{3}x^3 + 16x^2 + \lambda$ para una constante λ arbitraria. Observese que

$$g(0) = \lambda,\ g(2) = \frac{13}{15}2^5 + \lambda,\ g(-2) = \frac{17}{15}2^5 + \lambda,\ g(8) = -\frac{38}{15}8^3 + \lambda < \lambda.$$

En particular, si

$$-\lambda \in \left[\frac{13}{15}2^5, \frac{17}{15}2^5\right],$$

entonces g tiene exactamente tres raices reales. Por otro lado si λ es un racional de la forma $\frac{2r}{q}$ con r y q impares, entonces f es irreducible por el criterio de Eisenstein (aplicado en el anillo $\mathbb{Z}_{(2)} = \{\frac{a}{b} \in \mathbb{Q} | b \notin 2\mathbb{Z}\}$). Como el conjunto de todos los números racionales de la forma $\frac{2r}{q}$ con q y r impares es denso en $\mathbb{R}$, esto concluye la demostración. □

El teorema 90 de Hilbert

Proposición 21.6. *Sea L/K una extensión Galoisiana. Sea $\sigma \mapsto a_\sigma$ una función que asigna un elemento de L^* a cada automorfismo σ en $\mathrm{Gal}(L/K)$ y satisface $a_{\sigma\tau} = a_\sigma \sigma(a_\tau)$. Entonces existe $b \in L$ tal que $a_\sigma = b/\sigma(b)$ para todo σ en $\mathrm{Gal}(L/K)$.*

Demostración Por la independencia lineal de los automorfismos, existe $c \in L$ tal que

$$b = \sum_{\sigma \in G} a_\sigma \sigma(c) \neq 0.$$

Además se tiene

$$\rho(b) = \sum_{\sigma \in G} \rho(a_\sigma)\rho\sigma(c) = a_\rho^{-1} \sum_{\sigma \in G} a_{\rho\sigma}\rho\sigma(c) = a_\rho^{-1} b,$$

de donde se sigue lo pedido. □

La forma más conocida de la proposición anterior es el caso de una extensi'on Galoisiana L/K con grupo de Galois $\mathrm{Gal}(L/K)$ cíclico. Una tal extensión recibe el nombre de extensión cíclica.

Proposición 21.7. *Sea L/K una extensi'on cíclica. Sea σ un generador del grupo de Galois. Si $a \in L$ satisface $\prod_{\sigma\in G}\sigma(a) = 1$, entonces existe $b \in L^*$ con $b/\sigma(b) = a$.*

Demostración Basta aplicar el resultado anterior con $a_{\sigma^r} = \prod_{i=0}^{r-1}\sigma^i(a)$. Puesto que está bien definido, ya que

$$a_{\sigma^{r+n}} = a_r \prod_{i=r}^{r+n-1}\sigma^i(a) = a_r,$$

y se tiene

$$a_{\sigma^r}\sigma^r(a_{\sigma^s}) = \prod_{i=0}^{r-1}\sigma^i(a)\sigma^r\left(\prod_{i=0}^{s-1}\sigma^i(a)\right) = \prod_{i=0}^{r+s-1}\sigma^i(a) = a_{\sigma^{r+s}}.$$

□

Proposición 21.8. *Sea L/K una extensión cíclica de grado primo q, donde q no coincide con la característica de K. Suponga que K contiene las raices n-ésimas de 1. Entonces existe un elemento $a \in K$ tal que $L = K[\sqrt[q]{a}]$. En particular, L/K es una extensión de Kummer.*

Demostración Basta aplicar el resultado anterior a una raiz q-ésima primitiva ρ_0, ya que $\prod_\sigma \sigma(\rho_0) = \rho_0^q = 1$. Se tiene que, para cualquier generador σ de grupo de Galois, existe un elemento no nulo b tal que $\sigma(b) = \rho_0 b$. Se sigue que $\sigma(b^q) = \rho_0^q b^q = b^q$, de donde $a = b^q \in K$. □

El teorema 90 de Hilbert tiene un equivalente aditivo:

Proposición 21.9. *Sea L/K una extensión Galoisiana. Sea $\sigma \mapsto a_\sigma$ una función que asigna un elemento de L a cada automorfismo σ en $\mathrm{Gal}(L/K)$ y satisface $a_{\sigma\tau} = a_\sigma + \sigma(a_\tau)$. Entonces existe $b \in L$ tal que $a_\sigma = b - \sigma(b)$ para todo σ en $\mathrm{Gal}(L/K)$.*

Demostración Por la independencia lineal de los automorfismos, existe $c' \in L$ tal que

$$t = \sum_{\sigma \in G} \sigma(c') \neq 0.$$

Nótese que $\sigma(t) = t$ para todo $\sigma \in \mathrm{Gal}(L/K)$. Si definimos $c = c'/t$ se tiene que

$$\sum_{\sigma \in G} \sigma(c) = 1.$$

Luego, si definimos

$$b = \sum_{\sigma \in G} a_\sigma \sigma(c),$$

se tiene que

$$\rho(b) = \sum_{\sigma \in G} \rho(a_\sigma)\rho\sigma(c) = \sum_{\sigma \in G} (a_{\rho\sigma} - a_\rho)\rho\sigma(c) = b - a_\rho \sum_{\sigma \in G} \sigma(c) = b - a_\rho,$$

de donde se sigue lo pedido. □

Como antes, esto adquiere una forma mas simple en el caso de una extensión cíclica.

Proposición 21.10. *Sea L/K una extensi'on cíclica. Sea σ un generador del grupo de Galois. Si $a \in L$ satisface $\sum_{\sigma \in G} \sigma(a) = 0$, entonces existe $b \in L^*$ con $b - \sigma(b) = a$.*

Demostración Basta aplicar el resultado anterior con $a_{\sigma^r} = \sum_{i=0}^{r-1} \sigma^i(a)$. Puesto que está bien definido, ya que

$$a_{\sigma^{r+n}} = a_r + \sum_{i=r}^{r+n-1} \sigma^i(a) = a_r,$$

y se tiene

$$a_{\sigma^r} + \sigma^r(a_{\sigma^s}) = \sum_{i=0}^{r-1} \sigma^i(a) + \sigma^r \left(\sum_{i=0}^{s-1} \sigma^i(a) \right) = \sum_{i=0}^{r+s-1} \sigma^i(a) = a_{\sigma^{r+s}}.$$

□

Proposición 21.11. *Sea L/K una extensión cíclica de grado primo p, donde p es la característica de K. Entonces existe un elemento $a \in K$ tal que $L = K[\wp^{-1}(a)]$, donde $\wp(x) = x^p - x$. En particular, L/K es una extensión de Artin-Schreier.*

Demostración Basta aplicar el resultado anterior a $a = 1$. Se tiene que, para cualquier generador σ de grupo de Galois, existe un elemento no nulo b tal que $\sigma(b) = b+1$. Se sigue que $\sigma(b^p - b) = (b+1)^p - (b+1) = b^p - b$, de donde $a = \wp(b) \in K$. □

Ahora estamos listos para probar el teorema principal de este capítulo:

Proposición 21.12. *Sea $f(x) \in K[x]$ un polinomio con raices distintas, y sea L su cuerpo de descomposición sobre K. La ecuación $f(x) = 0$ es soluble por radicales si y sólo si el grupo* $\mathrm{Gal}(L/K)$ *es soluble.*

Demostración Supongamos primero que $\mathrm{Gal}(L/K)$ es soluble. Sea $n = [L : K]$, sea m el producto de los primos que dividen a n y que difieren de la característica de K, y sea ρ una raiz m-ésima primitiva de 1. Sea $F = K[\rho]$ y $E = L[\rho]$. Nótese que $L = K[\alpha_1, \ldots, \alpha_r]$, donde $\alpha_1, \ldots, \alpha_r$ son las raices de $f(x) = 0$. Entonces $E = [\rho, \alpha_1, \ldots, \alpha_r]$, de donde se sigue que E/K es Galoisiana. Nótese que existe un homomorfismo

$$\phi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(L/K),$$

donde $\phi(\sigma)$ es la restricción de σ a L. Como $E = F[\alpha_1, \ldots, \alpha_r]$ cada F-automorfismo σ de E que es la identidad en L debe fijar a cada α_i y es por lo tanto la identidad en L. Se concluye que ϕ es inyectiva y por lo tanto $G = \mathrm{Gal}(E/F)$ es soluble. En particular, existen subgrupos $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_N = \{\mathrm{Id}\}$, tales que G_{i+1} es normal en G_i y G_i/G_{i+1} es cíclico de order primo para cada $i = 0, \ldots, N-1$. Si $E_i = E^{G_i}$ entonces E_{i+1}/E_i es una extensión de Kummer o de Artin-Schreier por los resultados precedentes, de donde se concluye que $f(x) = 0$ es soluble por radicales sobre F. Como $F = K[\rho]$ se obtiene de K agregando una raiz (de 1), se tiene que $f(x) = 0$ es soluble por radicales sobre K. La conversa es proposición 21.3. □

Corolario 21.12.1. *La ecuación general de grado n es soluble sí y sólo si $n \leq 4$.*

Ejercicios

Chapter 22

Dependencia Algebraica

En este capítulo regresamos nuestro interés a las extensiones trascendentes. Recuerdese que un elemento α en una extensión L de K es trascendente si α no satisface ninguna ecuación con coeficientes en K, o equivalentemente, si el anillo $K[\alpha]$ es isomorfo al anillo $K[x]$ de polinomios en la variable x con coeficientes en K. En este caso el cuerpo $K(\alpha)$ generado por α sobre K es isomorfo al cuerpo $K(x)$ de funciones racionales con coeficientes en K. Definiremos un concepto análogo para n elementos $\alpha_1, \ldots, \alpha_n$ en L.

definición 22.1. Diremos que el conjunto $\{\alpha_1, \ldots, \alpha_n\}$ es algebraicamente dependiente sobre K si existe un polinomio $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ tal que $f(\alpha_1, \ldots, \alpha_n) = 0$. En caso contrario diremos que $\{\alpha_1, \ldots, \alpha_n\}$ es algebraicamente independiente. Nótese que $\{\alpha_1, \ldots, \alpha_n\}$ es algebraicamente independiente sobre K sí y sólo si el anillo $K[\alpha_1, \ldots, \alpha_n]$ es isomorfo al anillo de polinomios $K[x_1, \ldots, x_n]$. En este caso el cuerpo $K(\alpha_1, \ldots, \alpha_n)$ generado por $\alpha_1, \ldots, \alpha_n$ es isomorfo al cuerpo de funciones racionales $K(x_1, \ldots, x_n)$. Mas generalmente, diremos que un conjunto B de L es algebraicamente independiente si todo subconjunto finito de B lo es.

definición 22.2. Sea L/K una extensión arbitraria. Diremos que el conjunto $B \subseteq L$ genera algebraicamente L sobre K si todo elemento de L es algebraico sobre el cuerpo $K(B) = \mathfrak{Quot}(K[B])$. Una base de trascendencia de L/K es un conjunto algebraicamente independiente que genera algebraicamente L sobre K.

Los conjuntos algebraicamente independientes y las bases de trascendencia tienen propiedades análogas a las de los conjuntos linealmente independientes y las bases de un espacio vectorial.

Lema 22.3. *Sea $\{\alpha_1, \ldots, \alpha_n\} \subseteq L$ un conjunto algebraicamente independiente sobre K. Un elemento $\beta \in L$ es algebraico sobre $K(\alpha_1, \ldots, \alpha_n)$ sý sólo si $\{\alpha_1, \ldots, \alpha_n, \beta\}$ es algebraicamente dependiente.*

Demostración Si β es algebraico sobre $E = K(\alpha_1, \ldots, \alpha_n)$ entonces $h(y) = \mathrm{irr}_E(\beta, y)$ es un polinomio con coeficientes en E. Podemos escribir $h(y) = \nu f(y, \alpha_1, \ldots, \alpha_n)$ donde $f(y, \alpha_1, \ldots, \alpha_n)$ es un polinomio primitivo en

$$K[\alpha_1, \ldots, \alpha_n][y] \cong K[x_1, \ldots, x_n, y],$$

por lo que la imagen $f(y, x_1, \ldots, x_n)$ de $f(y, \alpha_1, \ldots, \alpha_n)$ en el anillo $K[x_1, \ldots, x_n, y]$ es no trivial y se anula en $(\alpha_1, \ldots, \alpha_n, \beta)$. Por otro lado, si un polinomio $f(y, x_1, \ldots, x_n)$ se anula en $(\alpha_1, \ldots, \alpha_n, \beta)$, entonces f necesariamente depende de y ya que $\{\alpha_1, \ldots, \alpha_n\}$ es algebraicamente independiente. Se sigue que si

$$f(y, x_1, \ldots, x_n) = \sum_{r=0}^{N} g_r(x_1, \ldots, x_n) y^r,$$

entonces

$$f(y, \alpha_1, \ldots, \alpha_n) = \sum_{r=0}^{N} g_r(\alpha_1, \ldots, \alpha_n) y^r,$$

es un polinomio no trivial con coeficientes en E que se anula en β. □

Como

$$K(D) = \bigcup_{\substack{T \subseteq D \\ T \text{ finito}}} K(T),$$

y dado que todo polinomio tiene un número finito de coeficientes se tiene el siguiente resultado:

Lema 22.4. *Todo elemento algebraico sobre $K(B)$ es algebraico sobre el cuerpo $K(\alpha_1, \ldots, \alpha_n)$ para algún subconjunto finito $\{\alpha_1, \ldots, \alpha_n\}$ de D.* □

De ambos lemas se deduce el siguiente resultado:

Proposición 22.5. *Sea $S \subseteq L$ un conjunto algebraicamente independiente sobre K. Un elemento $\beta \in L$ es algebraico sobre $K(S)$ sý sólo si $S \cup \{\beta\}$ es algebraicamente dependiente.*

Proposición 22.6. *Sea L/K una extensión arbitraria. Dados un conjunto $S \subseteq L$ algebraicamente independiente sobre K y un conjunto T que genera algebraicamente L sobre K, tales que $S \subseteq T$, existe una base de trascendencia B que satisface $S \subseteq B \subseteq L$.*

Demostración Es una aplicación directa del lema de Zorn que existe un conjunto B algebraicamente independiente maximal tal que $S \subseteq B \subseteq L$. Se sigue del lema previo que eso implica que B es base de trascendencia. □

Lema 22.7. *Si B y S son algebraicamente independientes y si $\beta \in S$ es algebraico sobre $K(B)$ pero trascendente sobre K, entonces existe $\alpha \in B - S$ tal que $(B - \{\alpha\}) \cup \{\beta\}$ es algebraicamente independiente.*

Demostración Como β es algebraico sobre $K(B)$, se tiene que existen $\alpha_1, \ldots, \alpha_n \in B$ tales que β es algebraico sobre $E = K(\alpha_1, \ldots, \alpha_n)$. Sea $f(x_1, \ldots, x_n, y) \in K[x_1, \ldots, x_n][y]$ primitivo y tal que $f(\alpha_1, \ldots, \alpha_n, y) = \nu \cdot \mathrm{irr}_E(y, \beta)$. Entonces f depende de al menos un α_i, y como S es algebraicamente independiente, puede suponerse que $\alpha_i \notin S$. Por otro lado f divide a cualquier otro polinomio que se anula en $(\alpha_1, \ldots, \alpha_n, \beta)$, luego cualquier tal polinomio depende de α_i. Se concluye que $(B - \{\alpha_i\}) \cup \{\beta\}$ es algebraicamente independiente. □

Proposición 22.8. *Sea S un subconjunto de L algebraicamente independiente sobre K y sea B una base de trascendencia de L/K. Entonces $|S| \leq |B|$.*

Demostración Un *remplazo parcial* de S en B es un par (T, ϕ) tal que $T \subseteq S$ y $\phi : T \to B$ es una función inyectiva, tal que $\Big(B - \phi(T)\Big) \cup T$ es algebraicamente independiente. Diremos que $(T, \phi) \leq (T', \phi')$ para dos remplazos parciales (T, ϕ) y (T', ϕ'), si $T \subseteq T'$ y ϕ' es una extensión de ϕ a T'. El conjunto de remplazos parciales está bien ordenado con esta relación y es claro que satisface las hipótesis del lema de Zorn, ya que contiene a $(\emptyset, \phi_\emptyset)$, donde $\phi_\emptyset$ es la unica función de $\emptyset$ en B, y la unión de una cadena de renplazos parciales es un remplazo parcial. El lema anterior prueba que un remplazo parcial maximal es de la forma (S, ϕ), luego existe al menos una función inyectiva de S en B. □

Corolario 22.8.1. *Dos bases de trascendencia cualesquiera de L/K tienen el mismo número de elementos.*

definición 22.9. El número de elementos de una base de trascendencia de L/K recibe el nombre de *Grado de Trascendencia* o bien de *Dimension trascendente* de L/K.

Corolario 22.9.1. *Sea L/K una extensión con grado de trascendencia $n < \infty$. Si $\alpha_1, \ldots, \alpha_n \in L$ son algebraicamente independientes entonces todo elemento de L es algebraico sobre $K(\alpha_1, \ldots, \alpha_n)$ y conversamente.*

Ejercicios

Chapter 23

Anillos Normales y Funciones Simétricas

Sean $A \subseteq B$ anillos conmutativos. Un elemento b de B se dice entero sobre A si b es raiz de un polinomio mónico con ceficientes en A. Si $B \subseteq \mathbb{C}$, un elemento de B entero sobre $\mathbb{Z}$ se llama un entero algebraico. Equivalentemente, b es entero sobre un anillo A si existe un entero n tal que b^n es una combinación lineal de $1, b, \ldots, b^{n-1}$ con coeficientes en A. Mas precisamente, se tiene la siguiente caracterización:

Proposición 23.1. *Sean $A \subseteq B$ anillos conmutativos, y sea b un elemento de B. Las suiguientes afirmaciones son equivalentes:*

1. *b es entero sobre A.*
2. *$A[b]$ es un A-módulo finitamente generado.*
3. *Existe un A-módulo finitamente generado $N \subseteq B$ que contiene a A y tal que $bN \subseteq N$.*

Demostración Si b es entero sobre A se sigue que b^n está en el A-módulo generado por $1, b, b^2, \ldots, b^{n-1}$, digamos $b^n = \sum_{i=0}^{n-1} a_i b^i$ con $a_i \in A$. Se sigue que para todo $k \geq 0$ se tiene $b^{n+k} = \sum_{i=0}^{n-1} a_i b^{i+k}$, de donde por inducción, (1) implica (2). Es trivial que (2) implica (3). Finalmente, supongamos que se cumple (3). Sean $v_1, \ldots, v_n$ generadores de N como A-módulo. Se sigue que para cada $i = 1, \ldots, n$ se tiene $bv_i = \sum_{j=1}^{n} a_{i,j} v_j$. En

particular se tiene la identidad matricial $(bI - M)V = 0$ donde I es la matriz identidad, M es la matriz $(a_{i,j})_{i,j}$ y V es el vector columna

$$V = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Multiplicando por la adjunta clásica $(bI - M)^*$ se tiene $\det(bI - M)V = 0$. En particular, $\det(bI - M)$ anula a cualquier combinación lineal de los v_i's. En particular a todo elemento de N. Como $1 \in A \subseteq N$, se tiene que $\det(bI - M) = 0$ y $\det(xI - M)$ es un polinomio mónico que anula b. □

Si $A \subseteq B$ diremos que B es entero sobre A si cada elemento de B es entero sobre A. Se sigue del resultado anterior que si B es finitamente generado como A-módulo, entonces es entero sobre A. En particular, si b es entero sobre A entonces $A[b]$ es entero sobre A. Mas generalmente se tiene el siguiente resultado.

Proposición 23.2. *Sea $B = A[b_1, \ldots, b_m]$, las siguientes afirmaciones son equivalentes:*

1. *B es entero sobre A.*
2. *Cada b_i es entero sobre A.*
3. *B es finitamente generado como A módulo.*

Demostración Es claro que (1) implica (2) y que (3) implica (1). Probaremos que (2) implica (3). Asumamos que cada b_i es entero sobre A. Se sigue que existe un entero positivo N tal que para todo $n > N$ y para cada $i = 1, \ldots, m$, tenemos una identidad de la forma $b_i^n = \sum_{j=0}^{N} a_{i,j}(n) b_i^j$ con $a_{i,j}(n) \in A$. Multiplicando estas expresiones se tiene que cada producto $b_1^{n_1} \ldots b_m^{n_m}$ es una combinación lineal con coeficientes en A de los productos $b_1^{k_1} \ldots b_m^{k_m}$ con $0 \leq k_i \leq N$, de donde B es finitamente generado como A-módulo. □

Corolario 23.2.1. *Si b_1 y b_2 son enteros sobre A, también lo son $b_1 - b_2$, $b_1 + b_2$, y $b_1 b_2$.*

Demostración Todos ellos son elementos de $A[b_1, b_2]$. □

Corolario 23.2.2. *El conjunto de los elementos de B que son enteros sobre A es un subanillo B^{ent} de B.*

El anillo B^{ent} recibe el nombre de clausura entera de A en B. Si $A = B^{\text{ent}}$ se dice que A es integralmente cerrado en B. Si A es un dominio de integridad se dice que es integralmente cerrado (o normal) si es integralmente cerrado en su cuerpo de cocientes.

Ejemplo 23.3. Sea $A = K[x^2, x^3] \subseteq K[x]$ donde x es trascendente sobre el cuerpo K. Como x es raiz de la ecuación $T^2 - (x^2) = 0$ es entero sobre A. Por otro lado $x = \frac{x^3}{x^2}$, de donde x está en el cuerpo de cocientes de A, por lo que A no es normal.

Ejemplo 23.4. Sea $A = \mathbb{Z}[\sqrt{-3}]$. Como $\omega = \frac{-1+\sqrt{-3}}{2}$ es raiz de la unidad es entero sobre $\mathbb{Z}$ y por lo tanto sobre A y ω está en el cuerpo de cocientes de A pero no en A, por lo que A no es normal.

Proposición 23.5. *Sean $A \subseteq B \subseteq C$ anillos conmutativos. Sea c un elemento de C. Si B es entero sobre A y c es entero sobre B, entonces c es entero sobre A.*

Demostración Como c es entero sobre B, satisface una ecuación $c^n = \sum_{k=0}^{n-1} b_i c^i$. Sea $B' = B[b_0, \ldots, b_{n-1}]$. Se sigue que c es entero sobre B'. En particular cada elemento de $B'[c]$ es de la forma $\sum_{i=0}^{n-1} \beta_i c^i$ con $\beta_i \in B'$. Como B' es finitamente generado como A-módulo tambien lo es

$$B'[c] = B' + cB' + c^2B' + \ldots + c^{n-1}B'.$$

□

Corolario 23.5.1. *Sean $A \subseteq B$ anillos conmutativos. El subanillo B^{ent} de B es integralmente cerrado en B.*

Corolario 23.5.2. *Sea A un dominio de integridad y B su cuerpo de cocientes. El subanillo B^{ent} de B es normal.*

Proposición 23.6. *Todo DFU es normal.*

Demostración Sea D un DFU y sea $\frac{m}{n}$ un elemento de su cuerpo de cocientes que es entero sobre D. Podemos suponer que n y m son relativamente primos. Si n es una unidad, no hay nada que demostrar. De otro modo, sea p un primo que divide a n, y por lo tanto no a m. Si

$$\left(\frac{m}{n}\right)^k = \sum_{i=0}^{k-1} s_i \left(\frac{m}{n}\right)^i,$$

multiplicamos esta identidad por n^k y se tiene

$$m^k = \sum_{i=0}^{k-1} s_i m^i n^{k-i},$$

donde p divide a cada término de la derecha pero no el lado izquierdo. □

Ejemplo 23.7. $\mathbb{Z}$ y $K[x_1, \ldots, x_n]$ son normales.

Ejemplo 23.8. Sea $\alpha = a + b\sqrt{d}$ con a y b racionales y d un entero libre de cuadrados. Si α es un entero algebraico, también lo es su conjugado $a - b\sqrt{d}$. En particular $2a$ y $2b\sqrt{d}$ son enteros. Así que también lo es $(2b\sqrt{d})^2 = (2b)^2 d$, por lo que siendo d libre de cuadrados, $2b$ debe ser un entero. Se sigue que podemos escoger enteros n y m tales que $a - n$ y $b - m$ sean 0 o $\frac{1}{2}$. Se sigue que $\alpha - n + m\sqrt{d} \in \{0, \frac{1}{2}, \frac{\sqrt{d}}{2}, \frac{1}{2} + \frac{\sqrt{d}}{2}\}$, de donde basta con verificar cuales de estos elementos son enteros. $\frac{1}{2}$ no es entero, y tampoco lo es $\frac{\sqrt{d}}{2}$ ya que su cuadrado es $\frac{d}{4}$. El elemento $\frac{1}{2} + \frac{\sqrt{d}}{2}$ tiene el polinomio irreducible

$$x^2 - x + \frac{1-d}{4},$$

de donde es un entero sí y sólo si $d \equiv 1$ módulo 4. En este caso los enteros de $\mathbb{Q}(\sqrt{d})$ son los elementos de $\mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$ y en los casos restantes de $\mathbb{Z}(\sqrt{d})$.

Ejemplo 23.9. Si $A = \mathbb{Z}[\sqrt{-5}]$, entonces A es normal pero A no es un DFU, por lo que la conversa a la proposición anterior es falsa.

Ejercicios

El teorema de las funciones simétricas

En este capítulo daremos una versión mas detallada del teorema de las funciones simétricas. Sea $\mathbb{Z}[x_1, \ldots, x_n]$ el anillo de polinomios simétricos en n

variables con coeficientes en $\mathbb{Z}$. Recordemos que las funciones simétricas elementales $\sigma_1, \ldots, \sigma_n \in \mathbb{Z}[x_1, \ldots, x_n]$ se definen mediante la relación

$$\prod_{i=1}^{n}(X - x_i) = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \ldots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n\sigma_n.$$

El polinomio

$$U_n(x_1 \ldots, x_n, X) = \prod_{i=1}^{n}(X - x_i) \in \mathbb{Z}[x_1, \ldots, x_n][X]$$

recibe el nombre de polinomio genrico con n raices.

Proposición 23.10. *El anillo $\mathbb{Z}[\sigma_1, \ldots, \sigma_n]$ es un anillo de polinomios en las variables $\sigma_1, \ldots, \sigma_n$.*

Daremos dos demostraciones distintas de este resultado. La primera utiliza el concepto de base de trascendencia y el segundo la propiedad universal del anillo de polinomios.

Demostración 1 Como cada x_i es algebraico sobre $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$, se tiene que $\{\sigma_1, \ldots, \sigma_n\}$ debe contener una base de trascendencia de $\mathbb{Q}(x_1, \ldots, x_n)/Q$. Como esta extensión tiene grado de trascendencia n, la base de trascendencia debe ser de hecho $\{\sigma_1, \ldots, \sigma_n\}$ por lo que estos elementos son algebraicamente independientes. □

Demostración 2 Sea $\mathbb{Z}[y_1, \ldots, y_n]$ el anillo de polinomios en n variables con coeficientes en $\mathbb{Z}$. Claramente, por la propiedad universal del anillo de polinomios existe un homomorfismo de anillos

$$\phi : \mathbb{Z}[y_1, \ldots, y_n] \to \mathbb{Z}[\sigma_1, \ldots, \sigma_n], \text{ tal que } \phi(x_i) = \sigma_i.$$

Probaremos que existe la inversa. Sea $k = \mathfrak{Quot}(\mathbb{Z}[y_1, \ldots, y_n])$. Entonces, existe un cuerpo L que contiene a k (por ejemplo, la clausura algebraica de k) en donde el polinomio

$$F(X) = X^n - y_1 X^{n-1} + y_2 X^{n-2} - \ldots + (-1)^{n-1}y_{n-1}X + (-1)^n y_n$$

se factoriza completamente en factores lineales. Si

$$F(X) = \prod_{i=1}^{n}(X - \alpha_i),$$

existe un homomorfismo ψ tal que $\psi(x_i) = \alpha_i$, en particular $\psi(\sigma_i) = y_i$. □

Proposición 23.11 (Teorema de las funciones simétricas)**.** *Sea C un anillo conmutativo. Todo polinomio simétrico en n variables con coeficientes en C es un polinomio en las funciones simétricas elementales.*

Demostración Supongamos primero que $C = \mathbb{Z}$. Como S_n actúa fielmente en el cuerpo $L = \mathbb{Q}(x_1, \ldots, x_n)$ mediante $\lambda(x_n) = x_{\lambda(n)}$, se tiene que L/L^G es una extensión Galoisiana con grupo de Galois S_n. En particular, $[L : L^G] = n!$. Por otro lado, si $K = \mathbb{Q}(\sigma_1, \ldots, \sigma_n)$, entonces el polinomio U_n tiene raices en K y su cuerpo de descomposición sobre K es L de donde $[L : K] \leq n!$. Como $K \subseteq L^G$, se tiene que $K = L^G$. Luego todo polinomio simétrico en $x_1, \ldots, x_n$ es un elemento de K. Por otro lado K es el cuerpo de cocientes del anillo $\mathbb{Z}[\sigma_1, \ldots, \sigma_n]$. Este anillo es un DFU, y por lo tanto normal, por ser isomorfo a un anillo de polinomios con coeficientes en $\mathbb{Z}$. Como cada x_i es entero sobre $\mathbb{Z}[\sigma_1, \ldots, \sigma_n]$, tambien lo es cada polinomio con coeficientes enteros en dichas variables. Luego

$$\mathbb{Z}[\sigma_1, \ldots, \sigma_n] \cap K = \mathbb{Z}[x_1, \ldots, x_n],$$

lo que termina la demostración.

En el caso general, para que un polinomio se simétrico, los monomios en la misma S_n-órbita deben tener el mismo coeficiente, de modo que es suficiente probar la proposición para sumas de monomios en la misma órbita, pero estos son imágenes de polinomios simétricos en $\mathbb{Z}[x_1, \ldots, x_n]$. □

Observación 23.12. Observese que cada σ_i es homogénea. Se sigue que cada monomio en las funciones simétricas elementales es homogénea. Tiene sentido, por lo tanto definir el grado de un monomio en las funciones simétricas elementales como la suma de los grados de sus factores. Además, todo polinomio es producto de grados, y dos polinomios son iguales si y sólo si las correspondientes partes hamogéneas son iguales. En particular, si f es un polinomio homogéneo de grado s, y si $f(x_1, \ldots, x_n) = g(\sigma_1, \ldots, \sigma_n)$, entonces podemos suponer que cada monomio de $g(\sigma_1, \ldots, \sigma_n)$ tiene grado s. En particular, cada monomio en $g(x_1, \ldots, x_n)$ tiene grado al menos s/n.

Proposición 23.13. *Sea C un anillo conmutativo. Toda serie de potencias simétrica en $C[[x_1, \ldots, x_n]]$ es una serie de potencias en las funciones simétricas elementales.*

Demostración Sea $f(x_1, \ldots, x_n)$ una serie de potencias y escribamos

$$f(x_1, \ldots, x_n) = \sum_{r=0}^{\infty} f_r(x_1, \ldots, x_n),$$

donde f_r es un polinomio homogéneo de grado r. Esta descomposición es única por lo que f es simétrica si y sólo si lo es cada polinomio f_r. Basta, entonces, escribir cada uno de ellos como polinomio en las funciones simétricas elementales. y la convergencia sigue de la observación anterior. □

Ejemplos

1. $x_1^2 + x_2^2 = \sigma_1^2 - 2\sigma_2$.
2. $\frac{1}{x_1} + \frac{1}{x_2} = \frac{\sigma_1}{\sigma_2}$.
3. $\text{Arctan}x_1 + \text{Arctan}x_2 = \text{Arctan}\left(\frac{\sigma_1}{1-\sigma_2}\right)$.
4. $\cos(x_1 - x_2) = g(\sigma_1^2 - 4\sigma_2)$, donde g es la única serie de potencias que es solución de la ecuación funcional $g(x^2) = \cos(x)$. En este ejemplo, el coseno puede remplazarse por cualquier función par.

Ejercicios

Chapter 24

Anillos de matrices

Aunque ya hemos utilizado algunos ejemplos con matrices, ahora formalizaremos este concepto. Aqui y en lo sucesivo utilizamos la convención de que $\mathbf{n}$ denota el conjunto $\{1, \ldots, n\}$.

definición 24.1. Sea R un anillo no necesariamente unitario. El anillo de matrices $\mathbb{M}_n(R)$ con coeficientes en R es el grupo abeliano $R^{\mathbf{n}\times\mathbf{n}}$, es decir el grupo de funciones en $\mathbf{n} \times \mathbf{n}$, a valores en R, que identificamos simplemente con arreglos $(a_{j,k})_{j,k=1}^{n}$ de $n \times n$ elementos de R con la adición por componentes. A este grupo abeliano le asociamos la multiplicación definida por

$$(a_{i,j})_{i,j=1}^{n} (b_{j,k})_{j,k=1}^{n} = \left(\sum_{j=1}^{n} a_{i,j} b_{j,k} \right)_{i,k=1}^{n}.$$

Todas las propiedades de un anillo se comprueban inmediatamente de la definición.

Ejemplo 24.2. En $\mathbb{M}_2(R)$, la definición se reduce a

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}.$$

Si R es un anillo unitario, también lo es $\mathbb{M}_n(R)$, con la unidad

$$1_{\mathbb{M}_n(R)} = \begin{pmatrix} 1_R & 0 & 0 & \cdots & 0 \\ 0 & 1_R & 0 & \cdots & 0 \\ 0 & 0 & 1_R & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1_R \end{pmatrix}.$$

Ejemplo 24.3. La funcion $\psi : \mathbb{M}_2(\mathbb{M}_2(R)) \to \mathbb{M}_4(R)$ definida por

$$\psi\left(\begin{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} & \begin{pmatrix}e & f\\ g & h\end{pmatrix}\\ \begin{pmatrix}i & j\\ k & l\end{pmatrix} & \begin{pmatrix}n & m\\ o & p\end{pmatrix}\end{pmatrix}\right) = \begin{pmatrix}a & b & e & f\\ c & d & g & h\\ i & j & m & n\\ k & l & o & p\end{pmatrix}$$

es un isomorfismo (ejercicio). Mas generalmente, puede probarse que el anillo $\mathbb{M}_n(\mathbb{M}_m(R))$ es isomorfo a $\mathbb{M}_{mn}(R)$. Este isomorfismo es el que permite realizar las operaciones de suma y producto de matrices *por bloques*.

El anillo R es isomorfo al subanillo de $\mathbb{M}_n(R)$ formado por las matrices de la forma

$$rI_n = \begin{pmatrix}r & 0 & 0 & \cdots & 0\\ 0 & r & 0 & \cdots & 0\\ 0 & 0 & r & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & r\end{pmatrix}.$$

Nótese sin embargo que este no es el producto de r por una matriz I_n, ni siquiera con una definición apropiada de multiplicación escalar a no ser que R sea un anillo unitario. El conjunto de estas matrices se denota RI_n y es un subanillo isomorfo a R. Podemos identificar a R con RI_n. Si R no es untario podemos asumir que está contenido en un anillo unitario R', de donde $\mathbb{M}_n(R) \subseteq \mathbb{M}_n(R')$. Asumiremos que R es unitario en todo lo que sigue. En este caso, la matriz identidad $I_n = 1I_n$ es realmente un elemento de $\mathbb{M}_n(R)$.

Sea $E_{i,j}$ La matriz que tiene un 1 en la intersección de la fila i con la columna j y que tiene un 0 en cada una de las restantes posiciones, entonces se tienen las siguientes identidades:

1. $E_{i,j}E_{j,k} = E_{i,k}$, $E_{i,j}E_{u,k} = 0$, si $u \neq j$.
2. $E_{1,1} + E_{2,2} + \ldots + E_{n,n} = I_n$.
3. $rE_{i,j} = E_{i,j}r$, si $r \in RI_n$.

Además, si A es cualquier anillo con un subanillo isomorfo a R y con elementos $E_{i,j}$ tales que satisfacen (1),(2) y (3), entonces el subconjunto A' de A formado por todas las combinaciones del tipo $a = \sum_{i,j} r_{i,j}E_{i,j}$ es un subanillo y la función que lleva a la matriz $(r_{i,j})_{i,j}$ al elemento $a = \sum_{i,j} r_{i,j}E_{i,j}$ es un

homomorfismo de anillos. Más aún, si una de estas expresiones se anula, digamos $\sum_{i,j} r_{i,j}E_{i,j} = 0$, premultiplicando por $E_{u,s}$ y postmultiplicando por $E_{t,u}$ se tiene $r_{s,t}E_{u,u} = 0$. Sumando sobre u estas identidades, se concluye que $r_{s,t} = 0$. Esto implica que $A' \cong \mathbb{M}_n(R)$.

Proposición 24.4 (Teorema de las unidades matriciales)**.** *Si existen elementos $E_{1,1}, \ldots, E_{n,n}$ que satisfacen (1) y (2) entonces*

$$R = \left\{ \sum_{u=1}^{n} E_{u,1} a E_{1,u} \middle| a \in A \right\}$$

es un subanillo de A que satisface (3), de donde en particular $A \cong \mathbb{M}_n(R)$.

Demostración. Basta comprobar (3):

$$\left(\sum_{u=1}^{n} E_{u,1} a E_{1,u} \right) E_{i,j} = \sum_{u=1}^{n} E_{u,1} a (E_{1,u} E_{i,j}) =$$

$$\sum_{u=1}^{n} E_{u,1} a \delta_{i,u} E_{1,j} = E_{i,1} a E_{1,j},$$

y del mismo modo se prueba que

$$E_{i,j} \left(\sum_{u=1}^{n} E_{u,1} a E_{1,u} \right) = E_{i,1} a E_{1,j}.$$

□

Ejemplo 24.5. Si $n = 2$ entonces

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = aE_{1,1} + bE_{1,2} + cE_{2,1} + dE_{2,2}.$$

Observación 24.6. En general no es cierto que si $\mathbb{M}_n(R) \cong \mathbb{M}_m(R')$ entonces $R \cong R'$. Basta tomar como ejemplo el caso $n = 2$, $m = 1$, con $R = \mathbb{R}$ y $R'' \cong \mathbb{M}_2(\mathbb{R})$. Sin embargo, cuando R es conmutativo, entonces $R \cong RI_n$ se puede caracterizar como el conjunto de matrices que conmutan con cualquier otra, es decir el centro de $\mathbb{M}_n(R)$. En tal caso podemos recuperar la estructura de un anillo R de la estructura de cualquiera de sus anillos de matrices.

Cocientes y matrices

Si J es un ideal bilátero de R, el anillo (no unitario) de matrices $\mathbb{M}_n(J)$ con coeficientes en J es un ideal bilátero de $\mathbb{M}_n(R)$ (ejercicio). La función $\psi : \mathbb{M}_n(R)/\mathbb{M}_n(J) \to \mathbb{M}_n(R/J)$ definida por

$$\psi\left[(a_{i,j})_{i,j=1}^n + \mathbb{M}_n(J)\right] = (a_{i,j} + J)_{i,j=1}^n$$

es un isomorfismo de anillos (ejercicio).

Ejercicios

1. Sea R un anillo, y sea J un ideal bilátero de

$$\mathbb{M}_n(R) = \{a = (a_{i,j})_{i,j=1}^n | a_{i,j} \in R\}.$$

   a) Sea $J_{m,p} = \{a_{m,p} | a \in \mathbb{M}_n(R)\}$. Probar que $J_{m,p}$ es un ideal bilátero de R.

   b) Probar que $J_{m,p} = J_{r,s}$ para todo $m, p, r, s \in \{1, \ldots, n\}$ (sugerencia, usar los elementos $E_{i,j}$ que tienen un 1 en la fila i y la columna j y 0's en el resto).

   c) Probar que $J = \mathbb{M}_n(J_{1,1}) = \{(a_{i,j})_{i,j=1}^n | a_{i,j} \in J_{1,1} \forall i, j\}$.

   d) Describa todos los ideales biláteros de $\mathbb{M}_n(\mathbb{Z})$.

2. Sea $A = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} | a, b, d \in R \right\}$. Probar que $J = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} | b \in R \right\}$ es un ideal bilátero de A.

3. Probar que si J es un ideal bilátero de R, entonces $\mathbb{M}_n(R)/\mathbb{M}_n(J) \cong \mathbb{M}_n(R/J)$.

4. Probar que

$$Z(\mathbb{M}_n(R)) = \left\{ \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ 0 & r & 0 & \cdots & 0 \\ 0 & 0 & r & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & r \end{pmatrix} \middle| \, r \in Z(R) \right\}.$$

5. Probar que $\mathbb{M}_n(R_1 \times R_2) \cong \mathbb{M}_n(R_1) \times \mathbb{M}_n(R_2)$.

6. Calcule el inverso, en $\mathbb{M}_3(\mathbb{Z}/125\mathbb{Z})$ de

$$\begin{pmatrix} 16 & 25 & 40 \\ 5 & 11 & 75 \\ 60 & 25 & 46 \end{pmatrix}.$$

7. Calcule el inverso, en $\mathbb{M}_3(\mathbb{Z}/8\mathbb{Z})$ de

$$B = \begin{pmatrix} 9 & 11 & 1 \\ 4 & 1 & 3 \\ 4 & 2 & 7 \end{pmatrix}.$$

   Sugerencia: Probar que $(B-1)^5 = 0$.

8. Sea I la matriz unitaria de 2×2 y sea O la matriz nula. Probar que si A es una subalgebra de $\mathbb{M}_4(R)$ que contiene a las matrices

$$\begin{pmatrix} I & O \\ O & O \end{pmatrix}, \quad \begin{pmatrix} O & I \\ O & O \end{pmatrix}, \quad \begin{pmatrix} O & O \\ I & O \end{pmatrix}, \quad \begin{pmatrix} O & O \\ O & I \end{pmatrix},$$

   entonces $A \cong \mathbb{M}_2(S)$ para algún anillo S. Dé un ejemplo donde:

   (a) $R = \mathbb{R}$ y $S \cong \mathbb{C}$.

   (b) $R = \mathbb{R}$ y $S \cong \mathbb{R} \times \mathbb{R}$.

9. Utilizando el Teorema de las unidades matriciales, probar que

$$\mathbb{M}_n\Big(\mathbb{M}_m(R)\Big) \cong \mathbb{M}_{mn}(R).$$

Chapter 25

Algebras simples y semisimples

En este capítulo todas las álgebras que aparecen son álgebras sobre un cuerpo K. Una K- álgebra se dice simple si no tiene ideales biláteros no triviales. Si L/K es una extensión cualquiera de cuerpos, la K-álgebra $\mathbb{M}_n(L)$ es simple. Más generalmente, si D es una K-álgebra en la que cada elemento $a \neq 0$ tiene un inverso entonces $\mathbb{M}_n(D)$ es simple. En este capítulo probaremos que toda álgebra simple de dimensión finita es de hecho de este tipo. Una K-álgebra en la que cada elemento $a \neq 0$ tiene un inverso se denomina un álgebra de división. Los términos *anillo de división* y *anillo simple* se define análogamente eliminando la condición de D o A sean K-álgebras. Observese que si A es una K-álgebra de dimensión finita, todo ideal izquierdo de A es un subespacio vectorial de A, por lo que A satisface la condición de cadenas ascendentes y descendentes para ideales izquierdos (o derechos, o biláteros). Se sigue que existen ideales izquierdos minimales (no nulos) en A. Recordemos que todo ideal izquierdo puede ser considerado como un A-módulo utilizando la multiplicación usual del anillo A como multiplicación escalar en el módulo. Se sigue que un ideal minimal I es un módulo que no tiene ningún submódulo no trivial. Un módulo con esta propiedad se denomina irreducible.

Proposición 25.1. *Sea M un A-módulo irreducible. Sea D el anillo de automorfismos (como A-módulo) de M. Entonces D es un anillo de división.*

Demostración Sea $\phi : M \to M$ un homomorfismo de A-módulos. Entonces $\phi(M)$ es un submódulo, es decir un ideal contenido en M. Se sigue que $\phi(M) = 0$ (en cuyo caso $\phi = 0$) o $\phi(M) = M$. Del mismo modo,

$\ker(\phi) = 0$ o $\ker(\phi) = M$. En el segundo caso se tiene de nuevo $\phi = 0$. Se sigue que si $\phi \neq 0$, entonces ϕ es una función lineal invertible. Es inmediato que en el segundo caso ϕ^{-1} es también un homomorfismo de módulos. □

Cuando A es una K-álgebra y M tiene dimensión finita como K-espacio vectorial, es suficiénte probar la inyectividad (o la epiyectividad), ya que ϕ es K-lineal.

Corolario 25.1.1. *Sea I un ideal izquierdo minimal de un anillo A. Sea D el anillo de automorfismos (como A-módulo) de I. Entonces D es un anillo de división.*

Ejemplo 25.2. Si $A = \mathbb{Z} \times \mathbb{Q}$, el ideal $\{0\} \times \mathbb{Q}$ es minimal y su grupo de automorfismos es isomorfo a $\mathbb{Q}$. Sin embargo $\mathbb{Z} \times \{0\}$ no contiene ningún ideal minimal no nulo.

Al hablar de anillos de división, sin embargo, la restricción a álgebras es inmaterial, por causa del siguiente resultado:

Proposición 25.3. *Si D es un anillo de división, su centro $L = Z(D)$ es un cuerpo. La inclusión $L \hookrightarrow D$ hace de D una K-álgebra.*

Demostración Basta observar que si $ab = ba$ para todo $b \in D$ se tiene, pre y post-multiplicando por a^{-1} que $ba^{-1} = a^{-1}b$ para todo b en D. Las última afirmación es trivial. □

El siguiente resultado es el análogo para anillos de división de la existencia de bases para espacios vectoriales.

Proposición 25.4. *Si D es un anillo de división, todo D-módulo finitamente generado es isomorfo al D-módulo libre D^n.*

Demostración Sea M un D-módulo finitamente generado. Sea $\{e_1, \ldots, e_n\}$ un conjunto minimal de generadores de M. Basta probar que $\{e_1, \ldots, e_n\}$ es linealmente independiente sobre D. Por otro lado, si $\sum_i a_i e_i = 0$ con, digamos, $a_1 \neq 0$, se tiene

$$e_1 = -\sum_{i=2}^{n} a_1^{-1} a^i e_i,$$

de donde $\{e_2, \ldots, e_n\}$ genera M. □

En lo que sigue, M denotará un A-módulo irreducible y D denotara a su anillo de endomorfismos, el cual es un anillo de división por lo dicho anteriormente. Para elementos $\phi \in D$, $a \in A$, y $m \in M$ cualesquiera, la propiedad de que los elementos de D son automorfismos como D-módulos de A se escribe

$$a\phi(m) = \phi(am),$$

pero esto puede interpretarse también como que los elementos de A actúan en I como automorfismos de D-módulos. Si M es finitamente generado como D-módulo, se tiene $M \cong D^d$ para algún entero d, por lo que el álgebra de endomorfismos como D-módulo de M se identifica naturalmente con el anilo de matrices $\mathbb{M}_d(D)$ (Crosreferencia). La acción de A en M por endomorfismos define un homomorfismo de anillos $\rho : A \to \mathbb{M}_d(D)$ o más generalmente $\rho : A \to \mathrm{End}_D(M)$. Sea J el núcleo de este homomorfismo. El anillo A/J se identifica con una sub-anillo de $\mathbb{M}_d(D)$ vía ρ. El ideal bilátero J recibe el nombre de anulador de M y se denota $\mathrm{Ann}(M)$. Puede caracterizarse como el conjunto de elementos $b \in A$ tales que $bm = 0$ para todo $m \in M$.

definición 25.5. Un anillo se dice simple si no tiene ideales biláteros no triviales.

Si A es simple, necesariamente $J = 0$ por lo que A se identifica con un sub-anillo de $\mathbb{M}_d(D)$.

Ejemplo 25.6. La $\mathbb{R}$-álgebra $\mathbb{C}$ es simple y tiene el $\mathbb{C}$-módulo $M = \mathbb{C} \cong \mathbb{R}^2$, por lo que se identifica con una subálgebra de $\mathbb{M}_2(\mathbb{R})$. Esta es la subálgebra formada por todas las matrices de la forma

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

El anillo de endomorfismos de M como $\mathbb{C}$-módulo es $\mathbb{C}$, no $\mathbb{R}$. Probaremos más adelante que si D es el anillo de A-endomorfismos de I, entonces A debe ser igual al álgebra $\mathbb{M}_m(D)$ completa.

Lema 25.7. *Si I es un ideal minimal de la K-álgebra simple A de dimensión finita sobre K entonces I contiene un elemento v tal que $uv = u$ para todo $u \in I$.*

Demostración Sea $r \in I$. Entonces $Ir \subseteq AI = I$ es un ideal izquierdo contenido en I. Se sigue que $Ir = 0$ o $Ir = I$. Si $I^2 = 0$, entonces I está contenido en su anulador J lo que contradice el hecho de que $J = 0$, pues A es simple. En caso contrario $Ir = I$. Se sigue que existe $\phi \in D$ tal que $\phi(u) = ur$ para todo $u \in I$. Como D es un álgebra de división sobre K, la subálgebra $K(\phi)$ es un cuerpo y de hecho una extensión finita de K. Se sigue que ϕ es raiz de alguna ecuación del tipo $1 + a_1X + \ldots + a_nX^n = 0$. Se sigue que si $v = -a_1r - \ldots - a_nr^n$ se cumple lo pedido. □

Nótese que el elemento v definido arriba es idempotente aunque no central. De hecho si v fuese cental, $I = Av$ tendría que ser un ideal bilátero, lo que es absurdo ya que A es simple.

Lema 25.8. *Si I es un ideal minimal (izquierdo) de la K-álgebra A de dimensión finita sobre K entonces existe un ideal izquierdo I' tal que $A = I' \oplus I$ como A-módulos.*

Demostración Sea $v \in I$ como en el lema precedente. Entonces el homomorfismo de A-módulos $\psi : A \to I$ definido por $\psi(a) = av$ tiene un núcleo I'. Como $\psi(u) = u$ para todo $u \in I$, el homomorfismo ψ satisface $\psi^2 = \psi$ por lo que $(\psi - 1)\psi = 0$. El resultado sigue si observamos que $(\psi - 1)A = I'$. □

Lema 25.9. *Todo álgebra simple A de dimensión finita es suma de ideales izquierdos minimales.*

Demostración Sea I_1 un ideal izquierdo minimal. Escribimos $A = I_1 \oplus I_1'$ como en el lema previo. Sea I_2 un ideal minimal contenido en I_1'. Nótese que $u \in I_1'$ si y sólo $uv_1 = 0$ si v_1 es el idempotente asociado a I_1. Se sigue que el idempotente v_2 asociado a I_2 satisface $v_2v_1 = 0$. El elemento $(1 - v_1)v_2$ está en el ideal I_2, es no nulo ya que

$$v_2(1 - v_1)v_2 = v_2^2 - v_2v_1v_2 = v_2$$

y es un idempotente, lo que se obtiene pre-multiplicando la identidad anterior por $(1 - v_1)$. Se sigue que remplazando v_2 por $(1 - v_1)v_2$ puede suponerse que $v_1v_2 = 0$. Esto implica que $v_1 + v_2$ es un idempotente y

$$A = A(1 - v_1 - v_2) \oplus A(v_1 + v_2) = A(1 - v_1 - v_2) \oplus Av_1 \oplus Av_2 = I'' \oplus I_1 \oplus I_2,$$

donde $I'' = A(1 - v_1 - v_2)$ es un ideal izquierdo. Iterando este proceso se tiene $A = I_1 \oplus I_2 \oplus \ldots \oplus I_r$. □

Lema 25.10. *En la descomposición $A = I_1 \oplus I_2 \oplus \ldots \oplus I_r$ mencionada arriba, para cada par de indices i y j, existe un elemento $a \in A$ tal que $I_i a = I_j$.*

Demostración En el conjunto $\{1, \ldots, r\}$ definimos la relación $>$ como sigue:

$$i > j \iff I_i = I_j a \text{ para algún } a \in A.$$

Esta relación es reflexiva y transitiva. Sea $\equiv$ la relación definida por

$$i \equiv j \iff i > j \wedge j > i.$$

Entonces $\equiv$ es una relación de equivalencia y $>$ induce un orden parcial entre las clases de equivalencia. Bastará por lo tanto probar que si $O = \{i_1, \ldots, i_s\}$ es una clase de equivalencia que es maximal con respecto al orden inducido, entonces $I_O = \bigoplus_{i \in O} I_i$ es un ideal bilátero. Como no hay ideales biláteros no triviales, esto implicará que existe una única clase de equivalencia y el resultado sigue.

Si I_O no es un ideal bilátero, existe $a \in A$ tal que $I_O a$ no está contenido en I_O. Como $1 = v_1 + \ldots + v_n$, necesariamente $I_O a v_i \neq 0$ para algún $i \notin O$. Se sigue que $I_O a v_i = I_i$ por lo que $I_j(av_i) = I_i$ para algún $j \in O$ lo que es una contradicción. □

Lema 25.11. *En la descomposición $A = I_1 \oplus I_2 \oplus \ldots \oplus I_r$ mencionada arriba, existe un elemento $v_{i,j}$ en A tales que $v_{i,j} v_{k,l} = \delta_{j,k} v_{i,l}$ y $v_{1,1} + \ldots + v_{r,r} = 1$.*

Demostración Para cada par $\{i, i+1\}$ existe un elemento a tal que $I_i = I_{i+1} a$. Remplazando a por $v_{i+1} a v_i$ si es necesario podemos suponer que $v_{i+1} a = a v_i = a$. En particular, $a \in I_i$. como $Aa \neq 0$, necesariamente $Aa = I_i$ por minimalidad. Del mismo modo existe $b \in A$ tal que $I_{i+1} = I_i b$ y satisface $v_i b = b v_{i+1} = b$. Se sigue que $c = ba$ es un elemento de I_i que satisface $v_i c = c v_i = c$. En particular $x \mapsto xc$ es un endomorfismo no nulo de I_i que tiene un inverso ψ en el anillo de división D. Sea $d = \psi(v_i)$. Entonces $v_i = dc$ por definición de inverso, mientras que $cd = c\psi(v_i) = \psi(c)$. Pero por ser $\psi^{-1}(v_i) = v_i c = c$ se tiene $cd = v_i$. En particular $e = a(db)$ satisface $v_{i+1} e = e v_{i+1} = e$. Como $e^2 = ad(ba)db = adb = e$, el endomorfismo $x \mapsto xe$ es un idempotente de D por lo que debe ser la identidad. Se sigue que $v_i = v_i e = e$.

Definimos ahora $v_{i+1,i} = a$ y $v_{i,i+1} = db$. Se sigue que $v_{i+1,i} v_{i,i+1} = v_{i+1,i+1} = v_{i+1}$ y $v_{i,i+1} v_{i+1,i} = v_{i,i} = v_i$. Ahora se define

$$v_{i,i+k} = v_{i,i+1} \ldots v_{i+k-1,i+k}, \qquad v_{i+k,i} = v_{i+k,i+k-1} \ldots v_{i+1,i},$$

y el resultado sigue por una comprobación de rutina. □

Proposición 25.12. *Si A es un álgebra simple de dimensión finita, entonces A es isomorfa a un álgebra de la forma $\mathbb{M}_r(D)$ donde D es un álgebra de división.*

Demostración Si $A = I_1 \oplus \ldots \oplus I_r$, se sigue del lema precedente y del teorema de las unidades matriciales, que $A = \mathbb{M}_r(B)$ para alguna álgebra de dimensión menor B, por lo que el resultado sigue por inducción excepto si $r = 1$. En este caso se tiene $A = I_1$ con I_1 minimal, es decir que A no tiene ideales izquierdos no triviales. Afirmamos que en este caso A es un álgebra de división. De hecho si $a \in A$ es no nulo, se tiene que $Aa = A$, de modo que existe $b \in A$ tal que $ba = 1$. Del mismo modo existe $c \in A$ tal que $cb = 1$. Se sigue que $a = c$ y b es el inverso de a. □

Lema 25.13. *Sea A un álgebra simple de dimensión finita con $A = I_1 \oplus \ldots \oplus I_r$ donde cada I_i es un ideal izquierdo minimal. Si J es un ideal izquierdo minimal, entonces J es isomorfo como A-módulo a algún I_i.*

Demostración Basta ver que se tiene la inclusión

$$J \subseteq J' = J_1 \oplus \ldots \oplus J_r,$$

donde $J_i = Jv_i$, ya que $a = av_1 + \ldots + av_r$. Como J es minimal, la proyección canónica $J \mapsto J_i$ es nula o un isomorfismo (pues el núcleo y la imagen son submódulos). Como la proyección es de hecho epiyectiva por definición, solo puede ser nula si J_i es $\{0\}$. Como J no es nulo, algún J_i es no nulo. Se sigue que J debe ser isomorfo como A-módulo a uno o más J_i's y los restantes deben ser nulos. Por otro lado $J_i = Jv_i$ es submódulo del submódulo minimal $I_i = Av_i$ por lo que deben ser iguales si J_i es no-nulo. □

Proposición 25.14. *Si I es un ideal minimal del álgebra simple A de dimensión finita, entonces I es isomorfo como A-módulo a D^m donde $A = \mathbb{M}_m(D)$.*

Demostración Basta ver que $A = I_1 \oplus \ldots \oplus I_m$ donde I_i es el ideal de matrices que tienen ceros fuera de la columna i-ésima y aplicar el lema precedente. □

Corolario 25.14.1. *Si I es un ideal minimal del álgebra simple A de dimensión finita, entonces el anillo de homomorfismos como D-módulo del ideal I concide con el anillo A.* □

Corolario 25.14.2. *Si I es un ideal minimal del álgebra simple A de dimensión finita, entonces el anillo de homomorfismos como A-módulo del ideal I es isomorfo a D donde $A \cong \mathbb{M}_m(D)$.* □

Corolario 25.14.3. *Si I es un ideal minimal del álgebra simple A de dimensión finita, y si el anillo de homomorfismos como A-módulo del ideal I es isomorfo a D entonces $A \cong \mathbb{M}_m(D)$. para algún entero m.* □

Corolario 25.14.4. *Si $\mathbb{M}_m(D) \cong \mathbb{M}_s(D')$ para dos álgebras de división D y D' de dimensión finita, y para algún par de enteros (s, m), entonces $s = m$ y $D \cong D'$.* □

Una manera de obtener anillos simples es cocientando un anillo cualquiera por un ideal bilátero maximal, ya que el teorema de la correspondencia implica lo siguiente:

Proposición 25.15. *Si J es un ideal bilátero maximal de A, entonces A/J es simple.* □

El siguiente resultado es análogo a la existencia de ideales maximales en un anillo conmutativo. La demostración es identica.

Proposición 25.16. *Todo ideal bilátero de un anillo A está contenido en un ideal bilátero maximal.* □

Anillos primitivos

A fin de generalizar los resultados de la sección anterior introducireel concepto de anillo primitivo, el cual también nos será útil en la sección siguiente.

definición 25.17. Un anillo A se dice primitivo si existe un A-módulo irreducible M tal que el homomorfismo canónico $A \mapsto \mathrm{End}_D(M)$, donde D es el anillo de endomorfismos de M como A-módulo, es inyectivo. Equivalentemente, si $a \in A$ satisface $am = 0$ para todo $m \in M$, entonces $a = 0$. Un módulo con esta propiedad se dice fiel.

Lema 25.18. *Todo módulo irreducible de un anillo A es isomorfo a A/I para algún ideal izquierdo maximal I de A.*

Demostración Sea $m \in M$ un elemento no nulo. Basta ver que el núcleo del homomorfismo $\psi : A \to M$ dado por $\psi(a) = am$ es epiyectivo y su núcleo es un ideal izquierdo maximal. La primera afirmación sigue de que $\psi(A)$ es un submódulo no nulo de M (pues contiene a m) y la segunda es inmediata del teorema de la correspondencia (para módulos). □

Proposición 25.19. *Un anillo A es primitivo si y sólo si existe un ideal izquierdo I tal que $J + I = A$ para todo ideal bilátero no trivial J.*

Demostración Si A es primitivo, existe un ideal I tal que A/I es fiel, es decir, la multiplicación por ningún elemento no nulo de A es trivial en A/I. En otras palabras, si a es un elemento no nulo de A, existe $b \in A$ tal que $ab \notin I$. Si J es un ideal bilátero no nulo de A, y si $a \in J$ es no-nulo, el elemento ab mencionado arriba está en J pero no en I por lo que $I + J$ contiene propiamente a I. Como I es maximal se tiene $I + J = A$. Por otro lado, si I es un ideal tal que $I + J = A$ para todo ideal bilátero J, podemos remplazar I por un ideal maximal que lo contenga, el cual gozará de la misma propiedad. Se sigue que podemos suponer que I era maximal. En tal caso el módulo A/I es irreducible y el núcleo J del homomorfismo natural $A \to \mathrm{End}_D(A/I)$ está contenido en I (ya que $a(1 + I) = a + I$). Se sigue que $J = 0$. □

Corolario 25.19.1. *Todo anillo simple es primitivo.* □

Proposición 25.20. *Sea A un anillo primitivo. Sea M un A-módulo irreducible y fiel. Sea D su anillo de endomorfismos como A módulo. Sean $x_1, \ldots, x_r$ elementos de M que son linealmente independientes sobre D y sean $y_1, \ldots, y_r$ elementos de M cualesquiera. Entonces existe $a \in A$ tal que $ax_i = y_i$ para todo $i = 1, \ldots, r$.*

Demostración Si $r = 1$ la afirmación es trivial, ya que $Ax_1 = M$. Probaremos la afirmación por inducción. De hecho, considerense las siguientes afirmaciones:

- Si $x_1, \ldots, x_r$ elementos de M que son linealmente independientes sobre D y si $y_1, \ldots, y_r$ son elementos de M cualesquiera, entonces existe $a \in A$ tal que $ax_i = y_i$ para todo $i = 1, \ldots, r$ (afirmación T_r).

- Si $x_1, \ldots, x_r$ elementos de M que son linealmente independientes sobre D existe un elemento $b \in A$ tal que $bx_r \neq 0$ mientras que $bx_i = 0$ para $i = 1, \ldots, r-1$ (afirmación S_r).

Probaremos que S_{n-1} y T_1 implican T_n, mientras que T_{n-1} implica S_n. Esto bastará.

Supongamos primero T_1 y S_{n-1}. Tomamos para cada $i = 1, \ldots, n-1$ un elemento $c_j \in A$ tal que $c_j x_i = 0$ para $i \neq j$ y $c_j x_j \neq 0$. Escogemos d_j tal que $d_j(c_j x_j) = y_j$ por T_1. Entonces $a = \sum_j d_j c_j$ satisface lo pedido en T_n.

Ahora probaremos S_n utilizando T_{n-1}. Si fuese falso tendriamos que $bx_i = 0$ para cada $i = 1, \ldots, r-1$ implica $bx_r = 0$. Sean $y_1, \ldots, y_{n-1}$ elementos arbitrarios de M. Entonces existe $a \in A$ tal que $ax_i = y_i$ para cada $i = 1, \ldots, n-1$. Para cada $(y_1, \ldots, y_{n-1}) \in M^{n-1}$ definimos $f(y_1, \ldots, y_{n-1}) = ax_n$. Afirmamos que f está bien definido y es un homomorfismo de A-módulos.

De hecho, si a' también satisface $a'x_i = y_i$ para $i = 1, \ldots, n-1$, entonces $a - a'$ anula $x_1, \ldots, x_{n-1}$ por lo que debe anular también a x_n y se tiene $ax_n = a'x_n$. La comprobación de que f es un homomorfismo es ahora rutinaria y se deja al lector.

Sea $\phi_i : M \to M^{n-1}$ la inclusión en la i-ésima coordenada. Entonces $y \mapsto f \circ \phi_i(y)$ es un endomorfismo de M y por lo tanto un elemento d_i de D. Además

$$f(y_1, \ldots, y_{n-1}) = f\left(\sum_{i=1}^{n-1} \phi_i(y_i)\right) = \sum_{i=1}^{n-1} f \circ \phi_i(y_i) = \sum_{i=1}^{n-1} d_i(y_i).$$

Nótese que si cada $y_i = x_i$ puede tomarse $a = 1$, por lo que $f(x_1, \ldots, x_{n-1}) = x_n$. Se sigue que

$$x_n = \sum_{i=1}^{n-1} d_i(x_i)$$

lo que contradice la independencia lineal. □

Tomando $x_1, \ldots, x_r$ de modo que formen una base de M, se tiene el siguiente resultado:

Corolario 25.20.1. *Si A es un anillo primitivo y M es un A-módulo irreducible y fiel con anillo de endomorfismos D, y si $M \cong D^n$ como D-módulo, entonces el homomorfismo natural $\phi : A \to \mathbb{M}_n(D)$ es un isomorfismo.* □

Corolario 25.20.2. *Si A es un anillo primitivo que satisface la condición de cadenas descendentes para ideales izquierdos, entonces $A \cong \mathbb{M}_n(D)$ para algún álgebra de división D.*

Demostración Basta ver que M es finitamente generado como D-módulo. Sea $x_1, \ldots$ una sucesión de elementos de M tal que cada x_i no pertenece al D-módulo generado por los anteriores. Sea L_i el comjunto de elementos de A que anula a $x_1, \ldots, x_i$. Es inmediato que L_i es un ideal izquierdo, ya que $ux_i = 0$ implica $(au)x_i = 0$ (y lo propio sucede con las sumas). También es claro que $L_{n+1} \subseteq L_n$. Afirmamos que esta última contención es estricta lo que termina la demostración, pero esto sigue de la proposición anterior, ya que si ningún x_i está en el módulo generado por los anteriores, ellos son linealmente independientes (precisar).

Corolario 25.20.3. *Si A es un anillo primitivo que satisface la condición de cadenas descendentes para ideales izquierdos, entonces A es simple.*

Algebras Semisimples

definición 25.21. Un anillo A se dice semisimple si el ideal $\{0\}$ es intersección de ideales biláteros maximales.

Proposición 25.22. *Si J_1 y J_2 son ideales biláteros comaximales, entonces*

$$A/(J_1 \cap J_2) = (A/J_1) \times (A/J_2).$$

Demostración Claramente existe un homomorfismo inyectivo de $A/(J_1 \cap J_2)$ en el producto $(A/J_1) \times (A/J_2)$. Basta ver que es epiyectivo. Como J_1 y J_2 son comaximales, se tiene $1 = a_1 + a_2$ con $a_1 \in J_1$ y $a_2 \in J_2$. Basta ver que a_1 representa la clase de 0 en A/J_1 y la clase de 1 en A/J_2 mientras que a_2 representa la clase de 0 en A/J_2 y la clase de 1 en A/J_1. El resultado sigue ahora como en el caso conmutativo. □

Proposición 25.23. *Si J_1 y J_2 son ideales biláteros comaximales con un ideal J, entonces $J_1 \cap J_2$ también lo es.*

Demostración Basta ver que si $a_1 + a = 1$ y $a_2 + a' = 1$, con $a_1 \in J_1$, $a_2 \in J_2$, y $a, a' \in J$, entonces $a_1a_2 + (aa_2 + a_1a' + aa') = 1$ y la suma en paréntesis está en J. □

De los dos resultados anteriores se tiene:

Proposición 25.24. *Si $J_1, \ldots, J_m$ son ideales biláteros comaximales a pares, entonces*

$$A\Big/\left(\bigcap_{i=1}^{m} J_i\right) = \prod_{i=1}^{m}(A/J_i).$$

□

Corolario 25.24.1. *Todo anillo semisimple que satisface la condición de cadenas descendentes para ideales biláteros es un producto de anillos simples.* □

En la literatura se dá ocasionalmente una definición diferente de anillo semisimple, que es lo que nosotros llamaremos un anillo semi-primitivo.

definición 25.25. Sea A un anillo. El radical de A el conjunto de elementos a de A, tales que $am = 0$ para todo elemento m de algún A-módulo irreducible M. Un anillo A es semi-primitivo si su radical es nulo. Un ideal bilátero J de un anillo A se dice primitivo si A/J es primitivo.

El siguiente resultado es inmediato de lo que ya sabemos sobre anillos simples y primitivos.

Proposición 25.26. *Todo anillo semisimple es semi-primitivo. Todo anillo semi-primitivo que satisface la condición de cadenas descendentes para ideales izquierdos es semi-simple.*

Corolario 25.26.1. *Todo anillo semi-primitivo que satisface la condición de cadenas descendentes para ideales izquierdos es un producto finito de álgebras de matrices sobre anillos de división.* □

Corolario 25.26.2. *Toda álgebra semi-primitiva de dimensión finita es un producto finito de álgebras de matrices sobre álgebras de división.* □

Demostración Basta ver que toda álgebra de dimensión finita satisface la condición de cadenas descendentes. □

Proposición 25.27. *El radical de un anillo A es la intersección de los ideales primitivos de A.*

Demostración Si a es un elemento del radical de A y si J es un ideal primitivo, existe un A/J-módulo irreducible y fiel que puede ser considerado como un A módulo con $bm = 0$ para todo $b \in J$. La multiplicación por a es trivial en M ya que M es irreducible. Como M es un A/J-módulo fiel, necesariamente $a \in J$. Se concluye que el radical está contenido en cada ideal primitivo.

Supongamos ahora que M es un A-módulo irreducible y sea J el núcleo del homomorfismo natural $\phi : A \to \mathrm{End}_{\mathbb{Z}}(M)$. entonces J es primitivo ya que M es un A/J-módulo irreducible y fiel. Se sigue que si a está contenido en cada ideal primitivo, entonces $am = 0$ para cada elemento m de cada módulo irreducible M. □

Corolario 25.27.1. *El radical es un ideal bilátero.* □

Proposición 25.28. *El radical de un anillo A es la intersección de los ideales izquierdos maximales de A.*

Demostración Sea $a \in A$. Supongamos primero que a está en cada ideal izquierdo maximal de A. Sea $m \in M$ un elemento no nulo. Como el homomorfismo $\phi(a) = am$ define un isomorfismo entre M y A/I para algún ideal izquierdo maximal I, el hecho de que $a \in I$ implica que $am = 0$. Por otro lado si a está en el radical e I es un ideal izquierdo maximal, entonces a debe anular a la clase $1 + I$ en A/I y por lo tanto $a \in I$. □

Corolario 25.28.1. *Un anillo A es semi-primitivo si y sólo si la intersección de los ideales izquierdos maximales de A es nula.* □

Algebras centrales simples

En esta sección todos los anillos considerados son álgebras sobre un cuerpo K. Se dice que la K-álgebra A es central si su centro $Z(A)$ coincide con la imagen $\phi(K)$, donde $\phi : K \to A$ es el homomorfismo que define el álgebra. Toda álgebra de división D es un álgebra de división sobre su centro $L = Z(D)$. Toda álgebra central simple de dimensión finita sobre un cuerpo K es de la forma $matrici_n(D)$ donde D es un álgebra central de división.

Proposición 25.29. *Si K es algebraicamente cerrado no existen algebras de división de dimensi-on finita no triviales sobre K.*

Demostración Si D es una K-álgebra de división y $a \in D$, entonces $K(a)$ es un cuerpo y por lo tanto una extensión finita de K. Se sigue que $K(a) = K$ y por lo tanto $a \in K$. Luego, a posteriori, $D = K$. □

Corolario 25.29.1. *Si K es algebraicamente cerrado toda K-álgebras simple de dimensi-on finita es isomorfa a $\mathbb{M}_n(K)$ para algún n.* □

Si A es un anillo simple entonces el ideal bilátero AaA debe ser igual a A. Esto significa que $1 \in AaA$, es decir existen elementos $c_{1,i}$ y $c_{2,i}$ tales que

$$\sum_{i=1}^{r} c_{1,i}\ a\ c_{2,i} = 1.$$

En otras palabras, existen vectores v_1 y v_2 en A^n tales que $v_1 a v_2^t = 1$ para algún n (que depende de a). En tal caso, la imágen de la función K-bilineal $f_a(v, w) = vaw^t$ es todo A. Si $\tilde{f}_a : A^n \otimes A^n \to A$ es la función lineal asociada, entonces induce un isomorfismo entre $(A^n \otimes_K A^n)/\ker(\tilde{f}_a)$ y A.

Lema 25.30. *Si A es una K-álgebra central simple y a_1, a_2 son elementos de A linealmente independientes sobre K, entonces existen vectores v y w en A^n, para algún n, tales que $va_1w^t \neq 0$ pero $va_2w^t = 0$.*

Demostración De otro modo, puede definirse una función lineal $g : A \to A$ del siguiente modo: Fijamos n lo bastante grande para que f_{a_2} sea epiyectiva. Para cada $c \in A$ tomamos v y w en A^n tales que $va_2w^t = c$ y definimos $g(c) = va_1w^t$. La función g está bien definida ya que va_1w^t se anula en el núcleo de f_{a_2}. Es claro que $g(ab) = ag(b) = g(a)b$. En particular $g(a) = ag(1) = g(1)a$ por lo que $g(1)$ está en el centro $\phi(K)$. Por otro lado $a_2g(1) = g(a_2) = a_1$, ya que para evaluar $g(a_2)$ podemos escoger $v = w = (1, 0, \ldots, 0)$. □

Lema 25.31. *Si A es una K-álgebra central simple y B es una K-álgebra arbitraria, entonces todo ideal de $A \otimes_K B$ contiene un elemento de la forma $1_A \otimes b$ con $b \in B$.*

Demostración Sea J un ideal bilátero de $A \otimes_K B$ y sea $u \in J$. Supongamos primero que $u = a \otimes b$ con $a \in A$ y $b \in B$. Observese que las identidades

$$a_1 \otimes b + a_2 \otimes b = (a_1 + a_2) \otimes b, \qquad (a_1 \otimes b)(a_2 \otimes 1) = (a_1 \otimes 1)(a_2 \otimes b) = (a_1 a_2 \otimes b)$$

implican que J debe contener a cada elemento de la forma $(vaw^t) \otimes b$ donde v y w están en A^n. Como 1 puede escribirse de este modo ya que A es simple, se tiene que $(1 \otimes b) \in J$. En el caso general

$$u = \sum_{i=1}^{r} a_i \otimes b_i.$$

Por el argumento anterior se tiene que J contiene a cualquier elemento del tipo

$$u = \sum_{i=1}^{r} (va_i w^t) \otimes b_i,$$

por lo que si escogemos v y w de modo que $va_r w^t = 0$ pero $va_{r-1}w^t \neq 0$, el argumento se concluye por inducción en r. □

Proposición 25.32. *Si A es una K-álgebra central simple y B es una K-álgebra simple, entonces $A \otimes_K B$ es simple.*

Demostración Sea J un ideal bilátero de $A \otimes_K B$. entonces J contiene un elemento de la forma $1 \otimes b$. Por el mismo argumento de la proposición anterior, se tiene que J contiene a $1 \otimes (vbw^t)$ para cada par de vectores v y w en B^n, por lo que $1 \otimes 1$ está en J, ya que B es simple. □

Corolario 25.32.1. *Si A es una K-álgebra central simple, entonces para toda extensión L/K, la L-álgebra $A_L = A \otimes_K L$ es simple.* □

en particular, si D es una K-álgebra de división central de dimensión finita, entonces $D_{\overline{K}}$ es un álgebra de matrices. El siguiente resultado es ahora inmediato.

Corolario 25.32.2. *Si D es una K-álgebra de división central de dimensión finita, entonces la dimensión de D sobre K es un cuadrado perfecto.* □

Chapter 26

Introducción a la teoría de representaciones

definición 26.1. Sea G un grupo. Una representación de G sobre K es una acción de G por transformaciones lineales en un K-espacio vectorial de dimensión finita (que por lo tanto puede identificarse con K^n). Equivalentemente, podemos definir una K-representación de G como un homomorfismo $\rho : G \to \mathrm{GL}_n(K) = \mathbb{M}_n(K)^*$. Un tal homomorfismo puede extenderse de manera única al álgebra de grupo $K[G]$ mediante

$$\rho(\sum_g \alpha_g g) = \sum_g \alpha_g \rho(g).$$

Llamaremos a este homomorfismo una representación del álgebra $K[G]$. Más generalmente, una representación de una K-álgebra A es un homomorfismo de K-álgebras $\phi : A \to \mathbb{M}_n(K)$. Como un homomorfismo de álgebras lleva unidades en unidades, existe una correspondencia entre las representaciones de G y las de $K[G]$. Si $\rho : G \to \mathrm{GL}_n(K)$ es una representación, su caracter es la función $\chi_\rho : G \to K$ definida por

$$\chi_\rho(g) = \mathrm{tr}[\rho(g)].$$

Ejemplo 26.2. Si G es el grupo simétrico S_n, entonces existe una representación de G en K^n dada por

$$\rho(\sigma)(e_i) = e_{\sigma(i)}.$$

Ejemplo 26.3. Mas generalmente, si G actúa en un conjunto finito X, entonces existe una representación de G en el espacio V con base $\{e_x | x \in X\}$ mediante

$$\rho(g)(e_x) = e_{g \cdot x}.$$

En particular, existe una acción natural de G en el espacio vectorial $K[G]$ dada por

$$\rho(g)(h) = gh.$$

Esta recibe el nombre de representación regular de G.

Ejemplo 26.4. El grupo de simetrías lineales de cualquier sólido T en $\mathbb{R}^3$ tiene una representación natural definida extendiendo la acción canónica de G en T a todo $\mathbb{R}^3$.

definición 26.5. Si $\rho_1 : G \to \mathrm{GL}_n(K)$ y $\rho_2 : G \to \mathrm{GL}_m(K)$ son dos representaciones de G, su suma directa es la representación $\rho : G \to \mathrm{GL}_{n+m}(K)$ definida por

$$\rho(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}.$$

Una representación se dice descomponible si es conjugada a una suma directa de dos representaciones de menor dimensión. En otras palabras, una representación ρ de dimensión n es descomponible si existe una matriz $B \in \mathrm{GL}_n(K)$ y dos representaciones ρ_1 y ρ_2, tales que

$$B\rho(g)B^{-1} = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}.$$

Una representación que no es descomponible es indescomponible. Definiciones similares se aplican a representaciones de álgebras.

Nótese que si $\rho : A \to \mathbb{M}_n(K)$ es una representación, K^n puede ser interpretado como un A-módulo mediante la multiplicación $a \cdot v = \rho(a)(v)$. Del mismo modo, si M es un A-módulo de dimensión finita sobre K, entonces la función que lleva a cada elemento $a \in A$ en la función lineal T_a definida por $T_a(v) = a \cdot v$ define una representación si identificamos M con K^n. Esto permite interpretar los conceptos de la teoría de representaciones en términos de módulos.

Proposición 26.6. *Dos representaciones son conjugadas si y sólo si definen módulos isomorfos.*

Demostración si ρ y λ son representaciones conjugadas de dimensión n, entonces existe una matriz $B \in \mathrm{GL}_n(K)$ tal que para todo a en A se tiene $\rho(a) = B\lambda(a)B^{-1}$. Llamemos M_ρ y M_λ a los módulos respectivos (ambos identificados con K^n). Entonces $\phi : M_\lambda \to M_\rho$ definida por $\phi(v) = B(v)$ define un isomorfismo entre ellos, ya que:

$$a \cdot \phi(v) = \rho(a)\phi(v) = B\lambda(a)B^{-1}B(v) = B\lambda(a)(v) = \phi(a \cdot v).$$

Similarmente, si dos módulos M_ρ y M_λ(ambos identificados con K^n) son isomorfos, existe una función lineal $\phi : M_\lambda \to M_\rho$ tal que $\phi(a \cdot v) = a \cdot \phi(v)$ para todo $a \in A$ y todo $v \in M_\lambda$. Si B es la matriz de ϕ con respecto a las bases canónicas de M_ρ y M_λ, esto nos dice que

$$B\lambda(a)(v) = \rho(a)B(v),$$

y como v es arbitrario,

$$B\lambda(a) = \rho(a)B,$$

de donde sigue lo pedido. □

definición 26.7. Un A-módulo M se dice indescomponible si no puede escribirse como suma directa de dos submódulos propios. Si M satisface la condición de cadenas descendentes, entonces es suma de submódulos indescomponibles. Si A es una K-álgebra, todo A-módulo de dimensión finita sobre K es suma de submódulos indescomponibles. En particular, si A tiene dimensión finita sobre K entonces A, visto como un A-módulo, es suma directa de ideales indescomponibles.

Proposición 26.8. *Una representación es irreducible si y sólo si su módulo asociado es irreducible.*

Demostración Basta comprobar, dado que módulos isomorfos son ambos reducibles o ambos irreducibles, que el modulo asociado a la suma directa de dos representaciones es isomorfo a la suma de los módulos asociados a las representaciones menores e inversamente, la representación definida por la suma directa de dos módulos es la suma directa de las representaciones definidas por cada sumando. Ambas afirmaciones son inmediatas de las definiciones. □

Si un A-módulo M tiene una descomposición del tiipo

$$M = \bigoplus_{i=1}^{r} M_i,$$

esta descomposición recibe el nombre de descomposición de Krull-Schmidt de M. Probaremos que tal descomposición es única para módulos que tienen dimensión finita sobre un cuerpo. Para ello necesitaremos algunos lemas previos.

definición 26.9. Un módulo M se dice un LE-módulo (o módulo con anillo de endomrfismos local) si en anillo $\mathrm{End}_A(M)$ es un anillo local.

Probaremos que, de hecho, la descomposición de Krull-Schmidt es única para módulos que son suma directa de LE-módulos. De hecho, los módulos irreducibles de dimensión finita sobre un cuerpo son LE-módulos.

Lema 26.10. *Si en un anillo A cada elemento es invertible o nilpotente, entonces A es local.*

Demostración Basta ver que el conjunto de elementos nilpotentes es un ideal bilátero ya que entonces será el único ideal bilátero maximal. Si a es nilpotente, y si c es un elemento arbitrario de A, entonces ac no puede ser invertible, por lo que debe ser nilpotente. Del mismo modo, si b es un segundo elemento nilpotente, probaremos que $a+b$ no puede ser invertible. Se sigue que es nilpotente y el resultado sigue. Si $a+b$ es invertible, llamemos c a su inverso. Se tiene que ac y bc son nilpotentes y conmutan ya que $bc = (a+b)c - bc = 1 - ac$. Se sigue que $1 = ac + bc$ es nilpotente lo que es imposible. □

Lema 26.11. *Si M es indescomponible y satisface las condiciones de cadenas ascendentes y descendentes para sub-módulos, entonces es un LE-módulo.*

Demostración Basta ver que cada endomorfismo es invertible o nilpotente. Sea $\phi : M \to M$ un tal endomorfismo. Como M satisface ambas condiciones de cadena, las cadenas

$$M \supseteq \phi(M) \supseteq \ldots \supseteq \phi^n(M) \supseteq \ldots, \qquad \{0\} \subseteq \ker(\phi) \subseteq \ldots \subseteq \ker(\phi^n) \subseteq \ldots,$$

se estabilizan. Se sigue que para n suficientemente grande $\phi^n(M) = \phi^{n+1}(M) = \ldots$ y $\ker(\phi^n) = \ker(\phi^{n+1}) = \ldots$. Sea $\alpha = \phi^n$. Entonces $\ker(\alpha) = \ker(\alpha^2)$ y $\alpha(M) = \alpha^2(M)$. Sea $u \in M$. Sea $v \in M$ tal que $\alpha^2(v) = \alpha(u)$ y sea $w = u - \alpha(v)$. Entonces $\alpha(w) = \alpha(u) - \alpha^2(v) = 0$ por lo que $M = \alpha(M) + \ker(\alpha)$. Por otro lado, si $z \in \alpha(M) \cap \ker(\alpha)$, entonces $z = \alpha(y)$

con $\alpha^2(y) = 0$, pero esto implica $z = \alpha(y) = 0$. Se sigue que, de hecho, $M = \alpha(M) \oplus \ker(\alpha)$. Si M es irreducible, uno de estos submódulos debe ser nulo. Si $\alpha(M) = 0$, entonces ϕ es nilpotente. Si $\ker(\alpha) = 0$, entonces α es invertible y como $\phi(\phi^{n-1}\alpha^{-1}) = 1$, también lo es ϕ. □

El final por ahora...