Infierno y Purgatorio
Saga de la Divina Comedia

Universidad de Murcia

Jesús González Abril

November 18, 2025

Contents

Chapter 1

Grupos

1.1 Operaciones binarias

Definition 1.1.1: Operación binaria

Sea X un conjunto. Una operación binaria en X es una aplicación $* : X \times X \to X$. Por lo general escribimos $*(a, b) = a * b$.

Remark. En general, si por el contexto se sobreentiende que una operación es binaria, se simplifica el lenguaje hablando simplemente de operaciones. De igual manera, normalmente se omite el conjunto sobre el que está definida la operación.

Definition 1.1.2: Tipos de operaciones

Una operación $*$ se dice

- **Conmutativa** si $x * y = y * x$ para todo $x, y \in X$.
- **Asociativa** si $x * (y * z) = (x * y) * z$ para todo $x, y, z \in X$.

Definition 1.1.3: Terminología sobre elementos

Un elemento $x \in X$ se dice que es:

- **Neutro por la izquierda (neutro por la derecha)** si $x*y = y$ para todo $y \in X$ ($y*x = y$ para todo $y \in X$).
- **Cancelable por la izquierda (cancelable por la derecha)** si para cada dos elementos distintos $a \neq b$ de X se verifica $x * a \neq x * b$ ($a * x \neq b * x$).
- **Neutro** si es neutro por la derecha y por la izquierda.
- **Cancelable** si es cancelable por la izquierda y por la derecha.

Supongamos que e es un elemento neutro de X con respecto a $*$. Sean x e y elementos de X. Decimos que x es simétrico de y por la izquierda y que y es simétrico de x por la derecha con respecto a $*$ si se verifica $x * y = e$. En este contexto decimos que x es:

- **Simétrico** de y si lo es por ambos lados. En tal caso decimos que x es invertible, siendo y su inverso ($y = x^{-1}$ si el inverso es único).

Example 1.1.4

Si x es cancelable por la izquierda, entonces para cualesquiera $a, b \in X$ se tiene

$$x * a = x * b \implies a = b$$

Proof

Supongamos que $x * a = x * b$, si $a = b$ ya hemos terminado. En caso contrario, a y b son elementos distintos, y, como x es cancelable por la izquierda, entonces debe ser $x*a \neq x*b$, pero eso contradice la suposición inicial, luego ha de ser $a = b$.

Example 1.1.5

Si x es cancelable por la derecha entonces, para cualesquiera $a, b \in X$ se tiene

$$a * x = b * x \implies a = b$$

Remark. Notemos que esta caracterización no es más que el contrarrecíproco de la primera definición que hemos dado de elemento cancelable.

Definition 1.1.6: Tipos de conjuntos con operaciones

Un par $(X, *)$ formado por un conjunto y una operación $*$ decimos que es un:

- **Semigrupo** si $*$ es asociativa.
- **Monoide** si es un semigrupo que tiene un elemento neutro con respecto a $*$.
- **Grupo** si es un monoide y todo elemento de X es invertible con respecto a $*$.
- **Grupo abeliano** si es un grupo y $*$ es conmutativa.

Example 1.1.7

Si tomamos la suma de elementos sobre distintos conjuntos de números obtenemos un ejemplo de cada uno de los tipos de conjuntos con operaciones:

(1) $(\mathbb{N} \setminus \{0\}, +)$ es un semigrupo, ya que la suma es asociativa, pero no tiene neutro.

(2) $(\mathbb{N}, +)$ es un monoide, ya que la suma es asociativa y tiene el 0 como neutro.

(3) $(\mathbb{Z}, +)$ es un grupo, ya que la suma es asociativa, tiene neutro y todos los elementos tienen inverso. De hecho, como la suma es conmutativa es un grupo abeliano.

Example 1.1.8: Grupo no abeliano

Un ejemplo de grupo no abeliano es $GL_n(\mathbb{R})$ si $n \geq 2$. $GL_n(\mathbb{R})$ es el grupo de las matrices invertibles $n \times n$ con entradas reales, donde la operación es la multiplicación de matrices.

Proof

En primer lugar, es inmediato que la operación es asociativa. También es fácil ver que tiene elemento neutro, la matriz identidad I_n. Si tomamos una matriz cualquiera $A \in GL_n(\mathbb{R})$ esta ha de tener inversa, por lo que su elemento inverso es A^{-1} que claramente pertenece a $GL_n(\mathbb{R})$.
Finalmente, para ver que el grupo no es conmutativo notemos que para $n = 2$ podemos tomar las matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

ambas invertibles por tener determinante no nulo, que verifican

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}.$$

En el caso de que sea $n > 2$ podemos tomar matrices de la forma

$$A' = \begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix}, B' = \begin{pmatrix} B & 0 \\ 0 & I_{n-2} \end{pmatrix}$$

cuyo producto no conmuta por las propiedades de la multiplicación de matrices por bloques.

Example 1.1.9

Sean A un conjunto y sea $X = A^A$ el conjunto de las aplicaciones de A en A. Probar que la composición de aplicaciones define una operación asociativa en X para la que la identidad 1_X es neutro. Esto prueba que $(A^A, \circ)$ es un monoide.

Proposition 1.1.10

Sea $*$ una operación en un conjunto X.

(1) Si e es un neutro por la izquierda y f es un neutro por la derecha de X con respecto a $*$, entonces $e = f$. En particular, X tiene a lo sumo un neutro.

(2) Supongamos que $(X, *)$ es un monoide y sea $a \in X$.

  (a) Si x es un simétrico por la izquierda de a e y es un simétrico por la derecha de a, entonces $x = y$. Por tanto, en tal caso a es invertible y tiene a lo sumo un simétrico.

  (b) Si a tiene un simétrico por un lado entonces es cancelable por ese mismo lado. En particular, todo elemento invertible es cancelable.

Proof

(1) Como e es neutro por la izquierda y f es neutro por la derecha tenemos

$$f = e * f = e.$$

(2a) Ahora suponemos que $(X, *)$ es un monoide. Por (1), $(X, *)$ tiene un único neutro que vamos a denotar por e. Como x es inverso por la izquierda de a e y es inverso por la derecha de a, usando la propiedad asociativa, tenemos que

$$y = e * y = (x * a) * y = x * (a * y) = x * e = x.$$

(2b) Supongamos que a es un elemento de X que tiene un inverso por la izquierda b y que $a * x = a * y$ para $x, y \in X$. Usando la asociatividad una vez más concluimos que

$$x = e * x = (b * a) * x = b * (a * x) = b * (a * y) = (b * a) * y = e * y = y.$$

Remark. Por la proposición anterior si X es un monoide cada elemento invertible a tiene un único inverso que denotaremos a^{-1}.

1.1.1 Subconjuntos y operaciones

Sea $*$ una operación en un conjunto A y sea B un subconjunto de A. Decimos que B es cerrado con respecto a $*$ si para todo $a, b \in B$ se verifica que $a * b \in B$. En tal caso podemos considerar $*$ como una operación en B que se dice inducida por la operación en A.

- Un subsemigrupo de un semigrupo es un subconjunto suyo que con la misma operación es un semigrupo.
- Un submonoide de un monoide es un subconjunto suyo que con la misma operación es un monoide con el mismo neutro.
- Un subgrupo de un grupo es un subconjunto suyo que con la misma operación es un grupo.

1.2 Definiciones y ejemplos

Definition 1.2.1: Grupo

Un grupo es una pareja $(G, \cdot)$, formada por un conjunto no vacío G junto con una operación binaria, que denotaremos por $\cdot$, que satisface los siguientes axiomas:

(1) (Asociativa) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in G$.

(2) (Neutro) Existe un elemento $e \in G$, llamado elemento neutro del grupo, tal que $e \cdot a = a = a \cdot e$, para todo $a \in G$.

(3) (Inverso) Para todo $a \in G$ existe otro elemento $a^{-1} \in G$, llamado elemento inverso de a, tal que $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Si además se verifica el siguiente axioma se dice que el grupo es abeliano o conmutativo:

(4) (Conmutativa) $a \cdot b = b \cdot a$, para todo $a, b \in G$.

Demostraremos ahora algunas propiedades de los grupos.

Lemma 1.2.2: Propiedades básicas de grupos

Sea $(G, \cdot)$ un grupo.

(1) (Unicidad del neutro) El neutro de G es único y lo denotaremos e. De hecho, si $a, b \in G$ satisfacen que $a \cdot b = a$ ó $b \cdot a = a$ entonces $b = e$.

(2) (Unicidad del inverso) El inverso de un elemento a de G es único y lo denotaremos a^{-1}. De hecho, si e es el neutro de G y $a, b \in G$ satisfacen $a \cdot b = e$ ó $b \cdot a = e$ entonces $b = a^{-1}$.

(3) (Propiedad Cancelativa) Todo elemento de G es cancelativo.

(4) Para todo $a, b \in G$, las ecuaciones $a \cdot X = b$ y $X \cdot a = b$ tienen una única solución en G.

(5) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Proof

(1) Haremos solo el caso por la derecha, en efecto, si $a \cdot b = a$ entonces

$$b = e \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot a = e.$$

(2) De nuevo hacemos solo el caso $a \cdot b = e$

$$a^{-1} = a^{-1} \cdot e = a^{-1} \cdot a \cdot b = e \cdot b = b.$$

(3) Sea $x \in G$, entonces x debe ser cancelable puesto que en caso contrario existirían $a, b \in G$ con $a \neq b$ tales que $x \cdot a = x \cdot b$, pero entonces

$$a = e \cdot a = x^{-1} \cdot x \cdot a = x^{-1} \cdot x \cdot b = e \cdot b = b$$

una contradicción.

(4) Sean $a, b \in G$ arbitrarios y x, y dos soluciones cualesquiera, entonces

$$x = e \cdot x = a^{-1} \cdot a \cdot x = a^{-1} \cdot b$$

y de igual manera

$$y = e \cdot y = a^{-1} \cdot a \cdot y = a^{-1} \cdot b$$

luego $x = y$. Para la otra ecuación se razona igual. Notemos que también hemos demostrado la existencia de una solución ($x = a^{-1} \cdot b$).

(5) Basta realizar un sencillo cálculo y aplicar el apartado 2

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot b \cdot b^{-1} \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e.$$

1.2.1 Ejemplos

Example 1.2.3: Grupo trivial

Sea X un conjunto y consideremos la aplicación identidad $1_X : X \to X$ tal que $1_X(x) = x$ para todo $x \in X$. Entonces el conjunto $T = \{1_X\}$ con la operación de composición es un grupo $(T, \circ)$ que llamaremos el grupo trivial (lo denotaremos 1).
En general, podríamos haber definido este grupo como un único elemento $\{x\}$ con la operación descrita por $x \cdot x = x$.

Example 1.2.4: Grupo simétrico

Sean X un conjunto y S_X el conjunto de todas las biyecciones de X en sí mismo. Entonces $(S_X, \circ)$ es un grupo, llamado grupo simétrico o grupo de las permutaciones de X.

Proof

Prescindiremos del uso de $\circ$ para simplificar la notación.

(1) Asociativa: sean f, g, h biyecciones, dado $x \in X$ cualquiera

$$((fg)h)x = (fg)(h(x)) = f(g(h(x))) = f(gh(x)) = (f(gh))x \implies (fg)h = f(gh)$$

(2) Neutro: basta considerar la aplicación identidad $\mathrm{id}(x) = x$.

(3) Inverso: claramente el inverso de una biyección cualquiera f es su inversa f^{-1}, que verifica

$$(ff^{-1})(x) = f(f^{-1}(x)) = x$$

luego $ff^{-1} = \mathrm{id}$.

Remark. En general S_X no es un grupo abeliano.

Example 1.2.5: Producto de grupos

Si $(G, *)$ y $(H, *)$ son dos grupos, entonces el producto directo $G \times H$ es un grupo en el que la operación viene dada componente a componente:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 * h_2).$$

Más generalmente, si $(G_i)_{i \in I}$ es una familia arbitraria de grupos, entonces el producto directo $\prod_{i \in I} G_i$ tiene una estructura de grupo en el que el producto se realiza componente a componente. Para más información ver la Definición A.5.1.

Probemos que el producto directo de dos grupos es un grupo:

Proof

(1) Asociativa:

$$((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) = (g_1 * g_2, h_1 * h_2) \cdot (g_3, h_3) = (g_1 * g_2 * g_3, h_1 * h_2 * h_3) = \\ = (g_1, h_1) \cdot (g_2 * g_3, h_2 * h_3) = (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3))$$

donde hemos usado la asociatividad de los grupos G, H.

(2) Neutro: basta considerar el elemento (e_G, e_H) donde e_G es el neutro de G y e_H el de H.

(3) Inverso: claramente el inverso de un elemento cualquiera (g_1, h_1) es (g_1^{-1}, h_1^{-1}), que verifica

$$(g_1, h_1) \cdot (g_1^{-1}, h_1^{-1}) = (g_1 * g_1^{-1}, h_1 * h_1^{-1}) = (e_G, e_H).$$

Example 1.2.6: Tabla de Cayley

Dado un grupo finito podemos construir lo que llamaremos su tabla de Cayley (también llamada tabla de multiplicación o de suma, dependiendo del nombre que le demos a la operación del grupo). Esta tabla se obtiene disponiendo cada uno de los elementos del grupo tanto por columnas como por filas y calculando sus productos. Si el grupo tiene 2 elementos a, b la tabla será de la forma:

$\cdot$	a	b
a	$a \cdot a$	$a \cdot b$
b	$b \cdot a$	$b \cdot b$

Como ejemplo concreto, la tabla del grupo $\mathbb{Z}_3$ (enteros módulo 3) es la siguiente:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

1.2.2 El grupo diédrico

Veamos ahora un grupo con especial significado geométrico. Consideremos un polígono regular de n lados y las transformaciones que lo dejan invariantes (rotaciones y reflexiones), a las que llamaremos simetrías. La composición de dos simetrías de un polígono regular es nuevamente una simetría de este objeto. Considerando la composición de simetrías como operación binaria, esto le da a las simetrías la estructura algebraica de un grupo finito.

La siguiente tabla de Cayley muestra el efecto de la composición en el grupo diédrico de orden 6, D_3 – las simetrías de un triángulo equilátero. Aquí, r_0 denota la identidad, r_1 y r_2 denotan rotaciones en sentido antihorario de 120° y 240° respectivamente, mientras que s_0, s_1 y s_2 denotan reflexiones a través de las tres líneas mostradas en la Figura 1.1.

$\circ$	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

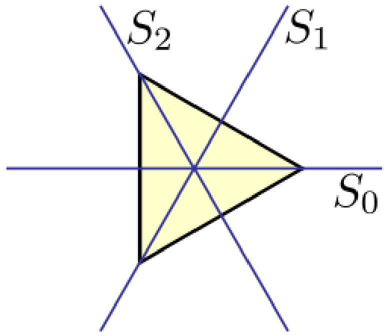

Figure 1.1: Simetrías del triángulo.

Por ejemplo, $s_2 s_1 = r_1$, porque la reflexión s_1 seguida de la reflexión s_2 resulta en una rotación de 120°. El orden de los elementos que denotan la composición es de derecha a izquierda, reflejando la convención de que el elemento actúa sobre la expresión a su derecha. La operación de composición no es conmutativa.

El siguiente ejemplo abstrae y generaliza el concepto de grupo diédrico prescindiendo de la interpretación geométrica.

Example 1.2.7: Grupo diédrico

Para cada número natural positivo n definimos un grupo formado por $2n$ elementos

$$D_n = \{1, a, a^2, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$$

en el que la multiplicación viene dada por la siguiente regla:

$$(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{[i_1+(-1)^{j_1}i_2]_n} b^{[j_1+j_2]_2}$$

donde $[x]_n$ denota el resto de dividir x entre n. Este grupo se llama grupo diédrico de orden $2n$.
El grupo diédrico infinito D_∞ está formado por elementos de la forma $a^n b^m$, con $n \in \mathbb{Z}$ y $m = 0, 1$ con el producto $(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{i_1+(-1)^{j_1}i_2} b^{[j_1+j_2]_2}$.

Si ahora consideramos únicamente las rotaciones que dejan invariante un polígono de n lados obtenemos otro grupo, en este caso con n elementos, cada uno de ellos correspondiente a rotar por un múltiplo de $\frac{360°}{n}$. El siguiente ejemplo abstrae este grupo de rotaciones.

Example 1.2.8: Grupo cíclico

Para cada número natural positivo n definimos un grupo C_n formado por n elementos

$$C_n = \{1, a, a^2, \dots, a^{n-1}\},$$

donde a es un símbolo, y en el que la multiplicación viene dada por la siguiente regla:

$$a^i a^j = a^{[i+j]_n}$$

con notación como en el ejemplo anterior. Este grupo se llama cíclico de orden n.
También definimos el grupo cíclico infinito como el conjunto $C_\infty = \{a^n : n \in \mathbb{Z}\}$, donde a es un símbolo y consideramos $a^n = a^m$ si y solo si $n = m$, y en el que el producto viene dado por $a^n \cdot a^m = a^{n+m}$.

Remark. Es fácil notar la similitud entre C_n y $\mathbb{Z}_n$, así como entre C_∞ y $\mathbb{Z}$. Más tarde formalizaremos esta *intuición probando que estos grupos son equivalentes (isomorfos).*

1.3 Subgrupos

Definition 1.3.1: Subgrupo

Sea G un grupo. Un subconjunto S de G se dice que es un subgrupo si la operación que define la estructura de grupo en G induce también una estructura de grupo en S.

Lemma 1.3.2: Caracterización de subgrupos

Sean G un grupo y S un subconjunto de G. Las siguientes condiciones son equivalentes:

(1) S es un subgrupo de G.

(2) $e \in S$ y para todo $a, b \in S$, se verifican $ab, a^{-1} \in S$.

(3) $S \neq \emptyset$ y para todo $a, b \in S$, se verifican $ab, a^{-1} \in S$.

(4) $e \in S$ y para todo $a, b \in S$, se verifica $ab^{-1} \in S$.

(5) $S \neq \emptyset$ y para todo $a, b \in S$, se verifica $ab^{-1} \in S$.

Proof

$(1) \Rightarrow (2)$: Que $ab \in S$ es inmediato porque S es un grupo, para ver que $a^{-1} \in S$ basta notar que los inversos son únicos: como a debe de tener un inverso en S, este debe coincidir con su inverso en G. Sea $a \in S$, entonces $a^{-1} \in S$, luego $e = aa^{-1} \in S$.
$(2) \Rightarrow (3)$: Inmediato.
$(3) \Rightarrow (4)$: Dado $a \in S$ (existe por hipótesis) tenemos que $a^{-1} \in S$, luego $e = aa^{-1} \in S$. Además, $b^{-1} \in S$, luego $ab^{-1} \in S$.
$(4) \Rightarrow (5)$: inmediato.
$(5) \Rightarrow (1)$: Dado $a \in S$ (existe por hipótesis) tenemos que $aa^{-1} \in S$, luego $e = aa^{-1} \in S$. Este elemento es el neutro de S puesto que el neutro es único. Sea $a \in S$, entonces $ea^{-1} \in S$, luego $a^{-1} \in S$, y este ha de ser el inverso de a puesto que el inverso es único en G.

1.3.1 Ejemplos de subgrupos

Para probar que un conjunto es un subgrupo podemos emplear cualquiera de las caracterizaciones del Lema 1.3.2, usualmente emplearemos (5) por ser la más sencilla.

Example 1.3.3

Si G es un grupo, entonces $\{1\}$ y G son subgrupos de G. El primero se llama subgrupo trivial, denotado 1 y el segundo subgrupo impropio de G. Los subgrupos de G diferentes de G se dice que son subgrupos propios.

Example 1.3.4

Si $(A, +)$ es el grupo aditivo de un anillo, entonces todo subanillo y todo ideal de A son subgrupos de este grupo.

Example 1.3.5: Subgrupos de $\mathbb{Z}$

Si S es un subgrupo de $(\mathbb{Z}, +)$, entonces dado $x \in S$ arbitrario, $x + x \in S$. Por inducción se deduce que $nx \in S$ para todo $n \in \mathbb{Z}$ y todo $x \in S$. Eso implica que S es un ideal de $\mathbb{Z}$ y por tanto los subgrupos de $(\mathbb{Z}, +)$ son los de la forma $n\mathbb{Z}$ para n un entero no negativo.

Example 1.3.6

Sea $GL_n(K)$ el grupo de las matrices invertibles de tamaño n con entradas en el cuerpo K. Entonces el conjunto $SL_n(K)$ formado por las matrices de determinante 1 es un subgrupo de $GL_n(K)$.

Proof

Claramente $SL_n(K)$ es no vacío. Sean $A, B \in SL_n(K)$, entonces $\det(A) = \det(B) = 1$, como además B es invertible sabemos que

$$1 = \det(I) = \det(BB^{-1}) = \det(B)\det(B^{-1}) = \det(B^{-1}),$$

luego

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = 1 \implies AB^{-1} \in SL_n(K)$$

como queríamos ver.

Example 1.3.7: Automorfismos

Supongamos que A es un anillo y sea S_A el grupo de las permutaciones de A. Entonces el conjunto $\mathrm{Aut}(A)$ formado por los automorfismos de A es un subgrupo de S_A.

Proof

$\mathrm{Aut}(A) \neq \emptyset$, dados $f, g \in \mathrm{Aut}(A)$, g^{-1} también es un automorfismo y, como la composición de homomorfismos de anillos es homomorfismo, $fg^{-1} \in \mathrm{Aut}(A)$ al ser un homomorfismo de A en A.

Ejemplos similares se pueden obtener con casi todas las estructuras matemáticas. Por ejemplo, si G es un grupo, entonces decimos que $f : G \to G$ es un automorfismo si f es biyectivo y $f(gh) = f(g)f(h)$ para todo $g, h \in G$. Entonces el conjunto $\mathrm{Aut}(G)$ formado por todos los automorfismos de G es un subgrupo del grupo simétrico S_G de G.

Example 1.3.8

Si X es un espacio topológico entonces el conjunto de todos los homeomorfismos de X de X en si mismo es un subgrupo de S_X. Recuérdese que un homeomorfismo entre dos espacios topológicos es una aplicación biyectiva tal que tanto ella como su inversa son continuas. Si X es un espacio métrico con distancia d, entonces el conjunto de las isometrías es un subgrupo de S_X. Recuérdese que una isometría entre dos espacios métricos es una biyección f de uno al otro verifica $d(f(x), f(y)) = d(x, y)$ para todos los elementos x, y del dominio de f.

Example 1.3.9: Subgrupo cíclico

Si G es un grupo y $g \in G$, entonces

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

es un subgrupo de G, llamado grupo cíclico generado por g.

Proof

Notemos que $e = g^0 \in \langle g \rangle$. Si $a, b \in \langle g \rangle$ entonces $a = g^{n_0}, b = g^{n_1}$ y es obvio que

$$bg^{-n_1} = g^0 = e \implies b^{-1} = g^{-n_1}$$

luego

$$ab^{-1} = g^{n_0} g^{-n_1} = g^{n_0 - n_1} \in \langle g \rangle.$$

Un grupo G se dice que es cíclico si tiene un elemento g tal que $G = \langle g \rangle$. En tal caso se dice que g es un generador de G. Por ejemplo, $(\mathbb{Z}, +)$ es cíclico generado por 1 y $(\mathbb{Z}_n, +)$ es otro grupo cíclico generado por la clase de 1. Otros ejemplos de grupos cíclicos son los grupos C_n y C_∞.

Example 1.3.10

Si X es un subconjunto arbitrario de G, entonces el conjunto formado por todos los elementos de G de la forma $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$, con $x_1, \dots x_m \in X$ y $n_1, \dots, n_m \in \mathbb{Z}$, es un subgrupo de G, que resulta ser el menor subgrupo de G que contiene a X y por tanto se llama subgrupo generado por X y se denota $\langle X \rangle$.

Proof

Sea $x \in X$, entonces $e = x^0 \in \langle X \rangle$. Sean $a, b \in \langle X \rangle$ de la forma

$$a = x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}, b = y_1^{l_1} y_2^{l_2} \dots y_k^{l_k}$$

es inmediato que

$$b(y_k^{-l_k} \dots y_1^{-l_1}) = e \implies b^{-1} = y_k^{-l_k} \dots y_1^{-l_1}$$

y por tanto

$$ab^{-1} = x_1^{n_1} x_2^{n_2} \dots x_m^{n_m} y_k^{-l_k} \dots y_1^{-l_1} = z_1^{j_1} \dots z_{m+k}^{j_k}$$

donde $z_i = x_i, j_i = n_i$ si $1 \leq i \leq m$, $z_i = y_{k+m+1-i}, j_i = l_{k+m+1-i} =$ si $m < i \leq m + k$. Luego $ab^{-1} \in \langle X \rangle$.

Example 1.3.11

El subgrupo generado por X se puede construir de otra forma. Es un sencillo ejercicio comprobar que la intersección de subgrupos de G, es un subgrupo.

Proof

Sean $G_i \subseteq G$ subgrupos de G y sea $H = \cap_{i \in I} G_i$. Entonces $e \in H$ ya que está en cada G_i. Si $a, b \in H$ entonces para todo $i \in I$

$$a, b \in G_i \implies ab^{-1} \in G_i \implies ab^{-1} \in H.$$

Por tanto la intersección de todos los subgrupos de G que contienen a X es un subgrupo de G y es el menor subgrupo de G que contiene a X, con lo que es el subgrupo generado por X.

Example 1.3.12: Suma directa de grupos

Si $(G_i)_{i \in I}$ es una familia arbitraria de grupos, entonces el subconjunto $\oplus_{i \in I} G_i$ formado por los elementos $(g_i) \in \prod_{i \in I} G_i$ tales que $g_i = 1$ para casi todo i, es un subgrupo de $\prod_{i \in I} G_i$.

Proof

El elemento neutro de $\prod_{i \in I} G_i$ está, obviamente, en $\oplus_{i \in I} G_i$. Si $a, b \in \oplus_{i \in I} G_i$ entonces el inverso de $b = (b_i)$ es el elemento $b^{-1} = (c_i) = (b_i^{-1})$, notemos que como $1^{-1} = 1$ casi todo $c_i = 1$, luego $b^{-1} \in \oplus_{i \in I} G_i$ y de hecho

$$ab^{-1} = (d_i)$$

donde todos los $d_i = 1$ salvo un número finito (como mucho, hay tantos distintos de 1 como la suma de los distintos de 1 de a y b). En resumen, $ab^{-1} \in \oplus_{i \in I} G_i$, luego es un subgrupo.

Example 1.3.13: Centro y centralizador

Si G es un grupo arbitrario, entonces

$$Z(G) = \{g \in G : gx = xg, \text{ para todo } x \in G\}$$

es un subgrupo abeliano de G, llamado centro de G. Más generalmente, si $x \in G$, entonces

$$C_G(x) = \{g \in G : gx = xg\}$$

es un subgrupo de G, llamado centralizador de x en G. Observese que $Z(G)$ es la intersección de todos los centralizadores de los elementos de G en G.

Proof

Dado $x \in G$ veamos que $C_G(x)$ es un subgrupo, a partir de esto es fácil ver que $Z(G)$ es un subgrupo abeliano. La identidad está en $C_G(x)$ ya que

$$ex = xe = x,$$

dados $a, b \in C_G(x)$ es fácil ver que

$$b^{-1}x = b^{-1}xbb^{-1} = b^{-1}bxb^{-1} = xb^{-1} \implies b^{-1} \in C_G(x)$$

y, además,

$$abx = axb = xab \implies ab \in C_G(x).$$

1.3.2 Clases laterales

Sea G un grupo y H un subgrupo de G. Se define la siguiente relación binaria en G:

$$a \equiv_i b \mod H \quad \Leftrightarrow \quad a^{-1}b \in H. \qquad (a, b \in G).$$

Se puede comprobar fácilmente que esta relación es de equivalencia y por tanto define una partición de G en clases de equivalencia. La clase de equivalencia que contiene a a es

$$aH = \{ah : h \in H\}$$

y se llama clase lateral de a módulo H por la izquierda.

Análogamente se puede definir otra relación de equivalencia:

$$a \equiv_d b \mod H \quad \Leftrightarrow \quad ab^{-1} \in H. \quad (a, b \in G)$$

para la que las clase de equivalencia que contiene a a es

$$Ha = \{ha : h \in H\}$$

y se llama clase lateral de a módulo H por la derecha.

El conjunto de las clases laterales por la izquierda de G módulo H se denota por G/H y el de clases laterales por la derecha $H\backslash G$.

Como consecuencia del Lema 1.2.2 las aplicaciones

$$\begin{array}{c} H \to aH \\ h \mapsto ah \end{array} \qquad \begin{array}{c} H \to Ha \\ h \mapsto ha \end{array}$$

son biyectivas, con lo que todas las clases laterales tienen el mismo cardinal. Además la aplicación

$$\begin{array}{ccc} G/H & \to & H\backslash G \\ aH & \mapsto & Ha^{-1} \end{array}$$

es otra biyección con lo que también G/H y $H\backslash G$ tienen el mismo cardinal.

Proof

Veamos que $L_a(h) = ah$ es una biyección. Si $ah = bh \implies a = b$ por la propiedad cancelativa, luego es inyectiva. Si $ax \in aH$ entonces $L_a(x) = ax$, luego es sobreyectiva.
En cuanto a $\phi(aH) = Ha^{-1}$ notemos que está bien definida y es inyectiva

$$\phi(aH) = \phi(bH) \iff Ha^{-1} = Hb^{-1} \iff a^{-1}b \in H \iff aH = bH.$$

También es sobreyectiva puesto que dada $Ha^{-1} \in H\backslash G$, $\phi(aH) = Ha^{-1}$.

Denotamos con $|X|$ el cardinal de un conjunto cualquiera. En el caso en que G sea un grupo el cardinal de G se suele llamar orden de G. Acabamos de ver que para cada subgrupo H de G se verifica:

$$|aH| = |Ha| = |H| \quad \text{y} \quad |G/H| = |H\backslash G|$$

El cardinal de G/H (y $H\backslash G$) se llama índice de H en G y se denota $[G : H]$. Una consecuencia inmediata de estas fórmulas es el siguiente Teorema.

Theorem 1.3.14: Teorema de Lagrange

Si G es un grupo finito y H es un subgrupo de G entonces $|G| = |H||G : H|$.

Corollary 1.3.15

Si G es un grupo finito de orden primo entonces los únicos subgrupos de G son 1 y G. En particular G es cíclico y cualquier elemento de G distinto de 1 es un generador de G.

Chapter 2

Anillos

2.1 Anillos

Definition 2.1.1: Anillo

Un anillo es una terna $(A, +, \cdot)$ formada por un conjunto no vacío A y dos operaciones $+$ (suma) y $\cdot$ (producto) en A que verifican:

(1) $(A, +)$ es un grupo abeliano.

(2) $(A, \cdot)$ es un monoide.

(3) Distributiva del producto respecto de la suma: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ para todo $a, b, c \in A$.

Si además $\cdot$ es conmutativo en A, decimos que $(A, +, \cdot)$ es un anillo conmutativo.

Remark.

- *El neutro de A con respecto a $+$ se llama cero y se denota 0.*
- *El neutro de A con respecto a $\cdot$ se llama uno y se denota 1.*
- *El simétrico de un elemento a con respecto a $+$ se llama opuesto y se denota $-a$.*
- *Si a es invertible con respecto a $\cdot$, su simétrico se llama inverso y se denota a^{-1}.*
- *En general para $+$ y $\cdot$ usamos la notación usual para sumas y productos*

$$a \cdot (b + c) = a(b + c) = ab + ac.$$

Como $(A, +)$ es un grupo, todo elemento de A es invertible respecto de la suma y por tanto cancelable. Diremos que un elemento de A es regular en A si es cancelable con respecto al producto. En caso contrario decimos que el elemento es singular en A o divisor de cero. El termino divisor de cero se justifica por lo siguiente. Supongamos que $x \in A$ no es cancelable respecto al producto, en tal caso existen dos elementos distintos $a \neq b$ tales que $ax = bx$. Pero entonces es inmediato que

$$(a - b)x = 0$$

sin embargo, ni $(a - b)$ ni x son cero, por lo que podemos interpretar que ambos son «divisores del cero».

2.1.1 Ejemplos de anillo

Example 2.1.2

Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos conmutativos con la suma y el producto usuales. Notemos que todo elemento no nulo de $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ es invertible. Sin embargo, en $\mathbb{Z}$ solo hay dos elementos invertibles (1 y -1) aunque todos los elementos son regulares menos el 0.

Proof

Demostrar que se trata de anillos conmutativos es muy sencillo, basta comprobar que se verifican todas las propiedades pertinentes.
Probaremos que en $\mathbb{C}$ todos los elementos salvo el 0 son invertibles, el resto de afirmaciones quedan como ejercicio. Sea $z = a + bi$ un número complejo cualquiera no nulo, en tal caso el número $w = \frac{a-bi}{a^2+b^2}$ verifica

$$zw = \frac{(a+bi)(a-bi)}{a^2+b^2} = \frac{a^2 - abi + abi - b(-1)}{a^2+b^2} = \frac{a^2+b^2}{a^2+b^2} = 1$$

luego $w = z^{-1}$ y por tanto z tiene inverso.

Example 2.1.3: Producto de anillos

Sean A y B dos anillos. Entonces el producto cartesiano $A \times B$ tiene una estructura de anillo con las operaciones definidas componente a componente:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

Obsérvese que $A \times B$ es conmutativo si y solo si lo son A y B, y que esta construcción se puede generalizar a productos cartesianos de cualquier familia (finita o no) de anillos.

Example 2.1.4

Dados un anillo A y un conjunto X, el conjunto A^X de las aplicaciones de X en A es un anillo con las siguientes operaciones:

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

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Si definimos la familia de conjuntos $\{A_i = A : i \in X\}$ entonces es inmediato que $\cup_{i \in X} A_i = A$. Recordemos ahora que el producto $\prod_{i \in X} A_i$ es el conjunto de funciones $f : X \to \cup_{i \in X} A_i$, es decir, el conjunto de funciones $f : X \to A$, luego A^X es un anillo correspondiente a un producto «infinito» del anillo A consigo mismo. Para más información ver la Definición A.5.1.

Example 2.1.5: Anillo de polinomios

Dado un anillo A, un polinomio en una indeterminada es una expresión:

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$

donde $n \geq 0$ y $a_i \in A$ para todo i. El conjunto de polinomios con coeficientes en A se denota $A[X]$. La suma y producto en $A[X]$ se definen de la forma usual.

Example 2.1.6: Sucesiones

Dado un anillo A, denotamos por $A[[X]]$ el conjunto de sucesiones $(a_0, a_1, a_2, \ldots)$ de elementos de A. Con las operaciones:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots),$$

$A[[X]]$ es un anillo llamado anillo de series de potencias con coeficientes en A.

2.1.2 Propiedades de los anillos

Lemma 2.1.7

Sea A un anillo y sean $a, b, c \in A$. Se verifican las siguientes propiedades

(1) Todo elemento de A es cancelable respecto de la suma.

(2) Todo elemento invertible de A es regular en A.

(3) Si $b + a = a$ entonces $b = 0$. Si $ba = a$ para todo a, entonces $b = 1$. En particular, el cero y uno son únicos.

(4) El opuesto de a es único y si a es invertible, entonces a tiene un único inverso.

(5) $0a = 0 = a0$.

(6) $a(-b) = (-a)b = -(ab)$.

(7) $a(b - c) = ab - ac$.

(8) a y b son invertibles si y solo si ab y ba son invertibles. En tal caso $(ab)^{-1} = b^{-1}a^{-1}$.

(9) Si $0 = 1$ entonces $A = \{0\}$.

Proof

(1) Como A es un grupo respecto de la suma todo elemento tiene inverso, y por la Proposición 1.1.10 todo elemento invertible (respecto a la suma) es cancelable (respecto a la suma).

(2) De nuevo por la Proposición 1.1.10 todo elemento invertible (respecto al producto) es cancelable (respecto al producto).

(3) Si $b + a = a$ entonces como a es cancelable por el apartado 1, tenemos $b = 0$. Si $ba = a$ para todo a, entonces como el neutro es único $b = 1$.

(4) De nuevo se sigue de la Proposición 1.1.10.

(5) Basta aplicar un pequeño truco

$$0a = (0+0)a = 0a + 0a \implies 0 = 0a$$

para el caso $a0$ se procede igual.

(6) Basta notar que

$$ab + a(-b) = a(b-b) = 0, ab + (-a)b = (a-a)b = 0 \implies -(ab) = a(-b) = (-a)b$$

ya que los opuestos son únicos.

(7) $a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-ac) = ab - ac$.

(8) En primer lugar si a, b son invertibles entonces existen a^{-1}, b^{-1} y es fácil ver que

$$ab(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab, ba(a^{-1}b^{-1}) = e = (a^{-1}b^{-1})ba$$

luego ab, ba son invertibles. Para el recíproco, si ab, ba son invertibles entonces

$$a(b(ab)^{-1}) = ab(ab)^{-1} = e, ((ba)^{-1}b)a = (ba)^{-1}ba = e$$

por tanto, por la Proposición 1.1.10 ambos simétricos $b(ab)^{-1}, (ba)^{-1}b$ son iguales (ambos son a^{-1}) y a es invertible. Para ver que b es invertible se procede igual.

(9) Si $0 = 1$ entonces dado $x \in A$ tenemos

$$x = x1 = x0 = 0 \implies A = \{0\}.$$

Dados un anillo A, un elemento $a \in A$ y un entero positivo n, la notación na (respectivamente a^n) representa el resultado de sumar (respectivamente multiplicar) a consigo mismo n veces, y si $n = 0$ convenimos que $0a = 0$ y $a^0 = 1$. Más rigurosamente, a partir de estas últimas igualdades se definen na y a^n de forma recurrente poniendo $(n+1)a = a + na$ y $a^{n+1} = aa^n$ para $n \geq 0$. Por último, si $n \geq 1$ se define $(-n)a = -(na)$, y si además a es invertible se define $a^{-n} = (a^{-1})^n$.

Lemma 2.1.8

Sea A un anillo, $a, b \in A$, y $m, n \in \mathbb{Z}$. Se verifican:

(1) $n(a+b) = na + nb$.

(2) $(n+m)a = na + ma$.

(3) Si $n, m \geq 0$, entonces $a^{n+m} = a^n a^m$. Si a es invertible, la igualdad vale para n, m arbitrarios.

(4) Si A es conmutativo y $n \geq 0$, entonces $(ab)^n = a^n b^n$. Si a y b son invertibles, la igualdad vale para todo n.

Proof

(1) Por inducción: el caso base $n = 0$ es inmediato, si lo suponemos para n entonces

$$(n+1)(a+b) = (a+b) + na + nb = (n+1)a + (n+1)b.$$

(2) Basta aplicar recursivamente que $(n+1)a = a + na$.

(3) Basta aplicar recursivamente que $a^{n+1} = aa^n$. Si a es invertible entonces podemos usar que $a^{-n} = (a^{-1})^n$ distinguiendo casos. Por ejemplo si $n > 0, m < 0, n > m$

entonces
$$a^n a^m = a^n (a^{-1})^{-m} = a^{n+m} a^{-m} (a^{-1})^{-m} = a^{n+m}.$$

(4) Por inducción: el caso base $n = 0$ es inmediato, si lo suponemos para n entonces
$$(ab)^{n+1} = ab(ab)^n = aba^n b^n = aa^n bb^n = a^{n+1} b^{n+1}.$$
Cuando a y b son invertibles, si $n < 0$
$$(ab)^n = ((ab)^{-1})^{-n} = (b^{-1} a^{-1})^{-n} = (b^{-1})^{-n} (a^{-1})^{-n} = b^n a^n.$$

2.2 Subanillos

Remark. A partir de ahora supondremos que todos los anillos que aparecen son conmutativos.

Sea $*$ una operación en un conjunto A y sea B un subconjunto de A. Decimos que B es cerrado con respecto a $*$ si para todo $a, b \in B$ se verifica que $a * b \in B$. En tal caso podemos considerar $*$ como una operación en B que se dice inducida por la operación en A.

Definition 2.2.1: Subanillo

Un subanillo de un anillo es un subconjunto suyo que con la misma suma y producto es un anillo con el mismo uno.

Proposition 2.2.2: Caracterización de subanillos

Las siguientes condiciones son equivalentes para $B \subseteq A$:

(1) B es un subanillo de A.

(2) B contiene al 1 y es un anillo, luego es cerrado para sumas, productos y opuestos.

(3) B contiene al 1 y es cerrado para restas y productos.

Proof

$(1) \implies (2)$: Si B es un subanillo de A entonces contiene al 1 y es cerrado para sumas y productos. Por otro lado, como B es un anillo, tiene un cero, que de momento denotamos 0_B y cada elemento $b \in B$ tiene un opuesto en B. En realidad $0_B + 0_B = 0_B = 0 + 0_B$, con lo que aplicando la propiedad cancelativa de la suma deducimos que $0_B = 0$, o sea, el cero de A está en B y por tanto es el cero de B (el único que puede tener). Por la unicidad del opuesto, el opuesto de b ha de ser el de A, con lo que B es cerrado para opuestos.
$(2) \implies (3)$: Inmediato.
$(3) \implies (1)$: Si B contiene al 1 y es cerrado para restas, entonces $0 = 1 - 1 \in B$, y para $b \in B$, $-b = 0 - b \in B$. Además, $a + b = a - (-b) \in B$, luego B es cerrado para sumas, por tanto, es un subanillo de A.

Example 2.2.3: Subanillo impropio

Todo anillo A es un subanillo de si mismo, al que llamamos impropio por oposición al resto de subanillos, que se dicen propios.

Example 2.2.4

En la cadena de contenciones $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ cada uno es un subanillo de los posteriores.

Example 2.2.5

Si A es un anillo, el subconjunto $\{0\}$ es cerrado para sumas, productos y opuestos. Si $A = \{0\}$ entonces $\{0\}$ sería subanillo de A, pero este es el único caso en el que esto pasa pues en todos los demás casos $1 \neq 0$.
En efecto si $1 = 0$ entonces para cualquier $a \in A$, $a = 1a = 0a = 0 \implies A = \{0\}$.

Example 2.2.6

Si A y B son anillos entonces $A \times \{0\}$ es un anillo, pero no es un subanillo de $A \times B$ porque no contiene a $(1_A, 1_B)$.
De igual manera, $A \times \{1_B\}$ con las operaciones

$$(a, 1_B) + (b, 1_B) = (a + b, 1_B), \quad (a, 1_B) \cdot (b, 1_B) = (ab, 1_B)$$

es un anillo, pero no es subanillo de $A \times B$ porque las operaciones no son las inducidas por la operaciones de $A \times B$.

Proof

Veamos que $A \times \{1_B\}$ es un anillo con las operaciones indicadas. Claramente es un grupo abeliano para la suma con $-(a, 1_B) = (-a, 1_B)$. También es un monoide para el producto con neutro $(1_A, 1_B)$ ya que $(1_A, 1_B)(a, 1_B) = (a, 1_B)$. Finalmente la conmutatividad es fácil de comprobar gracias a que A es un anillo

$$\begin{aligned}(a, 1_B)[(b, 1_B) + (c, 1_B)] &= (a, 1_B)(b + c, 1_B) = (ab + ac, 1_B) \\ &= (ab, 1_B) + (ac, 1_B) = (a, 1_B)(b, 1_B) + (a, 1_B)(c, 1_B).\end{aligned}$$

Example 2.2.7: Subanillo primo

Si A es un anillo entonces el conjunto:

$$\mathbb{Z}1 = \{n1 : n \in \mathbb{Z}\}$$

es un subanillo de A contenido en cualquier otro subanillo de A.
Este se conoce como el subanillo primo de A.

Remark. *$\mathbb{Z}$ y los $\mathbb{Z}_n$ son sus propios subanillos primos, por tanto, no tienen subanillos propios.*

Example 2.2.8

Dado un número entero m, los conjuntos:

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$$
$$\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$$

son subanillos de $\mathbb{C}$.
Observaciones:

- Si $m > 0$, ambos son subanillos de $\mathbb{R}$
- Si m es un cuadrado perfecto, estos conjuntos coinciden con $\mathbb{Z}$ y $\mathbb{Q}$ respectivamente
- Cuando m no es cuadrado perfecto, la igualdad $a + b\sqrt{m} = 0$ implica $a = 0$ y $b = 0$

Caso particular importante:

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ con $i = \sqrt{-1}$ es el anillo de los enteros de Gauss

Example 2.2.9

Todo anillo A puede verse como un subanillo del anillo de polinomios $A[X]$ identificando los elementos de A con los polinomios constantes (del tipo $P = a_0$).

Example 2.2.10: Diagonal

Sea A un anillo y X un conjunto. Entonces la diagonal:

$$B = \{f \in A^X : f(x) = f(y) \text{ para todo } x, y \in X\}$$

(es decir, el conjunto de las aplicaciones constantes de X en A) es un subanillo de A^X.

Proof

Claramente B contiene a la aplicación $1 : A \to X$ dada por $1(x) = 1_A$, $\forall x \in X$. Es fácil notar que esta aplicación es el elemento neutro del producto en A^X. Sean $f, g \in B$, entonces $h = f - g$ está en B ya que

$$\forall x, y \in X \quad h(x) = f(x) - g(x) = f(y) - g(y) = h(y)$$

luego B es cerrado para restas, de igual manera sea $H = fg$, entonces

$$\forall x, y \in X \quad H(x) = f(x)g(x) = f(y)g(y) = H(y)$$

lo que prueba que B es cerrado para productos. Por tanto, por 2.2.2 B es un subanillo de A^X.

Example 2.2.11

Sea $A = M_n(B)$, donde B es un anillo. Son subanillos:

- El conjunto de las matrices diagonales
- El conjunto de las matrices escalares: $\{aI_n : a \in B\}$
- El conjunto de las matrices triangulares superiores

Example 2.2.12

Sea $A = B \times B$, con B un anillo. Son subanillos:

- $A_1 = \{(b, b) : b \in B\}$ (la diagonal)
- $A_2 = B_1 \times B_2$, donde B_1 y B_2 son subanillos de B

Example 2.2.13

Sea A un anillo cualquiera y B un subanillo de A. Para $\alpha \in A$, el conjunto:

$$A_1 = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n : n \geq 0, a_0, a_1, \ldots, a_n \in B\}$$

es un subanillo de A llamado subanillo generado por B y α.

2.3 Homomorfismos de anillos

Definition 2.3.1: Homomorfismo de anillos

Sean A y B dos anillos. Un homomorfismo de anillos entre A y B es una aplicación $f : A \to B$ que satisface:

(1) $f(x + y) = f(x) + f(y)$

(2) $f(x \cdot y) = f(x) \cdot f(y)$

(3) $f(1) = 1$

Un isomorfismo es un homomorfismo biyectivo. Dos anillos A y B son isomorfos ($A \cong B$) si existe un isomorfismo entre ellos.

Remark. En la definición anterior hemos usado el mismo símbolo para las operaciones en ambos anillos, pero es importante notar que:

- *En* $f(x + y)$*, la suma se realiza en* A
- *En* $f(x) + f(y)$*, la suma se realiza en* B
- *Lo mismo aplica para el producto*

Definition 2.3.2: Tipos de homomorfismos

- Un endomorfismo es un homomorfismo de un anillo en sí mismo.
- Un isomorfismo es un homomorfismo biyectivo.
- Un automorfismo es un isomorfismo de un anillo en sí mismo.

Example 2.3.3

Si $B = \{0\}$ entonces la aplicación $f(a) = 0_B, \forall a \in A$ es un homomorfismo. Si $B \neq \{0\}$ entonces f no es un homomorfismo ya que $f(1) = 0_B \neq 1_B$.

Proposition 2.3.4: Propiedades básicas

Sea $f : A \to B$ un homomorfismo de anillos. Entonces para todo $a, b, a_1, \ldots, a_n \in A$ se verifica:

(1) $f(0_A) = 0_B$

(2) $f(-a) = -f(a)$

(3) $f(a - b) = f(a) - f(b)$

(4) $f(a_1 + \cdots + a_n) = f(a_1) + \cdots + f(a_n)$

(5) $f(na) = nf(a)$ para todo $n \in \mathbb{Z}$

(6) Si a es invertible en A, entonces $f(a)$ es invertible en B y $f(a^{-1}) = f(a)^{-1}$

(7) $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$

Proof

En la mayoría de apartados usaremos los anteriores.

(1) $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$, luego por cancelación en B, $f(0_A) = 0_B$.

(2) $f(a) + f(-a) = f(a + (-a)) = f(0_A) = 0_B$, luego $f(-a) = -f(a)$.

(3) $f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b)$.

(4) Por inducción, el caso $n = 2$ es inmediato. Si lo suponemos cierto para n entonces

$$f(a_1 + \cdots + a_{n+1}) = f(a_1 + \cdots a_n) + f(a_{n+1}) = f(a_1) + \cdots + f(a_n) + f(a_{n+1}).$$

(5) Por inducción, el caso $n = 1$ es inmediato. Si lo suponemos cierto para n entonces

$$f((n+1)a) = f(na + a) = f(na) + f(a) = nf(a) + f(a) = (n+1)f(a).$$

(6) Si a es invertible $aa^{-1} = 1_A$, luego $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$, por tanto $f(a^{-1}) = f(a)^{-1}$.

(7) Por inducción, el caso $n = 1$ es inmediato. Si lo suponemos cierto para n entonces

$$f(a_1 \cdots a_{n+1}) = f(a_1 \cdots a_n)f(a_{n+1}) = f(a_1) \cdots f(a_n)f(a_{n+1}).$$

Definition 2.3.5: Núcleo e imagen

Sea $f : A \to B$ un homomorfismo de anillos. Definimos:

- El núcleo de f: $\ker f = \{a \in A : f(a) = 0_B\}$
- La imagen de f: $\operatorname{Im} f = \{f(a) \in B : a \in A\}$

Resulta interesante ahora estudiar algunas propiedades del núcleo y la imagen, en concreto, su relación con los ideales (ver 2.4.1).

Proposition 2.3.6: Propiedades del núcleo e imagen

Sea $f : A \to B$ un homomorfismo de anillos. Entonces:

(1) $\ker f$ es un ideal de A

(2) $\operatorname{Im} f$ es un subanillo de B

(3) f es inyectivo si y solo si $\ker f = \{0_A\}$

(4) f es sobreyectivo si y solo si $\operatorname{Im} f = B$

Proof

(1) Para ver que $\ker f$ es un ideal:

- $0_A \in \ker f$ pues $f(0_A) = 0_B$, luego $\ker f$ es no vacío.
- Si $x, y \in \ker f$, entonces $f(x+y) = f(x)+f(y) = 0_B + 0_B = 0_B$, luego $x+y \in \ker f$.
- Si $x \in \ker f$ y $a \in A$, entonces $f(ax) = f(a)f(x) = f(a)0_B = 0_B$, luego $ax \in \ker f$

(2) Basta notar lo siguiente:

- $1_B = f(1_A) \in \operatorname{Im} f$.
- Si $a, b \in \operatorname{Im} f$, entonces $f(x) = a, f(y) = b$ para ciertos $x, y \in A$, luego $a - b = f(x) - f(y) = f(x - y) \in \operatorname{Im} f$.
- Si $a, b \in \operatorname{Im} f$, entonces $f(x) = a, f(y) = b$ para ciertos $x, y \in A$, luego $ab = f(x)f(y) = f(xy) \in \operatorname{Im} f$.

(3) Si f es inyectivo y $x \in \ker f$, entonces $f(x) = 0_B = f(0_A)$, luego $x = 0_A$. Recíprocamente, si $\ker f = \{0_A\}$ y $f(a) = f(b)$, entonces $f(a-b) = 0_B$, luego $a-b \in \ker f = \{0_A\}$, por tanto $a = b$.

(4) Es inmediato.

2.3.1 Ejemplos de homomorfismos

Example 2.3.7: Homomorfismo inclusión

Si B es un subanillo de A, la aplicación inclusión $i : B \hookrightarrow A$ dada por $i(b) = b$ es un homomorfismo inyectivo ya que $\ker i = \{0\}$.

Example 2.3.8: Homomorfismo proyección

Si I es un ideal de A, la proyección canónica $\eta : A \to A/I$ dada por $\pi(a) = a + I$ es un homomorfismo suprayectivo con $\ker \eta = I$.

Remark. Usamos indiscriminadamente η o p para denominar a esta proyección canónica.

Example 2.3.9: Homomorfismo de sustitución

Sea A un anillo y $b \in A$. La aplicación $\varphi_b : A[X] \to A$ dada por:

$$\varphi_b(a_0 + a_1 X + \cdots + a_n X^n) = a_0 + a_1 b + \cdots + a_n b^n$$

es un homomorfismo suprayectivo llamado homomorfismo de sustitución en b. Para ver que es suprayectivo notemos que dado $a \in A$ el polinomio $a = aX^0 \in A[X]$, luego $\eta(aX^0) = a$.

Example 2.3.10: Homomorfismo único $\mathbb{Z} \to A$

Para cualquier anillo A, existe un único homomorfismo $f : \mathbb{Z} \to A$ dado por $f(n) = n1_A$.

Example 2.3.11: Conjugación en $\mathbb{C}$

La conjugación compleja $f : \mathbb{C} \to \mathbb{C}$ dada por $f(a + bi) = a - bi$ es un automorfismo de $\mathbb{C}$. Claramente es inyectivo ($f(z) = 0 \iff z = 0 \implies \ker f = \{0\}$) y también sobreyectivo.

2.3.2 Propiedades de los homomorfismos

Proposition 2.3.12: Composición de homomorfismos

Si $f : A \to B$ y $g : B \to C$ son homomorfismos de anillos, entonces la composición $g \circ f : A \to C$ es un homomorfismo de anillos.

Proof

Claramente $g \circ f(1) = g(f(1)) = g(1) = 1$. Para la suma

$$g \circ f(x+y) = g(f(x+y)) = g(f(x)+f(y)) = g(f(x)) + g(f(y)) = g \circ f(x) + g \circ f(y)$$

y para el producto

$$g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = g \circ f(x) g \circ f(y).$$

Proposition 2.3.13: Propiedades de isomorfismos

(1) La composición de isomorfismos es un isomorfismo.

(2) Si $f : A \to B$ es un isomorfismo, entonces $f^{-1} : B \to A$ es un isomorfismo.

(3) La relación «ser isomorfo» es una relación de equivalencia en la clase de todos los anillos.

Proof

(1) La composición de homomorfismos es homomorfismo y la composición de aplicaciones biyectivas es biyectiva.

(2) Claramente $f^{-1}(1) = 1$. Para la suma

$$f(f^{-1}(x+y)) = x + y = f(f^{-1}(x)) + f(f^{-1}(y)) = f(f^{-1}(x) + f^{-1}(y))$$

luego por la inyectividad de f debe ser $f^{-1}(x+y) = f^{-1}(x) + f^{-1}(y)$. Para el producto hacemos el mismo truco

$$f(f^{-1}(xy)) = xy = f(f^{-1}(x))f(f^{-1}(y)) = f(f^{-1}(x)f^{-1}(y))$$

luego por la inyectividad de f tenemos $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$.

(3) Resumidamente

- Reflexividad: basta considerar la identidad id que es isomorfismo.
- Simetría: si $A \cong B$ entonces existe $f : A \to B$ isomorfismo, luego $f^{-1} : B \to A$ es isomorfismo y, por tanto, $B \cong A$.
- Transitividad: se sigue de que la composición de isomorfismos es isomorfismo.

Proposition 2.3.14: Preservación de subestructuras

Sea $f : A \to B$ un homomorfismo de anillos.

(1) Si A_1 es un subanillo de A, entonces $f(A_1)$ es un subanillo de B

(2) Si B_1 es un subanillo de B, entonces $f^{-1}(B_1)$ es un subanillo de A

(3) Si I es un ideal de B, entonces $f^{-1}(I)$ es un ideal de A

(4) Si f es sobreyectivo e I es un ideal de A, entonces $f(I)$ es un ideal de B.

Proof

(1) Como A_1 es subanillo contiene al uno, luego $f(A_1)$ también, que es cerrado para restas y productos es inmediato.

(2) Como B_1 es subanillo contiene al uno, luego $f^{-1}(B_1)$ también. Sean $x, y \in f^{-1}(B_1)$, es cerrado para restas ya que

$$f(x-y) = f(x) - f(y) \in B_1 \implies x - y \in f^{-1}(B_1)$$

al ser B_1 cerrado para restas. Para el producto se razona igual.

(3) Si I es un ideal contiene al 0, luego $f^{-1}(I)$ es no vacío. Si $x, y \in f^{-1}(I)$ entonces $f(x), f(y) \in I$, por tanto, $f(x+y) = f(x) + f(y) \in I$ y finalmente $x + y \in f^{-1}(I)$. De igual manera, sea $a \in A$, entonces

$$f(ax) = f(a)f(x) \in I \implies ax \in f^{-1}(I)$$

ya que $f(a) \in B$ e I es un ideal.

(4) Claramente $f(I)$ es no vacío ya que $0 \in I \implies f(0) \in f(I)$. Si $x, y \in f(I)$, entonces, $x = f(a), y = f(b)$ y

$$x + y = f(a) + f(b) = f(a+b) \in f(I)$$

ya que $a+b \in I$ al ser ideal. Para el producto necesitaremos la sobreyectividad, dado $z \in B$ entonces existe $c \in A$ tal que $z = f(c)$, luego

$$zx = f(c)f(a) = f(ca) \in f(I)$$

porque $ca \in I$ al ser ideal.

Remark. La imagen de un ideal por un homomorfismo no necesariamente es un ideal si el homomorfismo no es suprayectivo.

Example 2.3.15: Contraejemplo

Sea $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ la inclusión. El conjunto $2\mathbb{Z}$ es un ideal de $\mathbb{Z}$, pero $i(2\mathbb{Z}) = 2\mathbb{Z}$ no es un ideal de $\mathbb{Q}$, pues por ejemplo $\frac{1}{2} \in \mathbb{Q}$ y $2 \in 2\mathbb{Z}$, pero $\frac{1}{2} \cdot 2 = 1 \notin 2\mathbb{Z}$ en $\mathbb{Q}$.

Theorem 2.3.16: Homomorfismos en productos

Sean A, B, C anillos. Existe una biyección natural Φ tal que

$$\mathrm{Hom}(A, B \times C) \cong \mathrm{Hom}(A, B) \times \mathrm{Hom}(A, C)$$

dada por $f \mapsto (\pi_B \circ f, \pi_C \circ f)$, donde π_B y π_C son las proyecciones canónicas.

Example 2.3.17: Aplicación

Para determinar todos los homomorfismos $f : \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3$, basta determinar los homomorfismos $\mathbb{Z} \to \mathbb{Z}_2$ y $\mathbb{Z} \to \mathbb{Z}_3$ por separado.

Proof

Si $f : \mathbb{Z} \to \mathbb{Z}_2$ es un homomorfismo entonces

$$f(1) = [1]_2, f(n) = nf(1) = n[1]_2 = [n]_2$$

luego solo existe un homomorfismo de ese tipo.
Similarmente, si $f : \mathbb{Z} \to \mathbb{Z}_3$ es un homomorfismo entonces

$$f(1) = [1]_3, f(n) = nf(1) = n[1]_3 = [n]_3$$

por tanto este homomorfismo también esta totalmente determinado.
Finalmente deducimos que el único homomorfismo de $\mathbb{Z}$ a $\mathbb{Z}_2 \times \mathbb{Z}_3$ es

$$g(n) = ([n]_2, [n]_3).$$

2.4 Ideales y anillos cociente

Supongamos que queremos construir un anillo cociente A/I que herede la estructura algebraica de A. Para ello, necesitamos definir una relación de equivalencia compatible con las operaciones del anillo. Si consideramos $(A, +)$ como grupo abeliano bajo la suma, para formar el grupo cociente $(A/I, +)$ necesitamos que I sea un subgrupo normal de $(A, +)$. Como A es abeliano, todo subgrupo es normal, por lo que basta con que I sea un subgrupo de $(A, +)$, es decir:

- $0 \in I$
- Si $a, b \in I$, entonces $a + b \in I$
- Si $a \in I$, entonces $-a \in I$

Esto nos permite definir el grupo cociente $(A/I, +)$ con la operación:

$$(a + I) + (b + I) = (a + b) + I$$

que está bien definida gracias a que I es subgrupo.

Sin embargo, para que A/I herede la estructura de anillo, necesitamos definir también una multiplicación. La definición natural sería:

$$(a + I)(b + I) = ab + I$$

Sin embargo, debemos verificar que esta operación esta bien definida. Supongamos que tomamos diferentes representantes de las clases:

$$a + I = a' + I, \quad b + I = b' + I$$

esto significa que

$$a - a' \in I \quad \text{y} \quad b - b' \in I.$$

Para que el producto esté bien definido, debemos tener:

$$ab + I = a'b' + I$$

es decir

$$ab - a'b' \in I.$$

Finalmente observemos que:

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'$$

Como $b - b' \in I$ y $a - a' \in I$, para garantizar que $ab - a'b' \in I$, necesitamos que:

(1) Si $x \in I$ y $a \in A$, entonces $ax \in I$

(2) Si $x \in I$ y $a \in A$, entonces $xa \in I$

En un anillo conmutativo, estas dos condiciones son equivalentes. Esto nos lleva a la siguiente definición.

Definition 2.4.1: Ideal

Un subconjunto I de un anillo A es un ideal si:

(1) $I \neq \emptyset$

(2) Para todo $x, y \in I$, se verifica que $x + y \in I$

(3) Para todo $x \in I$ y $a \in A$, se verifica que $ax \in I$

Si I es un ideal de A escribiremos $I \leq A$.

Remark.

- *La condición* $I \neq \emptyset$ *puede sustituirse por* $0 \in I$, *ya que si* $a \in I$ *entonces* $0 = a + (-1)a \in I$.
- *Si* I *es un ideal de* A, *entonces para todo* $a_1, \ldots, a_n \in A$ *y* $x_1, \ldots, x_n \in I$ *se tiene que* $\sum_{i=1}^n a_i x_i \in I$.
- *Todo ideal es un grupo respecto de la suma.*

Example 2.4.2: Ideales triviales

- El ideal cero: $\{0\}$
- El ideal impropio: A

Todo aquel ideal que no sea impropio, es decir, que verifique $I \leq A, I \neq A$ se llama ideal propio. En ocasiones nos interesará trabajar solo con ideales que sean propios, por lo que resulta muy útil caracterizar aquellos que no lo son.

Lemma 2.4.3: Caracterización de ideales impropios

Sea A un anillo. Para un ideal $I \leq A$, las siguientes condiciones son equivalentes:

(1) $I = A$, es decir, I es un ideal impropio.

(2) $1 \in I$

(3) I contiene una unidad de A (i.e., $I \cap A^* \neq \emptyset$)

Proof

- (1) $\implies$ (2): si $I = A$, entonces $1 \in I$
- (2) $\implies$ (3): 1 es una unidad
- (3) $\implies$ (1): si $u \in I \cap A^*$, entonces $1 = uu^{-1} \in I$, luego $I = A$

2.4.1 Ejemplos de ideales

Example 2.4.4: Ideales principales

Sea A un anillo y $b \in A$. El conjunto:

$$(b) = bA = \{ba : a \in A\}$$

es un ideal de A llamado ideal principal generado por b.
Observaciones:

- $(1) = A$
- $(0) = \{0\}$
- (b) es el menor ideal de A que contiene a b

Example 2.4.5: Ideal generado por un conjunto

Sea $T \subseteq A$. El ideal generado por T es:

$$(T) = \left\{ \sum_{i=1}^{n} a_i t_i : n \geq 0, a_i \in A, t_i \in T \right\}$$

Este es el menor ideal de A que contiene a T.

Remark. Frecuentemente, cuando el conjunto sea finito escribiremos

$$(\{x_1, x_2, \ldots, x_n\}) = (x_1, x_2, \ldots, x_n)$$

Example 2.4.6: Ideales en anillos producto

Si A y B son anillos, entonces $A \times \{0\} = \{(a, 0) : a \in A\}$ es un ideal de $A \times B$.

Proof

Claramente es no vacío. Si $x, y \in A \times \{0\}$ entonces

$$x = (a, 0),\ y = (b, 0) \implies x + y = (a + b, 0) \in A \times \{0\}.$$

Si $(a', b') \in A \times B$ entonces

$$(a', b')x = (a', b')(a, 0) = (aa', 0) \in A \times \{0\}.$$

Example 2.4.7: Ideales en anillos de polinomios

Sea $A[X]$ el anillo de polinomios.

- $I = \{a_1 X + \cdots + a_n X^n : a_i \in A\}$ (polinomios sin coeficiente independiente) es un ideal
- Si I es ideal de A, entonces $J = \{a_0 + a_1 X + \cdots + a_n X^n : a_0 \in I\}$ es un ideal de $A[X]$
- $I[X] = \{a_0 + a_1 X + \cdots + a_n X^n : a_i \in I\}$ es un ideal de $A[X]$

Proof

- Que I es no vacío es inmediato. Si $P, Q \in I$ entonces son de la forma

  $$P = a_1 X + \cdots + a_n X^n,\ Q = b_1 X + \cdots + b_m X^m$$

  donde podemos suponer sin pérdida de generalidad que $m \geq n$, luego definiendo $c_k = a_k + b_k$ (tomando $a_k = 0$ si $k > n$) tenemos

  $$P + Q = c_1 X + \cdots + c_m X^m \in I.$$

  De igual manera, el producto de polinomios sin término independiente es un polinomio sin término independiente. Sea $d_0, d_1 = 0, d_k = \sum_{i+j=k} a_i b_j$

  $$PQ = a_1 b_1 X^2 + \cdots + a_n b_m X^{n+m} = d_2 X^2 + \cdots + d_{n+m} X^{n+m} \in I.$$

- Como I es no vacío existe $y \in I$, luego el polinomio $y = yX^0 \in J$ y J es no vacío. Dados $P, Q \in J$ su suma es el polinomio con coeficientes obtenidos sumando los de

P y Q, como ambos coeficientes independiente están en I, que es un ideal, su suma también está en I, luego $P + Q \in J$. Para el producto, notemos que el coeficiente independiente de PQ es el producto de dos elementos de I, luego está en I y por tanto $PQ \in J$.

- Como I es no vacío existe $y \in I$, luego el polinomio $y = yX^0 \in I[X]$ e $I[X]$ es no vacío. Dados $P, Q \in I[X]$ su suma es el polinomio con coeficientes obtenidos sumando los de P y Q, como estos coeficientes están en I, que es un ideal, su suma también está en I, luego $P + Q \in I[X]$. Para el producto, notemos que los coeficientes de PQ son combinaciones de elementos obtenidos como producto de dos elementos de I, luego los coeficientes de PQ están en I y por tanto $PQ \in I[X]$.

Proposition 2.4.8: Intersección de ideales

La intersección de cualquier familia de ideales de A es un ideal de A.

Proof

Si I_α es una familia de ideales indexada por X y $J = \cap_{\alpha \in X} I_\alpha$ entonces

$$0 \in I_\alpha \ \forall \alpha \in X \implies 0 \in J \implies J \neq \emptyset$$

Además,

$$x, y \in J \implies x, y \in I_\alpha \ \forall \alpha \in X \implies x + y \in I_\alpha \ \forall \alpha \in X \implies x + y \in J$$

y para cualquier $a \in A$

$$x \in J \implies x \in I_\alpha \ \forall \alpha \in X \implies ax \in I_\alpha \ \forall \alpha \in X \implies ax \in J.$$

Proposition 2.4.9: Ideales de $\mathbb{Z}$

Todos los ideales de $\mathbb{Z}$ son principales. Es decir, para todo ideal $I \subset \mathbb{Z}$, existe $n \in \mathbb{Z}$ tal que $I = (n)$.

Proof

Sea I un ideal de $\mathbb{Z}$. Si $I = 0$ entonces $I = (0)$ con lo que I es principal. Supongamos que $I \neq 0$ y sea $n \in I \setminus 0$. Entonces $-n \in I$, con lo que I tiene un elemento positivo, o sea $I \cap \mathbb{N} \neq \emptyset$. Como $\mathbb{N}$ está bien ordenado, $I \cap \mathbb{N}$ tiene un mínimo que denotamos como a. Como $a \in I$ se tiene que $(a) \subseteq I$.
Para ver que se da la igualdad tomamos $b \in I$ y sean q y r el cociente y el resto de la división entera de b entre a. Entonces $b = qa + r$ y $0 \leq r < a$. Pero $r = b - qa \in I$, por que I es un ideal de $\mathbb{Z}$ que contiene a a y b y $q \in \mathbb{Z}$. Como r es estrictamente menor que a y a es mínimo en $I \cap \mathbb{N}$, necesariamente $r \notin \mathbb{N}$, es decir r no es positivo. Luego $r = 0$, con lo que $b = qa \in (a)$.

2.4.2 Anillos cociente

Definition 2.4.10: Congruencia módulo un ideal

Sea I un ideal de un anillo A. Decimos que $a, b \in A$ son congruentes módulo I, y escribimos $a \equiv b \pmod{I}$, si $b - a \in I$.

Lemma 2.4.11: Propiedades de la congruencia

Sea I ideal de A. Para todo $a, b, c, d \in A$:

(1) $a \equiv a \pmod{I}$ (reflexiva).

(2) Si $a \equiv b \pmod{I}$, entonces $b \equiv a \pmod{I}$ (simétrica).

(3) Si $a \equiv b \pmod{I}$ y $b \equiv c \pmod{I}$, entonces $a \equiv c \pmod{I}$ (transitiva).

(4) $a \equiv b \pmod{(0)}$ si y solo si $a = b$.

Proof

(1) Como $0 \in A$, dado $x \in I$ debe ser $0x = 0 \in I$, luego $a - a = 0 \in I \implies a \equiv a \pmod{I}$.

(2) Si $a \equiv b \pmod{I}$, entonces

$$b - a \in I \implies (-1)(b - a) = a - b \in I \implies b \equiv A \pmod{I}.$$

(3) Si $a \equiv b \pmod{I}$ y $b \equiv c \pmod{I}$, entonces

$$b - a \in I, c - b \in I \implies c - a \in I \implies a \equiv c \pmod{I}.$$

(4) $a \equiv b \pmod{(0)} \iff b - a = 0 \iff a = b$.

Del Lema 2.4.11 se deduce que la relación «ser congruente módulo I» es una relación de equivalencia en A y, por tanto, las clases de equivalencia por esta relación definen una partición de A.

La clase de equivalencia que contiene a un elemento $a \in A$ es

$$a + I = \{a + x : x \in I\}$$

(en particular $0 + I = I$), de modo que

$$a + I = b + I \Leftrightarrow a \equiv b \pmod{I}$$

(en particular $a + I = 0 + I \Leftrightarrow a \in I$).

El conjunto de las clases de equivalencia se denota

$$A/I = \frac{A}{I} = \{a + I : a \in A\}.$$

En ocasiones se escriben las clases de equivalencia como

$$\bar{a} = a + I, \bar{b} = b + I, \bar{0} = 0 + I = I.$$

Definition 2.4.12: Anillo cociente

Sea I un ideal de A. El conjunto de clases de equivalencia:

$$A/I = \{a + I : a \in A\}$$

con las operaciones:

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = (ab) + I$$

es un anillo llamado anillo cociente de A módulo I.

Proposition 2.4.13: Buena definición del cociente

Las operaciones en A/I están bien definidas y dotan a A/I de estructura de anillo con:

- Elemento cero: $0 + I$
- Elemento uno: $1 + I$

Proof

Sean $a + I = a' + I$ y $b + I = b' + I$. Entonces $a - a', b - b' \in I$. Luego

- La suma está bien definida, para ello veamos que $(a + b) + I = (a' + b') + I$, o equivalentemente, $(a + b) - (a' + b') \in I$, en efecto

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I$$

ya que $a - a', b - b' \in I$.

- El producto está bien definido, para ello veamos que $(ab) + I = (a'b') + I$, es decir, $(ab) - (a'b') \in I$

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I$$

de nuevo porque $a - a', b - b' \in I$.

Por tanto las operaciones están bien definidas. La comprobación del cero y el uno son inmediatas.

Definition 2.4.14: Proyección canónica

La aplicación $\eta : A \to A/I$ dada por $\eta(a) = a + I$ es un homomorfismo sobreyectivo llamado proyección canónica.

Proof

Que la proyección es sobreyectiva es inmediato, dado $a + I \in A/I$ es inmediato que $\eta(a) = a + I$. Comprobar que es un homomorfismo es trivial por la manera en que hemos definido las operaciones en A/I.

Example 2.4.15: Anillos $\mathbb{Z}_n$

Para $n > 0$, $\mathbb{Z}_n$ es el anillo cociente $\mathbb{Z}/(n)$. Tiene exactamente n elementos: $0 + (n), 1 + (n), \ldots, n - 1 + (n)$.

Example 2.4.16: Cocientes triviales

- $A/\{0\} \cong A$
- $A/A \cong \{0\}$

Example 2.4.17: Cociente por ideales en polinomios

Sea $I = \{a_1 X + \cdots + a_n X^n\} \leq A[X]$. Entonces:

$$A[X]/I \cong A$$

mediante el isomorfismo que envía $P(X) + I$ al término constante de P.

Proof

Sea $P(X) \in A[X], P(X) = a_0 + a_1 X + \cdots + a_n X^n$ entonces $P(X) + I \in A[X]/I$ es de la forma $P(X) + I = a_0 + I$ ya que

$$P(X) - a_0 = a_1 X + \cdots + a_n X^n \in I.$$

luego el isomorfismo es $\phi(a_0 + I) = a_0$. Claramente es un homomorfismo sobreyectivo, para ver que es inyectivo supongamos

$$\phi(a_0 + I) = \phi(b_0 + I) \implies a_0 = b_0 \implies a_0 - b_0 = 0 \in I \implies a_0 + I = b_0 + I.$$

Example 2.4.18: Cociente en productos

Sean A, B anillos, $I = A \times \{0\}$. Entonces:

$$(A \times B)/I \cong B$$

2.4.3 Teorema de correspondencia

Recordemos algunas definiciones y caracterizaciones útiles.

Definition 2.4.19: Núcleo de un homomorfismo

Sea $f : A \to B$ un homomorfismo de anillos. El núcleo de f es:

$$\ker f = \{a \in A : f(a) = 0\}$$

Proposition 2.4.20: Inyectividad y núcleo

Un homomorfismo $f : A \to B$ es inyectivo si y solo si $\ker f = \{0\}$.

Proof

- Si f es inyectivo y $a \in \ker f$, entonces $f(a) = 0 = f(0)$, luego $a = 0$
- Si $\ker f = \{0\}$ y $f(a) = f(b)$, entonces $f(a-b) = 0$, luego $a - b \in \ker f = \{0\}$, por tanto $a = b$

El siguiente resultado describe los ideales de un anillo cociente. Consideremos la proyección canónica $\eta : A \to A/I$. La imagen de un subconjunto $J \subset A$ es

$$\eta(J) = \{a + I : a \in J\}$$

si J contiene a I denotaremos a este conjunto $\eta(J) = J/I$.

Theorem 2.4.21: Teorema de correspondencia

Sea I un ideal de un anillo A. Sea $\mathcal{A}$ el conjunto de ideales de A que contienen a I

$$\mathcal{A} = \{J \leq A : I \subseteq J\}.$$

Sea $\mathcal{K}$ el conjunto de todos los ideales de A/I

$$\mathcal{K} = \{K \leq A/I\}.$$

Entonces las asignaciones

$$\Phi : \mathcal{A} \to \mathcal{K},\ \Phi(J) = J/I$$
$$\Psi : \mathcal{K} \to \mathcal{A},\ \Psi(K) = \eta^{-1}(K)$$

definen aplicaciones biyectivas, una inversa de la otra, que conservan la inclusión en $\mathcal{A}$ y $\mathcal{K}$.

Proof

En primer lugar, veamos que son aplicaciones, para ello necesitamos que se cumpla

- Si J es un ideal que contiene a I entonces $\eta(J) = J/I$ es un ideal.
  - Como J es un ideal $0 \in J$, luego $0 + I = \eta(0) \in \eta(J) = J/I \neq \emptyset$.
  - Sean $x + I, y + I \in J/I$ (es decir, $x, y \in J$ tales que $\eta(x) = x + I, \eta(y) = y + I$). Es claro que
  $$\eta(x+y) = (x+y) + I = (x+I) + (y+I) \in J/I$$
  como necesitamos.
  - Sea $x + I \in J/I$, $a + I \in A/I$ entonces
  $$(a+I)(x+I) = ax + I = \eta(ax) \in J/I$$
  ya que $ax \in J$ al ser J ideal.
- Si K es un ideal de A/I entonces $\eta^{-1}(K)$ es un ideal que contiene a I.
  - Como K es un ideal $0 + I \in K$, y al ser $0 + I = \eta(0) \implies 0 \in \eta^{-1}(K) \neq \emptyset$.
  - Sean $x, y \in \eta^{-1}(K)$, entonces $x + I, y + I \in K \implies (x+y) + I \in K$. Finalmente
  $$\eta(x+y) = (x+y) + I = \in K \implies (x+y) \in \eta^{-1}(K)$$
  como necesitamos.

- Sean $x \in \eta{-}1(K)$, $a \in A$ entonces

$$\eta(ax) = ax + I = (a+I)(x+I) \in K$$

ya que $a + I \in A/I$ y K es un ideal, pero entonces $ax \in \eta^{-1}(K)$ como queríamos ver.

- Sea $x \in I$, entonces

$$\eta(x) = 0 + I \in K \implies x \in \eta^{-1}(K).$$

Veamos ahora que una es inversa de la otra, lo cual implica directamente que son biyectivas.

- Dado $J \in \mathcal{A}$
$$\Psi(\Phi(J)) = \eta^{-1}(\eta(J)) \supseteq J$$
por las propiedades básicas de las aplicaciones. Para la otra inclusión, si $x \in \eta^{-1}(\eta(J))$ entonces $\eta(x) \in \eta(J)$, luego existe $y \in J$ tal que
$$x + I = \eta(y) = y + I \implies x - y \in I \subseteq J \implies x = (x-y) + y \in J$$
usando que J es ideal.

- Sea ahora $K \in \mathcal{K}$, entonces
$$\Phi(\Psi(K)) = \eta(\eta^{-1}(K)) \subseteq K$$
por las propiedades de las aplicaciones. Por otro lado, si $x + I \in K$ entonces, al ser η sobreyectiva existe $y \in \eta^{-1}(K)$ tal que $\eta(y) = x + I \in K$. Por tanto $x + I \in \eta(\eta^{-1}(K))$

Finalmente veamos que respetan las inclusiones.

- Si $J, J' \in \mathcal{A}$, $J \subseteq J'$ entonces dado
$$x + I \in \Phi(J) = \eta(J) \implies x + I = \eta(j),\ j \in J \subseteq J' \implies x + I \in \eta(J') = \Phi(J'),$$
es decir $\Phi(J) \subseteq \Phi(J')$.

- De igual manera, si $K, K' \in \mathcal{K}$, $K \subseteq K'$ entonces
$$x \in \Psi(K) = \eta^{-1}(K) \implies \eta(x) \in K \subseteq K' \implies x \in \eta^{-1}(K') = \Psi(J'),$$
es decir, $\Psi(K) \subseteq \Psi(K')$.

Remark. *En 2.3.14 ya habíamos probado casi todo lo que necesitabamos para ver que Φ, Ψ son aplicaciones.*

Remark. *Recordemos que*
$$\eta(\eta^{-1}(K)) = K$$
es una de las caracterizaciones vista en Conjuntos y Números para que una aplicación η sea sobreyectiva.

Example 2.4.22: Aplicación del teorema de correspondencia

En $\mathbb{Z}_n = \mathbb{Z}/(n)$, los ideales son de la forma $d\mathbb{Z}_n = (d)/(n)$ donde $d \mid n$. Además, $d\mathbb{Z}_n \subseteq d'\mathbb{Z}_n$ si y solo si $d' \mid d$.

2.5 Operaciones con ideales

Definition 2.5.1: Suma de ideales

Si I y J son ideales de A, su suma es:

$$I + J = \{x + y : x \in I, y \in J\} = (I \cup J)$$

Definition 2.5.2: Producto de ideales

Si I y J son ideales de A, su producto es:

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J, n \geq 0 \right\} = \Big(\{xy : x \in I, y \in J\}\Big)$$

Remark. Más generalmente, para ideales $I_1, \dots, I_n$*:*

- $I_1 + \cdots + I_n = \{x_1 + \cdots + x_n : x_i \in I_i\}$
- $I_1 \cdots I_n$ *está generado por productos* $x_1 \cdots x_n$ *con* $x_i \in I_i$

Proposition 2.5.3: Propiedades de las operaciones

Para ideales I, J, K de A:

(1) $IJ \subseteq I \cap J$

(2) $I(J \cap K) \subseteq IJ \cap IK$

(3) $I(JK) = (IJ)K$

(4) $I(J + K) = IJ + IK$

(5) $IA = I$

Proof

(1) Sea $x \in IJ$, entonces $x = \sum_{i=1}^{n} x_i y_i$ con cada $x_i \in I, y_i \in J$. Por tanto $x_i y_i \in I$ al ser I un ideal, de hecho $\sum_{i=1}^{n} x_i y_i \in I$ al ser suma de elementos de I. Para J ocurre igual ya que los $y_i \in J$, luego $\sum_{i=1}^{n} x_i y_i \in J$ y finalmente $x \in I \cap J$.

(2) Sea $x \in I(J \cap K)$, entonces $x = \sum_{i=1}^{n} x_i y_i$ con cada $x_i \in I, y_i \in J \cap K$. En concreto $x \in IJ$ ya que cada $y_i \in J$, de igual manera $x \in IK$, por tanto $x \in IJ \cap IK$.

(3) Sea $x \in I(JK)$, entonces $x = \sum_{i=1}^{n} x_i y_i$ con cada $x_i \in I, y_i \in JK$, en concreto cada $y_i = \sum_{k=1}^{m} a_k b_k$ con $a_k \in J, b_k \in K$. Entonces

$$x = \sum_{i=1}^{n} \left(x_i \left[\sum_{k=1}^{m} a_k b_k \right] \right) = \sum_{k=1}^{m} \left(a_k b_k \left[\sum_{i=1}^{n} x_i \right] \right) = \sum_{k=1}^{m} \left(b_k \left[\sum_{i=1}^{n} x_i a_k \right] \right)$$

sea $c_k = \sum_{i=1}^{n} x_i a_k$, entonces cada $c_k \in IJ$ ya que $x_i \in J, a_k \in J$, por tanto

$$x = \sum_{k=1}^{m} (b_k c_k) \in (IJ)K$$

ya que cada $c_k \in IJ, b_k \in K$. Esto prueba que $I(JK) \subseteq (IJ)K$.

El otro contenido es inmediato ya que $IJ = JI$, luego $(IJ)K = K(IJ) \subseteq (KI)J = J(KI) \subseteq (JK)I = I(JK)$ usando lo anterior.

(4) Sea $x \in I(J+K)$, entonces

$$x = \sum_{i=1}^{n} x_i y_i = \sum_{i=1}^{n} x_i(a_i + b_i)$$

con $a_i \in J, b_i \in K$ ya que cada $y_i \in J+K$. Finalmente

$$x = \sum_{i=1}^{n} x_i a_i + \sum_{i=1}^{n} x_i b_i \in IJ + IK$$

ya que $\sum_{i=1}^{n} x_i a_i \in IJ, \sum_{i=1}^{n} x_i b_i \in IK$.
Para la otra inclusión, si $x \in IJ + IK$ entonces $x = a + b$ con $a \in IJ, b \in IK$, luego

$$a = \sum_{i=1}^{n} x_i a_i,\ b = \sum_{k=1}^{m} y_k b_k; \quad x_i, y_k \in I, a_i \in J, b_k \in K$$

pero notemos que $a_i = a_i + 0 \in J+K$ ya que $0 \in K$, de igual manera $b_k = 0 + b_k \in J+K$, luego definiendo

$$c_l = \begin{cases} x_l, & 1 \leq l \leq n \\ y_{n-l}, & n < l \leq n+m \end{cases}$$
$$d_l = \begin{cases} a_l, & 1 \leq l \leq n \\ b_{n-l}, & n < l \leq n+m \end{cases}$$

tenemos que $c_l \in I, d_l \in J+K$ y

$$x = \sum_{l=1}^{n+m} c_l d_l$$

luego $x \in I(J+K)$.

(5) Por 1. tenemos que $IA \subseteq I \cap A = I$. Por otro lado, si $x \in I$ entonces definiendo $x_1 = x, a_1 = 1_A$ tenemos

$$x = x1_A = \sum_{i=1}^{1} x_i a_i \implies x \in IA.$$

Example 2.5.4: Operaciones en $\mathbb{Z}$

Sean (n) y (m) ideales de $\mathbb{Z}$. Entonces:

$$(n)(m) = (nm)$$
$$(n) \cap (m) = (\mathrm{mcm}(n,m))$$
$$(n) + (m) = (\mathrm{mcd}(n,m))$$

Example 2.5.5: Ideal no principal

En $\mathbb{Z}[X]$, el ideal $(2) + (X)$ (polinomios con término constante par) no es principal.

Proof

Supongamos que $(2) + (X) = (a)$ para algún $a \in \mathbb{Z}[X]$. Entonces:

- $2 = aP$ para algún $P \in \mathbb{Z}[X]$, pero entonces P ha de ser un polinomio solo con término independiente y a también.
- Como $a \in (2) + (X)$, a debe ser par.
- Si suponemos $X \in (a)$ debe ser $X = aP$ para algún $P \in \mathbb{Z}[X]$, pero aP tiene coeficiente par en la X porque a es par, luego $X \notin (a) = (2) + (X)$ lo cual es contradictorio.

Example 2.5.6

Sea A un anillo y sean $a, b \in A$, entonces $(a, b) = (a) + (b)$

Proof

En efecto si $x \in (a, b)$ entonces

$$x = ax_1 + bx_2 \implies x \in (a) + (b).$$

De igual manera, si $x \in (a) + (b)$ entonces

$$x = a_1 + b_1$$

con $a_1 \in (a) \implies a_1 = ax_1, b_1 \in (b) \implies b_1 = bx_2$, por tanto

$$x = ax_1 + bx_2 \in (a, b).$$

2.6 Teoremas de isomorfía y Teorema chino de los restos

Theorem 2.6.1: Primer teorema de isomorfía

Sea $f : A \to B$ un homomorfismo de anillos. Entonces existe un único isomorfismo de anillos $\bar{f} : A/\ker f \to \operatorname{Im} f$ que hace conmutativo el diagrama

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"'] & B \\ A/\ker f \arrow[r, "\bar{f}"'] & \operatorname{Im} f \arrow[u, "i"'] \end{tikzcd}$$

es decir, $i \circ \bar{f} \circ p = f$, donde i es la inclusión y p es la proyección. En particular

$$\frac{A}{\ker f} \cong \operatorname{Im} f.$$

Proof

Sean $K = \ker f$ e $I = \operatorname{Im} f$. La aplicación $\bar{f} : A/K \to I$ dada por $\bar{f}(x + K) = f(x)$ está bien definida (no depende de representantes) pues si $x + K = y + K$ entonces $x - y \in K$ y por lo tanto $f(x) - f(y) = f(x - y) = 0$; es decir, $f(x) = f(y)$. Además es elemental ver que es un homomorfismo de anillos

$$\bar{f}((x + K) + (y + K)) = \bar{f}((x + y) + K) = f(x + y) = f(x) + f(y) = \bar{f}(x + K) + \bar{f}(y + K)$$

$$\bar{f}((x + K)(y + K)) = \bar{f}(xy + K) = f(xy) = f(x)f(y) = \bar{f}(x + K)\bar{f}(y + K)$$

$$\bar{f}(1 + K) = f(1) = 1.$$

Que es suprayectiva también es inmediato, dado $b \in I$ existe $a \in A$ tal que $b = f(a)$, luego

$$\bar{f}(a + K) = f(a) = b.$$

Para ver que es inyectiva usamos la Proposición 2.3.6: si $x + K$ está en el núcleo de $\bar{f}$ entonces $0 = \bar{f}(x + K) = f(x)$, de modo que $x \in K$ y así $x + K = 0 + K$. Es decir $\ker \bar{f} = 0$ y por lo tanto $\bar{f}$ es inyectiva. En conclusión, $\bar{f}$ es un isomorfismo, y hace conmutativo el diagrama porque, para cada $x \in A$, se tiene

$$i(\bar{f}(p(x))) = i(\bar{f}(x + K)) = i(f(x)) = f(x).$$

En cuanto a la unicidad, supongamos que otro homomorfismo $\bar{f}' : A/K \to I$ verifica $i \circ \bar{f}' \circ p = f$; entonces para cada $x \in K$ se tiene

$$\bar{f}'(x + K) = i(\bar{f}'(p(x))) = f(x) = \bar{f}(x + K).$$

Finalmente, $\bar{f}' = \bar{f}$.

Theorem 2.6.2: Segundo teorema de isomorfía

Sea A un anillo y sean I y J dos ideales tales que $I \subseteq J$. Entonces J/I es un ideal de A/I y existe un isomorfismo de anillos

$$\frac{A/I}{J/I} \cong \frac{A}{J}.$$

Proof

Por el Teorema de la Correspondencia 2.4.21, J/I es un ideal de A/I. Sea $f : A/I \to A/J$ la aplicación definida por $f(a+I) = a+J$. Es elemental ver que f está bien definida, sean $a+I = b+I \in A/I$, entonces $a-b \in I \subset J$, luego

$$a-b \in J \implies a+J = b+J \implies f(a+I) = f(b+I).$$

Que es un homomorfismo de anillos se deja como ejercicio. Que es suprayectivo es inmediato, pues dado $a+J \in A/J$ es claro que $f(a+I) = a+J$. Veamos que $\ker f = J/I$

$$f(a+I) = a+J = 0+J \iff a \in J \implies a+I \in \eta(J) = J/I$$

si por el contrario $a+I \in J/I$ entonces

$$a+I = \eta(j) = j+I \implies f(a+I) = f(j+I) = j+J = 0+J \implies a+I \in \ker f.$$

Entonces el isomorfismo buscado se obtiene aplicando el Primer teorema de isomorfía a f.

Theorem 2.6.3: Tercer teorema de isomorfía

Sea A un anillo con un subanillo B y un ideal I. Entonces:

(1) $B \cap I$ es un ideal de B.

(2) $B + I$ es un subanillo de A que contiene a I como ideal.

(3) Se tiene un isomorfismo de anillos $\dfrac{B}{B \cap I} \cong \dfrac{B+I}{I}$.

Proof

(1) Claramente $0 \in B \cap I$. Sean $x, y \in B \cap I$, como B es subanillo e I ideal $x+y \in B, I \implies x+y \in B \cap I$. Dado $a \in B$, como B subanillo $ax \in B$, y como I es ideal de A y $a \in B \subseteq A$ tenemos $ax \in I$, luego $ax \in B \cap I$.

(2) Claramente $1 = 1 + O \in B + I$. Además, es obvio que es cerrado para restas y productos por ser B subanillo e I ideal, luego es un subanillo. Que I es ideal de $B+I$ porque está contenido en la suma, el resto de condiciones se verifican trivialmente porque se cumplen en A.

(3) Sea $f : B \to A/I$ la composición de la inclusión $j : B \to A$ con la proyección $\eta : A \to A/I$
$$f(b) = \eta(j(b)) = b + I.$$
Es claro que $\ker f = B \cap I$, puesto que dado $b \in B$
$$f(b) = b + I = 0 + I \iff b \in I \iff b \in B \cap I$$
y que $\operatorname{Im} f = (B+I)/I$, ya que dado $b + I \in \operatorname{Im} f$ existe un cierto $b_0 \in B$ tal que
$$b + I = f(b_0) = b_0 + I \iff b - b_0 \in I \iff b - b_0 = i \in I \implies b = b_0 + i \in B + I.$$
Por tanto, el resultado se sigue del Primer Teorema de Isomorfía.

Example 2.6.4: Aplicaciones del Primer Teorema de Isomorfía

(1) Si A y B son anillos, el homomorfismo $A \times B \to A$ de proyección en la primera componente es suprayectivo y tiene núcleo $I = 0 \times B$, por lo que $\frac{A \times B}{0 \times B} \simeq A$. En realidad ya habíamos visto esto en 2.4.18.

(2) Sea n un entero positivo. Hemos visto que todo ideal de $\mathbb{Z}_n = \mathbb{Z}/(n)$ es de la forma $(\overline{d}) = (d)/(n)$, para cierto divisor positivo d de n. El Segundo Teorema de Isomorfía nos permite identificar el cociente $\mathbb{Z}_n/(\overline{d})$, pues

$$\frac{\mathbb{Z}_n}{(\overline{d})} = \frac{\mathbb{Z}/(n)}{(d)/(n)} \simeq \frac{\mathbb{Z}}{(d)} = \mathbb{Z}_d.$$

(3) Si A es un anillo, el homomorfismo $f : A[X] \to A$ de sustitución en 0 (dado por $a_0 + a_1X + \cdots \mapsto a_0$) es suprayectivo y tiene por núcleo el ideal (X) generado por X (consistente en los polinomios con coeficiente independiente nulo), de modo que $A[X]/(X) \simeq A$, como ya habíamos observado en el Ejemplo 2.4.17.

(4) Sean A un anillo e I un ideal de A. Para cada $a \in A$, sea $\overline{a} = a + I$. La aplicación $f : A[X] \to (A/I)[X]$ dada por $f(a_0 + a_1X + \cdots + a_nX^n) = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$ es un homomorfismo suprayectivo de anillos cuyo núcleo es $I[X] = \{a_0 + a_1X + \cdots + a_nX^n : a_i \in I\}$ (estas afirmaciones quedan como ejercicio para el lector). Del Primer Teorema de Isomorfía se deduce entonces que

$$\frac{A[X]}{I[X]} \simeq (A/I)[X].$$

Definition 2.6.5: Característica

Sea A un anillo, y recordemos que si $n \in \mathbb{Z}^+$ escribimos $n1 = 1 + \cdots + 1$ (n veces). Si existe $n \in \mathbb{Z}^+$ tal que $n1 = 0$, definimos la característica de A como el menor $n \in \mathbb{Z}^+$ que verifica tal igualdad. Si no existe un tal n, decimos que la característica de A es 0.

Proposition 2.6.6: Caracterización de la característica

Sea A un anillo y sea $f : \mathbb{Z} \to A$ el único homomorfismo de anillos (dado por $f(n) = n1$). Para un número natural n las condiciones siguientes son equivalentes:

(1) n es la característica de A.

(2) $n\mathbb{Z}$ es el núcleo de f.

(3) El subanillo primo de A es isomorfo a $\mathbb{Z}_n$ (recuérdese que $\mathbb{Z}_0 = \mathbb{Z}$ y $\mathbb{Z}_1 = 0$).

(4) A contiene un subanillo isomorfo a $\mathbb{Z}_n$.

Proof

(1) $\Rightarrow$ (2): Claramente $n\mathbb{Z} \subseteq \ker f$ puesto que para todo $nm \in n\mathbb{Z}, f(nm) = nm1 = m(n1) = 0$. Sea $m \in \ker f$, sabemos que $m = nq + r$ para cierto $q \in \mathbb{Z}$, $0 \leq r < n$, luego

$$0 = f(m) = f(nq + r) = f(nq) + f(r) = r1 \implies r = 0$$

luego $m \in n\mathbb{Z}$.
(2) $\Rightarrow$ (1): Supongamos que existe $0 \leq m < n$ tal que $f(m) = 0$, entonces $m \in \ker f = n\mathbb{Z}$, luego $m = nq$ para cierto $q \in \mathbb{Z}$, lo cual es claramente imposible, por tanto n es el menor

tal que $n1 = f(n) = 0$.
(3) $\Rightarrow$ (4): Es inmediato.
(2) $\Rightarrow$ (3). Aplicando el Primer Teorema de Isomorfía

$$\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker f \cong \operatorname{Im} f.$$

Basta ver ahora que $\operatorname{Im} f$ es el subanillo primo de A. En efecto si $x \in \mathbb{Z}1$ entonces $x = n1 = f(n)$. De igual manera, si $x \in \operatorname{Im} f \implies x = f(n) = n1 \in \mathbb{Z}1$.
(4) $\Rightarrow$ (2). Si B es un subanillo de A y $g : \mathbb{Z}_n \to B$ es un isomorfismo, considerando la proyección $\pi : \mathbb{Z} \to \mathbb{Z}_n$ y la inclusión $u : B \hookrightarrow A$ se obtiene un homomorfismo de anillos $u \circ g \circ \pi : \mathbb{Z} \to A$ que debe coincidir con f por su unicidad.
Además, como $m \in \ker f$ si y solo si

$$0 = f(m) = u(g(\pi(m))) \iff \pi(m) \in \ker(u \circ g)$$

pero como $u \circ g$ es inyectiva su núcleo es trivial, por lo que debe ser

$$\pi(m) = 0 \iff m \in n\mathbb{Z}.$$

Theorem 2.6.7: Teorema Chino de los Restos

Sea A un anillo y sean $I_1, \dots, I_n$ ideales de A tales que $I_i + I_j = A$ para todo $i \neq j$. Entonces $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. Además

$$\frac{A}{I_1 \cap \cdots \cap I_n} \cong \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}.$$

Proof

Razonamos por inducción sobre n, empezando con el caso $n = 2$.
La hipótesis $I_1 + I_2 = A$ nos dice que existen $x_1 \in I_1$ y $x_2 \in I_2$ tales que $x_1 + x_2 = 1$, y entonces para cada $a \in I_1 \cap I_2$ se tiene

$$a = ax_1 + ax_2 \in I_1 I_2,$$

de modo que $I_1 \cap I_2 \subseteq I_1 I_2$, y la otra inclusión es clara.
Claramente la aplicación $f : A \to A/I_1 \times A/I_2$ dada por $f(a) = (a + I_1, a + I_2)$ es un homomorfismo de anillos con núcleo $I_1 \cap I_2$, y es suprayectiva pues, dado un elemento arbitrario $(a_1 + I_1, a_2 + I_2)$ de $A/I_1 \times A/I_2$, el elemento $a = a_1 + a_2$ verifica $f(a) = (a_1 + I_1, a_2 + I_2)$. Ahora el resultado se obtiene aplicando el Primer Teorema de Isomorfía.
En el caso general ($n > 2$) basta ver que las hipótesis implican que $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$, pues entonces la hipótesis de inducción nos da

$$I_1 \cap \cdots \cap I_{n-1} \cap I_n = (I_1 \cap \cdots \cap I_{n-1}) I_n = I_1 \cdots I_{n-1} I_n$$

y

$$\frac{A}{I_1 \cap \cdots \cap I_n} = \frac{A}{(\cap_{i=1}^{n-1} I_i) \cap I_n} \simeq \frac{A/(\cap_{i=1}^{n-1} I_i)}{I_n} \times \frac{A}{I_n} \simeq \frac{A}{I_1} \times \cdots \times \frac{A}{I_{n-1}} \times \frac{A}{I_n}.$$

Para ver que $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$ notemos que, para cada $i \leq n-1$, existen $a_i \in I_i$ y $b_i \in I_n$ tales que $1 = a_i + b_i$, y multiplicando todas esas expresiones se obtiene

$$1 = \prod_{i=1}^{n-1} (a_i + b_i) = a_1 \cdots a_{n-1} + b,$$

donde b engloba a todos los sumandos que se obtendrían desarrollando los productos (excepto $a_1 \cdots a_{n-1}$) y está en I_n porque en cada sumando hay al menos un factor del ideal

I_n. Como además $a_1 \cdots a_{n-1} \in I_1 \cap \cdots \cap I_{n-1}$, deducimos que $1 \in (I_1 \cap \cdots \cap I_{n-1}) + I_n$ y así $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$, como queríamos ver.

Chapter 3

Divisibilidad en dominios

3.1 Cuerpos y dominios

Definition 3.1.1

Un elemento a de un anillo A se dice regular si la relación $ab = ac$ con $b, c \in A$ implica que $b = c$; es decir, si a es cancelable respecto del producto. Claramente, el 0 nunca es regular (obsérvese la importancia de la hipótesis $1 \neq 0$ en este caso.)
Un cuerpo es un anillo en el que todos los elementos no nulos son invertibles, y un dominio (o dominio de integridad) es un anillo en el que todos los elementos no nulos son regulares. Un subanillo de un anillo A que sea un cuerpo se llama un subcuerpo de A, y un homomorfismo de anillos entre dos cuerpos se llama homomorfismo de cuerpos.

Remark. *Si A es un dominio y $0 \neq a, b \in A$, luego a y b son regulares. Supongamos que $ab = 0$, entonces*

$$ab = 0 = a0 \implies b = 0$$

ya que a es cancelable, pero esto es una contradicción, luego no puede cumplirse $ab = 0$ si $a, b \neq 0$.

En otras palabras

$$a, b \neq 0 \implies ab \neq 0$$

el contrarrecíproco de esta afirmación es

$$ab = 0 \implies a = 0 \text{ ó } b = 0$$

Proposition 3.1.2

Todo cuerpo es un dominio.

Proof

Si A es un cuerpo y $a \in A$, $a \neq 0$, entonces a es invertible. Si $ab = ac$, multiplicando por a^{-1} obtenemos $b = c$, luego a es regular. Como esto vale para todo $a \neq 0$, A es un dominio.

Proposition 3.1.3

Sea A un anillo.

(1) Las condiciones siguientes son equivalentes:

  (a) A es un cuerpo.
  (b) Los únicos ideales de A son 0 y A.
  (c) Todo homomorfismo de anillos $A \to B$ con $B \neq 0$ es inyectivo.

(2) Un elemento $a \in A$ es regular si y solo si la relación $ab = 0$ con $b \in A$ implica $b = 0$ (por este motivo, los elementos no regulares se suelen llamar divisores de cero).

(3) A es un dominio si y solo si, para cualesquiera $a, b \in A$ no nulos, se tiene $ab \neq 0$.

(4) Todo subanillo de un dominio es un dominio.

(5) La característica de un dominio es cero o un número primo.

Proof

(1) Demostramos las equivalencias.

(a) $\Rightarrow$ (b) Si A es cuerpo e I es un ideal no nulo de A, entonces I tiene un elemento $a \neq 0$. Como A es cuerpo, a es invertible, luego $I = A$.

(b) $\Rightarrow$ (c) Si $f : A \to B$ es un homomorfismo con $B \neq 0$, entonces $\ker f$ es un ideal pero $\ker f \neq A$, pues $f(1) = 1 \neq 0$. Entonces, por (b), $\ker f = 0$, luego f es inyectivo.

(c) $\Rightarrow$ (a) Haremos el contrarrecírpoco. Si A no es cuerpo, existe $a \neq 0$ no invertible. Entonces (a) es un ideal propio no nulo, y el homomorfismo canónico

$$\pi : A \to A/(a), \quad \pi(x) = x + (a)$$

no es inyectivo ya que

$$a \in \ker \pi \neq 0.$$

(2) Si a es regular y $ab = 0$, entonces $ab = 0 = a0$, luego $b = 0$. Recíprocamente, si a no es regular, existen $b \neq c$ con $ab = ac$, luego $a(b - c) = 0$ con $b - c \neq 0$.

(3) Es consecuencia inmediata de (2).

(4) Si B es subanillo de un dominio A y $x, y \in B$ son no nulos, entonces $xy \neq 0$ en A, luego también en B ya que su cero es el mismo que el de A.

(5) Sea D un dominio y consideremos el homomorfismo $f : \mathbb{Z} \to D$ dado por $f(n) = n \cdot 1$. Como $\ker f$ es un ideal de $\mathbb{Z}$, existe $n \geq 0$ tal que $\ker f = (n)$. Si $n = ab$ con $0 < a, b < n$, entonces $f(a)f(b) = f(ab) = 0$, luego $f(a) = 0$ o $f(b) = 0$, contradicción. Así que n es primo o $n = 0$.

Example 3.1.4: Dominios y cuerpos

(1) Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos y $\mathbb{Z}$ es un dominio que no es un cuerpo (aunque es subanillo de un cuerpo).

(2) Para $n \geq 2$, el anillo $\mathbb{Z}_n$ es un dominio si y solo si es un cuerpo, si y sólo si n es primo.

> **Proof**
>
> Si n es primo y $\overline{a} \neq 0$ en $\mathbb{Z}_n$, entonces $\mathrm{mcd}(a, n) = 1$, luego existen x, y con $ax + ny = 1$, así que $\overline{ax} = \overline{1}$. Recíprocamente, si n no es primo, existen a, b con $1 < a, b < n$ y $n = ab$, luego $\overline{a}\overline{b} = \overline{0}$ con $\overline{a}, \overline{b} \neq 0$.

(3) Si m es un entero que no es el cuadrado de un número entero entonces $\mathbb{Z}[\sqrt{m}]$ es un dominio (subanillo de $\mathbb{C}$) que no es un cuerpo (el 2 no tiene inverso). Sin embargo, $\mathbb{Q}[\sqrt{m}]$ sí que es un cuerpo; de hecho, si $a + b\sqrt{m} \neq 0$, entonces $q = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2 m$ es un número racional no nulo y $(a + b\sqrt{m})^{-1} = \frac{a}{q} - \frac{b}{q}\sqrt{m}$.

(4) Un producto de anillos diferentes de 0 nunca es un dominio, pues $(1, 0)(0, 1) = (0, 0)$.

(5) Los anillos de polinomios no son cuerpos, pues la indeterminada genera un ideal propio y no nulo. Por otra parte, $A[X]$ es un dominio si y solo si lo es A.

> **Proof**
>
> Si A es dominio y $P, Q \in A[X]$ son no nulos, sean $a_n X^n$ y $b_m X^m$ sus términos de mayor grado. Entonces el coeficiente de X^{n+m} en PQ es $a_n b_m \neq 0$, luego $PQ \neq 0$. El recíproco es claro pues A es subanillo de $A[X]$.

3.2 Ideales primos y maximales

Definition 3.2.1: Ideal primo

Un ideal propio $P \leq A, P \neq A$ es primo si para todo $a, b \in A$:

$$ab \in P \Rightarrow a \in P \text{ o } b \in P$$

Definition 3.2.2: Ideal maximal

Un ideal propio $M \leq A, M \neq A$ es maximal si no existe ningún ideal I tal que $M \subsetneq I \subsetneq A$.

Proposition 3.2.3: Caracterizaciones de ideales maximales y primos

Sean A un anillo e I un ideal propio de A. Entonces:

(1) I es maximal si y solo si A/I es un cuerpo.

(2) I es primo si y solo si A/I es un dominio.

(3) Si I es maximal entonces es primo.

(4) A es un cuerpo si y solo si el ideal 0 es maximal.

(5) A es un dominio si y solo si el ideal 0 es primo.

Proof

(1) Por el teorema de correspondencia, los ideales de A/I corresponden a los ideales de A que contienen a I.

Así, si I es maximal entonces el único ideal distinto de I que contiene a I es A. Pero entonces, dado un ideal $J/I \leq A/I$ este ha de corresponder a A/I o a $I/I = 0$, luego los únicos ideales de A/I son 0 y A/I, lo cual es una de las caracterizaciones para que un anillo sea un cuerpo.

De igual manera, si A/I es un cuerpo, entonces los únicos ideales son 0 y A/I, pero entonces los únicos ideales que contienen a I son I, A, es decir, I es maximal.

(2) Si I es primo y tomamos $(a + I)(b + I) = ab + I = 0 + I$ entonces

$$ab \in I \implies a \in I \text{ ó } b \in I \implies a + I = 0 + I \text{ ó } b + I = 0 + I$$

luego A/I es dominio.

Por el contrario, si A/I es dominio entonces dados a, b tales que $ab \in I$

$$0 + I = ab + I = (a + I)(b + I) \iff a + I = 0 + I \text{ ó } b + I = 0 + I \iff a \in I \text{ ó } b \in I$$

es decir, si $ab \in I$ entonces $a \in I$ o $b \in I$.

(3) Se sigue de (1) y (2) ya que

$$I \text{ maximal} \iff A/I \text{ cuerpo} \implies A/I \text{ dominio} \iff I \text{ primo}.$$

(4) Es inmediato aplicando (1) ya que $A \cong A/(0)$.

(5) Es inmediato aplicando (2) ya que $A \cong A/(0)$

Remark. *La parte 3. de la proposición anterior se puede probar directamente.*

Proof

Supongamos que I *es maximal pero no primo. Entonces existen* $a, b \in A$ *tales que* $ab \in I$ *pero* $a, b \notin I$. *Consideremos entonces el siguiente ideal*

$$I + (a) = \{x + ay : x \in I, y \in A\}.$$

Claramente $I \subseteq I + (a) \subseteq A$, *y claramente* $I \neq I + (a)$ *ya que* $a = 0 + a1 \in I + (a)$, $a \notin I$. *Pero también tenemos* $I + (a) \neq A$ *ya que si no fuera así entonces existirían* $x_0 \in I, y_0 \in A$ *tales que*

$$x_0 + ay_0 = 1 \implies bx_0 + aby_0 = b \implies b \in I$$

ya que $bx_0, aby_0 \in I$, *lo cual es contradictorio.*
Luego $I + (a)$ *es un ideal propio que contiene a* I, *pero eso contradice la maximalidad de* I, *por tanto* I *debe ser primo.*

Example 3.2.4: Ejemplos en $\mathbb{Z}$

- Los ideales primos de $\mathbb{Z}$ son (0) y (p) con p primo.
- Los ideales maximales de $\mathbb{Z}$ son (p) con p primo.

Proof

Como sabemos que los ideales de $\mathbb{Z}$ son de la forma (n) basta hacer unas cuantas cuentas. Sea (n) un ideal primo de $\mathbb{Z}$. Dados $a, b \in Z$ tales que $ab \in (n)$ entonces $a \in (n)$ o $b \in (n)$. Notemos entonces que

$$x \in (n) \implies x = ny \implies n|x$$

por tanto la condición para que un ideal sea primo es que

$$n|ab \implies n|a \text{ ó } n|b$$

pero esto solo se cumple para $n = 0$ o n primo, como queríamos ver.
Notemos que si $(n) \subseteq (m)$ entonces

$$n \in (n) \subseteq (m) \implies n = my \implies m|n$$

y de igual manera, si $m|n \implies n = my \implies (n) \subseteq (m)$. Sea (n) un ideal maximal, entonces no existe $m \neq \pm 1, \pm n$ tal que $(n) \subsetneq (m) \subsetneq \mathbb{Z}$, es decir, no existe ningún número distinto de $\pm 1, \pm n$ que divida a n, luego n es primo como queríamos ver.

Remark. *El ejemplo anterior también se puede completar considerando los anillos cociente apropiados. Queda como ejercicio para el lector.*

Proposition 3.2.5

Todo ideal propio de un anillo está contenido en un ideal maximal.

Proof

Sea I un ideal propio de A y sea Ω el conjunto de los ideales propios de A que contienen a I. Obsérvese que la unión de una cadena $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ de elementos de Ω es un ideal, que además es propio, pues si no lo fuera, contendría a 1 y por tanto algún I_n contendría a 1 en contra de que todos los I_n son ideales propios. Aplicando el Lema de Zorn deducimos que Ω tiene un elemento maximal que obviamente es un ideal maximal de A.

Remark. El uso del Lema de Zorn en la demostración anterior implica que este resultado depende del Axioma de Elección. En anillos noetherianos (como $\mathbb{Z}$ o $K[X]$ con K cuerpo) se puede demostrar sin el Axioma de Elección.

3.3 Divisibilidad

Definition 3.3.1: Divisibilidad

Sea A un anillo y sean $a, b \in A$. Si existe $c \in A$ tal que $b = ac$ entonces se dice que a divide a b en A, o que a es un divisor de b en A, o que b es un múltiplo de a en A. Para indicar que a divide a b en A escribiremos $a \mid b$ en A. Si el anillo A esta claro por el contexto escribiremos simplemente $a \mid b$.

Obsérvese que la nocion de divisibilidad depende del anillo. Por ejemplo, si a es un entero diferente de 0, entonces a divide a todos los numeros enteros en $\mathbb{Q}$, pero no necesariamente en $\mathbb{Z}$.

Lemma 3.3.2

Si A es un anillo y $a, b, c \in A$ entonces se verifican las siguientes propiedades:

(1) (Reflexiva) $a \mid a$.

(2) (Transitiva) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

(3) $a \mid 0$ y $1 \mid a$.

(4) $0 \mid a$ si y solo si $a = 0$.

(5) $a \mid 1$ si y solo si a es una unidad; en este caso $a \mid x$ para todo $x \in A$ (es decir, las unidades dividen a cualquier elemento).

(6) Si $a \mid b$ y $a \mid c$ entonces $a \mid rb + sc$ para cualesquiera $r, s \in A$ (y en particular $a \mid b + c$, $a \mid b - c$ y $a \mid rb$ para cualquier $r \in A$). Mas generalmente, si a divide a ciertos elementos, entonces divide a cualquier combinacion lineal suya con coeficientes en A.

(7) Si c no es divisor de cero y $ac \mid bc$, entonces $a \mid b$.

Proof

(1) $a = a \cdot 1$, luego $a \mid a$.

(2) Si $a \mid b$ y $b \mid c$, existen $x, y \in A$ tales que $b = ax$ y $c = by$. Entonces $c = a(xy)$, luego $a \mid c$.

(3) $0 = a \cdot 0$, luego $a \mid 0$. Tambien $a = 1 \cdot a$, luego $1 \mid a$.

(4) Si $0 \mid a$, existe $x \in A$ tal que $a = 0 \cdot x = 0$. Recíprocamente, si $a = 0$, entonces $0 \mid a$ por (3).

(5) Si $a \mid 1$, existe $u \in A$ tal que $1 = au$. Entonces $u = a^{-1}$ y a es unidad. Recíprocamente, si a es unidad, entonces $1 = aa^{-1}$, luego $a \mid 1$. Ademas, para cualquier $x \in A$, $x = a(a^{-1}x)$, luego $a \mid x$.

(6) Si $a \mid b$ y $a \mid c$, existen $x, y \in A$ tales que $b = ax$ y $c = ay$. Entonces $rb + sc = a(rx + sy)$, luego $a \mid rb + sc$.

(7) Si $ac \mid bc$, existe $d \in A$ tal que $bc = acd$. Como c no es divisor de cero, podemos cancelar: $b = ad$, luego $a \mid b$.

Definition 3.3.3: Elementos asociados

Dos elementos a y b de un anillo A se dice que son asociados en A si se dividen mutuamente en A; es decir, si $a \mid b$ y $b \mid a$ en A. Cuando este claro por el contexto en que anillo estamos trabajando, diremos simplemente que a y b son asociados.

Por ejemplo, una unidad es lo mismo que un elemento asociado a 1. Es elemental ver que «ser asociados» es una relacion de equivalencia en A, y que dos elementos son asociados si y solo si tienen los mismos divisores, si y solo si tienen los mismos múltiplos. Por lo tanto, al estudiar cuestiones de divisibilidad, un elemento tendrá las mismas propiedades que sus asociados.

Lemma 3.3.4: Asociados en dominios

Si D es un dominio entonces $a, b \in D$ son asociados en D si y solo si existe una unidad u de D tal que $b = au$.

Proof

Si $b = au$ con u unidad entonces $a = bu^{-1}$ con lo que $a \mid b$ y $b \mid a$, es decir a y b son asociados.
Recíprocamente, supongamos que a y b son asociados. Entonces $b = au$ y $a = bv$ para ciertos $u, v \in D$. Claramente si a o b es 0 entonces el otro tambien es 0, con lo que en este caso $a = b1$. Por otro lado, si a y b son ambos distintos de 0 tambien lo son u y v con lo que $uv \neq 0$ por ser D un dominio. Como ademas $auv = bv = a = a1$ y a es cancelable por ser distinto de 0 y D un dominio, deducimos que $uv = 1$ con lo que u es una unidad de D.

Sabemos que cualquier elemento a de un anillo A es divisible por sus asociados y por las unidades de A, y que si a divide a uno de los elementos b o c entonces divide a su producto bc. A continuacion estudiamos los elementos que verifican los recíprocos de estas propiedades.

A menudo consideraremos elementos a de un anillo A que no son cero ni unidades, lo que sintetizaremos en la forma $0 \neq a \in A \setminus A^*$.

Definition 3.3.5: Elementos irreducibles y primos

Diremos que un elemento a del anillo A es irreducible si $0 \neq a \in A \setminus A^*$ y la relacion $a = bc$ en A implica que $b \in A^*$ o $c \in A^*$ (y por lo tanto que uno de los dos es asociado de a).
Diremos que a es primo si $0 \neq a \in A \setminus A^*$ y la relacion $a \mid bc$ en A implica que $a \mid b$ o $a \mid c$. Ambas nociones dependen del anillo ambiente, y si este no esta claro por el contexto hablaremos de irreducibles y primos en A.

Proposition 3.3.6

En un dominio A todo elemento primo es irreducible.

Proof

Sea p un elemento primo de A y supongamos que $p = ab$, con $a, b \in A$. Entonces $p \mid ab$ y como p es primo, $p \mid a$ o $p \mid b$. Supongamos que $p \mid a$. Entonces existe $u \in A$ tal que $a = pu$. Sustituyendo en $p = ab$ obtenemos $p = pub$, luego $p(1 - ub) = 0$. Como $p \neq 0$ y A es dominio, $1 - ub = 0$, es decir, $ub = 1$, luego b es unidad. Esto demuestra que p es irreducible.

El recíproco no se verifica en general, como muestra el siguiente ejemplo.

Example 3.3.7: Irreducible no implica primo: Parte 1

Veamos primero el contraejemplo y luego una justificación de cómo se llega al resultado. En el anillo $\mathbb{Z}[\sqrt{-5}]$ consideremos la factorización:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Veamos que 2 es irreducible pero no primo:

- 2 es irreducible. Supongamos que $2 = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Considerando la norma $N(a+b\sqrt{-5}) = a^2+5b^2$, tenemos:

  $$N(2) = 4 = N(\alpha)N(\beta).$$

  Las únicas factorizaciones de 4 en enteros positivos son $4 = 1 \cdot 4 = 2 \cdot 2 = 4 \cdot 1$. No existe ningún elemento en $\mathbb{Z}[\sqrt{-5}]$ con norma 2 (pues $a^2+5b^2 = 2$ no tiene soluciones enteras). Por tanto, una de las normas debe ser 1 y la otra 4. Si $N(\alpha) = 1$, entonces α es unidad; si $N(\beta) = 1$, entonces β es unidad. Luego 2 es irreducible.

- 2 no es primo. Observemos que:

  $$2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

  pero $2 \nmid (1+\sqrt{-5})$ y $2 \nmid (1-\sqrt{-5})$, pues si $2 \mid (1+\sqrt{-5})$, existiría $\gamma \in \mathbb{Z}[\sqrt{-5}]$ tal que $1+\sqrt{-5} = 2\gamma$, lo cual es imposible (comparando partes enteras e irracionales). De igual manera podemos ver que $2 \nmid (1-\sqrt{-5})$. Por tanto, 2 no es primo.

Example 3.3.8: Irreducible no implica primo: Parte 2

En el anillo $\mathbb{Z}[\sqrt{-5}]$ hay elementos irreducibles que no son primos. Comencemos observando que el cuadrado del modulo de un elemento $a + b\sqrt{-5}$ de $\mathbb{Z}[\sqrt{-5}]$, con $a, b \in \mathbb{Z}$ es

$$N(a + b\sqrt{-5}) = |a + b\sqrt{-5}|^2 = a^2 + 5b^2.$$

notemos además que $N(xy) = N(x)N(y)$.
Claramente, si $x \mid y$ en $\mathbb{Z}[\sqrt{-5}]$, entonces $N(x)$ divide a $N(y)$ en $\mathbb{Z}$. En particular, si $x = a + b\sqrt{-5}$ y $N(x) = 1$ entonces

$$N(x) = a^2 + 5b^2 = 1 \implies a = \pm 1, b = 0 \implies x = \pm 1.$$

De aqui deducimos que si un cierto elemento u cumple $uv = 1$ entonces

$$N(u)|N(1) = 1 \implies N(u) = 1$$

por tanto las unidades en $\mathbb{Z}[\sqrt{-5}]$ son

$$\mathbb{Z}[\sqrt{-5}]^* = \{x \in \mathbb{Z}[\sqrt{-5}] : |x|^2 = 1\} = \{1, -1\}.$$

Por otro lado los cuadrados en $\mathbb{Z}_5$ son $0 + (5)$ y $\pm 1 + (5)$, y por lo tanto la congruencia

$$a^2 \equiv \pm 2 \mod 5$$

no tiene solucion. Esto implica que en $\mathbb{Z}[\sqrt{-5}]$ no hay elementos cuyo modulo al cuadrado valga 2, 3 o 12.
Sea ahora $x \in \mathbb{Z}[\sqrt{-5}]$ con $N(x) = 4$. Si un cierto elemento y divide a x, entonces

$$y \mid x \implies N(y)|N(x) = 4$$

pero al estar en $\mathbb{Z}$, $N(y)$ debe valer 1, 2 o 4.

- Si $N(y) = 1$ entonces y es una unidad.
- $N(y) = 2$ es imposible porque ya hemos visto que no hay elementos con norma 2.
- Si $N(y) = 4$ entonces y es asociado de x. En efecto como sabemos que

  $$y|x \implies x = ay \implies N(x) = 4 = N(a)N(y) = 4N(a)$$

  es decir, $N(a) = 1$, luego a es una unidad y por tanto $y = xa^-1 \implies x|y$.

Con esto hemos probado que 2 es irreducible.
De igual modo se puede ver que los elementos con modulo 6 o 9 son irreducibles, en particular lo son todos los factores de la igualdad

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Pero ninguno de ellos es primo. En concreto, de la igualdad se deduce que

$$2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$$

y es claro que $2 \nmid (1 + \sqrt{-5})$ y $2 \nmid (1 - \sqrt{-5})$.

3.3.1 Divisibilidad en términos de ideales principales

Todas las nociones de divisibilidad que hemos presentado pueden enunciarse en terminos de los ideales principales generados por los elementos involucrados.

Proposition 3.3.9

Si D es un dominio y $a, b \in D$ entonces se verifican las siguientes propiedades:

(1) $a = 0$ si y solo si $(a) = 0$.

(2) $a \in D^*$ si y solo si $(a) = D$.

(3) $a \mid b$ si y solo si $(b) \subseteq (a)$ (o si $b \in (a)$).

(4) a y b son asociados si y solo si $(a) = (b)$.

(5) a es primo si y solo si (a) es un ideal primo no nulo de D.

(6) a es irreducible si y solo si (a) es maximal entre los ideales principales propios no nulos de D; es decir, $a \neq 0$ y $(a) \subseteq (b) \subset D$ implica $(a) = (b)$.

Proof

(1) Si $a = 0$ entonces $(a) = \{0\} = 0$. Recíprocamente, si $(a) = 0$ entonces $a \in \{0\} \implies a = 0$.

(2) Si a es unidad, existe $a^{-1} \in D$ tal que $aa^{-1} = 1$, luego $1 \in (a)$ y $(a) = D$. Recíprocamente, si $(a) = D$, entonces $1 \in (a)$, luego existe $b \in D$ tal que $ab = 1$, por lo que a es unidad.

(3) Si $a \mid b$, existe $c \in D$ tal que $b = ac$, luego $b \in (a)$ y $(b) \subseteq (a)$. Recíprocamente, si $(b) \subseteq (a)$, entonces $b \in (b) \subseteq (a)$, luego existe $c \in D$ tal que $b = ac$, es decir, $a \mid b$.

(4) Si a y b son asociados, entonces $a \mid b$ y $b \mid a$, luego $(b) \subseteq (a)$ y $(a) \subseteq (b)$, es decir, $(a) = (b)$. Recíprocamente, si $(a) = (b)$, entonces por (3) $a \mid b$ y $b \mid a$.

(5) Si a es primo, entonces $a \neq 0$ y si $bc \in (a)$, entonces $a \mid bc$, luego $a \mid b$ o $a \mid c$, es decir, $b \in (a)$ o $c \in (a)$. Recíprocamente, si (a) es primo no nulo, entonces $a \neq 0$ y si $a \mid bc$, entonces $bc \in (a)$, luego $b \in (a)$ o $c \in (a)$, es decir, $a \mid b$ o $a \mid c$.

(6) Si a es irreducible y $(a) \subseteq (b) \subset D$, entonces $a \in (b)$, luego existe $c \in D$ tal que $a = bc$. Como a es irreducible, b es unidad o c es unidad. Si b es unidad, entonces $(b) = D$, contradiccion. Luego c es unidad y a y b son asociados, por lo que $(a) = (b)$. Recíprocamente, si $a = bc$, entonces $(a) \subseteq (b)$. Si b no es unidad, entonces $(b) \subset D$, luego por hipotesis $(a) = (b)$, por lo que a y b son asociados y c es unidad.

Remark. ***Pregunta para el lector:*** *¿en algún momento hemos usado que D es un dominio?*
Respuesta del autor: *Yo diría que en ningún momento, pero como no estoy seguro rezo porque siempre que tenga que usar esta proposición esté trabajando con un dominio...*

3.3.2 Máximo común divisor y mínimo común múltiplo

Definition 3.3.10

Sea A un anillo y sean S un subconjunto de A y $a \in A$.

(1) a es un máximo común divisor de S en A si a es divisor de cada elemento de S, y múltiplo de cada elemento de A que sea divisor de todos los elementos de S.

(2) a es un mínimo común múltiplo de S en A si a es múltiplo de cada elemento de S, y divisor de cada elemento de A que sea múltiplo de todos los elementos de S.

Obsérvese que no hablamos del máximo común divisor ni del mínimo común múltiplo, sino que en ambos casos usamos el articulo indeterminado un. En la siguiente proposición se precisa por qué tenemos que usar el articulo indeterminado y hasta qué punto el máximo común divisor y el mínimo común múltiplo son únicos. Sin embargo, en ocasiones abusaremos del lenguaje diciendo el máximo común divisor o el mínimo común múltiplo, entendiendo que son conceptos que son únicos salvo asociados. Tambien abusaremos del lenguaje escribiendo $d = \text{mcd}(S)$ o $m = \text{mcm}(S)$ queriendo decir en tal caso que d es un máximo común divisor de S en A y que m es un mínimo común múltiplo de S en A, respectivamente.

Proposition 3.3.11

Sea A un anillo y sean S un subconjunto de A y $a, b \in A$. Entonces

(1) a es un máximo común divisor de S en A si y solo si (a) es el menor ideal principal de A que contiene a S. En particular si $(S) = (a)$ entonces a es el máximo común divisor de S.

(2) a es un mínimo común múltiplo de S en A si y solo si (a) es el mayor ideal principal contenido en $\cap_{s \in S}(s)$. En particular, si $(a) = \cap_{s \in S}(s)$ entonces a es mínimo común múltiplo de S.

(3) Sea a un máximo común divisor de S. Entonces b tambien es máximo común divisor de S si y solo si a y b son asociados en A.

(4) Sea a es un mínimo común múltiplo de S. Entonces b tambien es mínimo común múltiplo de S si y solo si a y b son asociados en A.

(5) Si a es un divisor común de los elementos de S y $a \in (S)$ entonces $a = \text{mcd}(S)$.

Obsérvese que la condicion $a \in (S)$ significa que existen elementos $s_1, \dots, s_n \in S$ y $a_1, \dots, a_n \in A$ tales que
$$a = a_1 s_1 + \cdots + a_n s_n.$$
En el caso en que $a = \text{mcd}(S)$ se dice que esta expresion es una identidad de Bezout para S.

(6) Se verifica $1 = \text{mcd}(S)$ si y solo si los unicos divisores comúnes de los elementos de S son las unidades de A.

(7) Si $1 \in (S)$ (o sea, 1 es combinacion lineal de elementos de S) entonces $1 = \text{mcd}(S)$.

Proof

(1) Usando la definicion de máximo común divisor tenemos que si $a = \text{mcd}(S)$, entonces $a|s$ para todo $s \in S$. Entonces, por el apartado (3) de 3.3.9, $(s) \subseteq (a)$ para todo $s \in S$.

Además, dado un ideal principal (b) tal que $S \subseteq (b)$ se verifica

$$s \in S \subseteq (b) \implies s = bc$$

para cualquier elemento $s \in S$. Pero entonces $b|s$, por lo que a debe ser múltiplo de b, es decir $a = bc$, pero entonces $(a) \subseteq (b)$ como queríamos ver.

Por el contrario, supongamos que (a) es el menor ideal principal de A que contiene a S. En concreto $S \subseteq (a)$, por tanto dado $s \in S$

$$s \in (a) \implies s = ac \implies a|s$$

luego a divide a todos los elementos de S. Supongamos que b es otro elemento que también divide a todos, en tal caso

$$b|s \implies (s) \subseteq (b) \implies S \subseteq (b)$$

pero entonces por hipótesis $(a) \subseteq (b)$, por tanto $a = bc$, es decir, a es múltiplo de b, luego $a = \text{mcd}(S)$.

(2) La demostración es similar a (1), omitimos algunos pequeños detalles.

Si a es un mcm entonces dado $s \in S$ tenemos $a = sx_s$, luego $(a) \subseteq (s)$, por tanto

$$(a) \subseteq \cap_{s \in S}(s).$$

Si (b) es otro ideal tal que $(b) \subseteq \cap_{s \in S}(s)$ entonces $(b) \subseteq (s)$, luego $b = sy_s$ para cada s y por la definición de mcm debe ser $a|b$, lo cual implica

$$(b) \subseteq (a)$$

luego (a) es el máximo ideal contenido en la interesección.

Por el contrario, si (a) es el máximo ideal contenido en $\cap_{s \in S}(s)$ entonces $a \in (a) \subseteq (s) \implies a = sx_s$ para cada s. Supongamos que $b = sy_s$ también para todo $s \in S$, en tal caso

$$(b) \subseteq \cap_{s \in S}(s) \implies (b) \subseteq (a) \implies a|a.$$

(3) Claramente si b también es máximo común divisor entonces $a = bc, b = ad$, luego $b|a, a|b$, es decir, a y b son asociados. Si por el contrario $a|b, b|a$ entonces dado $s \in S$, $b|a|s \implies b|s$, y si c es otro elemento que divide a cada s tenemos entonces $a = cx$, pero como $a|b \implies b = ay = cxy$ es decir, b es también un mcd.

(4) Si b también es mínimo común múltiplo entonces $a|b, b|a$, luego a y b son asociados. Si por el contrario $a|b, b|a$ entonces $b = ac$, y dado $s \in S$, $a = sx_s \implies b = scx_s$, y si c es otro elemento que es múltiplo de cada s tenemos entonces $b|a|c$, es decir, b es también un mcm.

(5) Supongamos que a satisface la condicion dada y sea b un elemento de A que divide a todos los elementos de S. Entonces divide a $a_1 s_1 + \cdots + a_k s_k = a$. Esto demuestra que $a = \text{mcd}(S)$.

(6) Si $1 = \text{mcd}(S)$ y d es un divisor común de los elementos de S, entonces $d \mid 1$, luego d es unidad. Recíprocamente, si los unicos divisores comunes son unidades, entonces 1 es un máximo común divisor.

(7) Es consecuencia inmediata de (5).

Example 3.3.12

Los recíprocos de las propiedades (5) y (7) no se verifican. Por ejemplo, los unicos divisores comunes de 2 y X en $\mathbb{Z}[X]$ son 1 y -1, es decir las unidades de $\mathbb{Z}[X]$. Por tanto, $1 = \text{mcd}(2, X)$. Sin embargo, $1 \notin (2, X)$.

Definition 3.3.13: Coprimos

Si $1 = \text{mcd}(S)$ decimos que los elementos de S son coprimos en A. Si para cada par de elementos distintos $a, b \in S$ se verifica $\text{mcd}(a, b) = 1$, decimos que los elementos de S son coprimos dos a dos.

3.4 Dominios de factorización única

Definition 3.4.1: Factorización en irreducibles

Sea D un dominio. Una factorización en producto de irreducibles de un elemento a de D es una expresión del tipo

$$a = up_1 \cdots p_n$$

donde $n \in \mathbb{Z}^{\geq 0}$, u es una unidad de D y $p_1, \dots, p_n$ son irreducibles de D. Obsérvese que se admite la posibilidad de que sea $n = 0$, en cuyo caso la factorización se reduce a $a = u$ ya que, por convenio, el producto vacío es 1.

Definition 3.4.2: Dominio de factorización

Diremos que D es un dominio de factorización o DF si todo elemento no nulo de D admite una factorización en producto de irreducibles.

Dos factorizaciones de $a \in D$ en producto de irreducibles se dice que son equivalentes si solo se diferencian en el orden y en asociados. Dicho con más rigor, las factorizaciones

$$a = up_1 \cdots p_n = vq_1 \cdots q_m$$

(con $u, v \in D^*$ y el resto de factores irreducibles) son equivalentes si $n = m$ y existe una permutación σ de N_n (una biyección de $N_n = \{1, 2, \dots, n\}$ en sí mismo) tal que p_i y $q_{\sigma(i)}$ son asociados para cada $i = 1, \dots, n$.

Definition 3.4.3: Dominio de factorización única

Diremos que D es un dominio de factorización única o DFU (UFD, en inglés) si es un dominio de factorización en el que, para cada $0 \neq a \in D$, todas las factorizaciones de a son equivalentes.

Example 3.4.4

El Teorema Fundamental de la Aritmética simplemente nos dice que el anillo de los números enteros $\mathbb{Z}$ es un DFU.

Example 3.4.5

Sea m un entero positivo. Vamos a ver que $\mathbb{Z}[\sqrt{m}]$ es un dominio de factorización. Si m es un cuadrado en $\mathbb{Z}$ entonces $\mathbb{Z}[\sqrt{m}] = \mathbb{Z}$ que es un dominio de factorización. Por tanto, a partir de ahora suponemos que m no es un cuadrado en $\mathbb{Z}$ y siempre que utilicemos una expresión $a + b\sqrt{m}$ suponemos implícitamente que a y b son enteros. Vamos a utilizar la conjugación en $\mathbb{Z}[\sqrt{m}]$ que es la siguiente aplicación (si m es negativo, esta aplicación es la conjugación compleja, si m es positivo entonces es una aplicación diferente, que también llamaremos conjugación).

$$\overline{(\cdot)} : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z}[\sqrt{m}], \quad a + b\sqrt{m} \mapsto \overline{a + b\sqrt{m}} = a - b\sqrt{m}$$

Es fácil comprobar que esta aplicación es un homomorfismo de anillos. Además, la siguiente aplicación

$$N : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z}, \quad a + b\sqrt{m} \mapsto a^2 - b^2 m = (a + b\sqrt{m})(a - b\sqrt{m})$$

satisface $N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[\sqrt{m}]$ ya que

$$N(xy) = (xy)\overline{(xy)} = x\overline{x}y\overline{y} = N(x)N(y)$$

usando que la conjugación es un homomorfismo.
Sea $x \in \mathbb{Z}[\sqrt{m}]$. Si x es invertible en $\mathbb{Z}[\sqrt{m}]$ entonces $1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$ con lo que $N(x)$ es invertible en $\mathbb{Z}$, es decir $N(x) = \pm 1$. Recíprocamente, si $N(x) = \pm 1$, entonces $x\overline{x} = \pm 1$, con lo que x es invertible en $\mathbb{Z}[\sqrt{m}]$. Esto demuestra que las unidades son los elementos de norma ± 1

$$\mathbb{Z}[\sqrt{m}]^* = \{x \in \mathbb{Z}[\sqrt{m}] : |N(x)| = 1\}.$$

Vamos a demostrar que si $x \neq 0$ entonces tiene una factorización en $\mathbb{Z}[\sqrt{m}]$ por inducción en $|N(x)|$. Observese que $N(x) \neq 0$ pues si $a^2 - b^2 m = 0$ entonces m es un cuadrado en $\mathbb{Z}$ en contra de la hipótesis. Por tanto, el menor valor posible para $|N(x)|$ es 1 y en el caso en que $|N(x)| = 1$ entonces x es una unidad con lo que efectivamente tiene una factorización. Asumamos pues la hipótesis de inducción y supongamos que $|N(x)| > 1$. Entonces x no es unidad. Si x es irreducible por supuesto que tiene una factorización con lo que podemos suponer que x no es irreducible. Por tanto $x = ab$ con a y b no unidades. Por tanto $|N(a)|$ y $|N(b)|$ son divisores propios de $|N(x)|$ y por hipótesis de inducción a y b son productos de irreducibles. Luego x también es producto de irreducibles.

En el siguiente lema vemos que en un DFU los elementos irreducibles coinciden con los primos.

Lemma 3.4.6

Si D es un DFU, entonces todo elemento irreducible de D es primo.

Proof

Sea $p \in D$ irreducible, y sean $a, b \in D$ tales que $p \mid ab$. Se trata de ver que $p \mid a$ o $p \mid b$. Esto está claro si $a = 0$ o $b = 0$ con lo que suponemos que ambos son diferentes de 0. Por hipótesis $pt = ab$ para algún $t \in D$. Si $t = wp_1 \cdots p_n$, $a = vq_1 \cdots q_m$ y $b = ur_1 \cdots r_k$ son factorizaciones en irreducibles (con $w, v, u \in D^*$), entonces se tiene

$$pt = tp = wp_1 \cdots p_n p = (vu)q_1 \cdots q_m r_1 \cdots r_k,$$

y por la unicidad de la factorización p es asociado de algún q_i (y entonces $p \mid a$) o de algún

r_i (y entonces $p \mid b$).

Según hemos visto en el Ejemplo 3.4.5 $\mathbb{Z}[\sqrt{-5}]$ es un DF. Sin embargo, en el Ejemplo 3.3.7 hemos visto que tiene elementos irreducibles no primos, y por tanto no es DFU.

Introducimos ahora una definición muy similar a la de factorización en irreducibles.

Definition 3.4.7: Factorización en primos

Sea D un dominio. Una factorización en producto de primos de un elemento a de D es una expresión del tipo

$$a = up_1 \cdots p_n$$

donde $n \in \mathbb{Z}^{\geq 0}$, u es una unidad de D y $p_1, \ldots, p_n$ son primos de D. Obsérvese que se admite la posibilidad de que sea $n = 0$, en cuyo caso la factorización se reduce a $a = u$ ya que, por convenio, el producto vacío es 1.

Proposition 3.4.8

Para un dominio D, las condiciones siguientes son equivalentes:

(1) D es un dominio de factorización única.

(2) D es un dominio de factorización en el que todo elemento irreducible es primo.

(3) Todo elemento no nulo de D es producto de primos.

Proof

(1) $\Rightarrow$ (2): Por ser un DFU, D es en concreto un DF. Además, por el Lema 3.4.6 todo elemento irreducible es primo, como queríamos ver.
(2) $\Rightarrow$ (3): Sea $0 \neq a \in D$, como D es DF a admite una factorización en producto de irreducibles

$$a = up_1 \ldots p_n$$

y por hipótesis todos los elementos irreducibles son primos, luego los p_i son primos y por tanto a es producto de primos (salvo la unidad u).
(3) $\Rightarrow$ (1): Sea $0 \neq a \in D$, por hipótesis sabemos que a es producto de primos, luego

$$a = up_1 \cdots p_k.$$

Como todo primo es irreducible esta es también una factorización en producto de irreducibles, luego D es un dominio de factorización. Supogamos que existe otra factorización

$$a = u'q_1 \cdots q_l.$$

Entonces deducimos que

$$p_1 \cdots p_k = (u'u^{-1})q_1 \cdots q_l$$

con $w = u'u^{-1}$ una unidad. Razonamos por inducción sobre k. Si $k = 0$ entonces necesariamente $l = 0$. Supongamos que $k > 0$ y que la propiedad se verifica para factorizaciones con menos de k primos. Como p_k es primo y divide a $q_1 \cdots q_l$ se tiene que p_k divide a algún q_i y podemos suponer que p_k divide a q_l. Como q_l es irreducible necesariamente p_k y q_l son asociados. Escribiendo $q_l = vp_k$ y cancelando p_k obtenemos $p_1 \cdots p_{k-1} = (wv)q_1 \cdots q_{l-1}$. Por la hipótesis de inducción estas dos factorizaciones son equivalentes con lo que $k = l$ y después de reordenar los q_i podemos suponer que p_i es asociado de q_i para todo $i = 1, \ldots, k$.

Theorem 3.4.9: Máximo común divisor y mínimo común múltiplo en un DFU

Si D es un DFU entonces $\forall a, b \in D$ existen $\operatorname{mcd}(a, b), \operatorname{mcm}(a, b)$.

Proof

En primer lugar, vamos a ver que existe un conjunto de representantes P de irreducibles tal que cualquier $0 \neq a \in D$ se escribe como

$$a = u \prod_{p \in P} p^{\alpha_p(a)},$$

donde u es una unidad, $\alpha_p(a) \in \mathbb{Z}^{\geq 0}$ y solo un número finito de α_p es distinto de 0.
Sea $\mathcal{I}$ el conjunto de todos los elementos irreducibles de D. Definimos en $\mathcal{I}$ la relación de equivalencia:

$$p \sim q \iff p \text{ es asociado de } q$$

Por el axioma de elección, podemos elegir exactamente un elemento de cada clase de equivalencia de $\mathcal{I}/\sim$. Llamemos P a este conjunto de representantes.
Ahora, sea $0 \neq a \in D$, entonces

$$a = vq_1 \cdots q_n$$

con cada q_i irreducible, pero entonces cada uno de ellos es asociado de algún $p \in P$, luego $q_i = u_i p_i$ para cada i, es decir,

$$a = (vu_1 \cdots u_n)p_1 \cdots p_n = u \prod_{p \in P} p^{\alpha_p(a)}$$

donde la última igualdad se obtiene agrupando todas las unidades y agrupando cada $p_i \in P$. Cada número $\alpha_p(a)$ corresponde al número de veces que aparece un elemento asociado a p en la factorización de a. Como hay un número finito de q_i en la factorización, está claro que casi todos los $\alpha_p(a)$ son 0.
Sean $a, b \in D$, por hipótesis a y b tienen factorizaciones únicas en irreducibles, luego

$$a = u \prod_{p \in P} p^{\alpha_p}, \quad b = v \prod_{p \in P} p^{\beta_p}.$$

Probemos ahora la existencia de mcd y mcm.

- Sea $\gamma_p = \min(\alpha_p, \beta_p)$, entonces

  $$d = \prod_{p \in P} p^{\gamma_p}$$

  divide a ambos a, b, y si c es otro divisor de ambos entonces

  $$c = u_c \prod_{p \in P} p^{\delta_p} \mid a, b \implies \delta_p \leq \alpha_p, \beta_p \implies \delta_p \leq \min(\alpha_p, \beta_p) = \gamma_p$$

  es decir, $c \mid d$. Por tanto, d es un mcd de a, b.

- Definimos

  $$m = \prod_{p \in P} p^{\mu_p}, \quad \mu_p = \max(\alpha_p, \beta_p).$$

  Como $\mu_p \geq \alpha_p$ y $\mu_p \geq \beta_p$ y u, v son unidades entonces $a \mid m$ y $b \mid m$. Además, si $a \mid t$ y $b \mid t$, podemos escribir

  $$t = u_t \prod_p p^{\tau_p}.$$

  Sabemos que $a \mid t$ implica $\alpha_p \leq \tau_p$, $b \mid t$ implica $\beta_p \leq \tau_p$, luego $\max(\alpha_p, \beta_p) = \mu_p \leq \tau_p$. Así $m \mid t$.

  Por tanto, m es un mcm de a y b.

3.5 Dominios de ideales principales

Definition 3.5.1: Dominio de ideales principales

Un dominio de ideales principales, o DIP (PID, en la literatura en ingles), es un dominio en el que todos los ideales son principales.

Proposition 3.5.2

Si D es un DIP y $0 \neq a \in D \setminus D^*$, las siguientes condiciones son equivalentes:

(1) a es irreducible.

(2) (a) es un ideal maximal.

(3) $D/(a)$ es un cuerpo.

(4) a es primo.

(5) (a) es un ideal primo.

(6) $D/(a)$ es un dominio.

Proof

(1) $\Leftrightarrow$ (2): Por la Proposición 3.3.9, a es irreducible si y solo si (a) es maximal entre los ideales principales propios. Pero como D es DIP, todo ideal es principal, luego (a) es maximal entre todos los ideales propios, es decir, es maximal.
(2) $\Leftrightarrow$ (3): Por un resultado previo, (a) es maximal si y solo si $D/(a)$ es cuerpo.
(4) $\Leftrightarrow$ (5): Por la Proposición 3.3.9, a es primo si y solo si (a) es primo.
(5) $\Leftrightarrow$ (6): Por un resultado previo, (a) es primo si y solo si $D/(a)$ es dominio.
(2) $\Rightarrow$ (5): Por un resultado previo, todo ideal maximal es primo.
(4) $\Rightarrow$ (1): En cualquier dominio, todo elemento primo es irreducible.

Remark. Hemos probado $(1) \Leftrightarrow (2) \Leftrightarrow (3)$ *y* $(4) \Leftrightarrow (5) \Leftrightarrow (6)$*, por tanto solo hace falta probar que alguno de los 3 primeros implica alguno de los 3 últimos y viceversa.*

Theorem 3.5.3: DIP implica DFU

Todo dominio de ideales principales D es un dominio de factorizacion unica.

Proof

Por la Proposición 3.5.2 sabemos que al ser D un DIP los elementos irreducibles son primos. Por la Proposición 3.4.8 basta entonces con demostrar que D es un dominio de factorizacion.
Por reducción al absurdo supongamos que D no lo es. Vamos a construir, por recurrencia, una sucesion $a_1, a_2, \ldots$ de elementos de D que no admiten factorizacion y tales que

$$(a_1) \subset (a_2) \subset \cdots$$

es una cadena estrictamente creciente de ideales de D.
Para el primer paso simplemente elegimos un elemento arbitrario a_1 de D que no admita factorizacion en irreducibles. Supongamos ahora que hemos elegido $a_1, \ldots, a_n$ satisfaciendo las condiciones requeridas. Entonces a_n no es irreducible, luego existen

$x, y \in D \setminus D^*$ tales que $a_n = xy$. Como a_n no es producto de irreducibles, al menos uno de los factores x o y (digamos que x) no es producto de irreducibles. Entonces, poniendo $a_{n+1} = x$, tenemos $(a_n) \subset (a_{n+1})$ con la inclusion estricta porque y no es una unidad.
Una vez construida la sucesion (a_i), tomamos $I = (a_1, a_2, \ldots) = \cup_{i \in \mathbb{Z}^+}(a_i)$ (dejamos que el lector compruebe la igualdad anterior). Como D es un DIP, existe $x \in D$ tal que $I = (x)$; en particular $x \in I = \cup_{i \in \mathbb{Z}^+}(a_i)$ y por tanto existe un indice i tal que $x \in (a_i)$; como es claro que $a_i \in (x)$, se tiene $(a_i) = (x) = I$ y por lo tanto $(a_i) = (a_{i+1})$, en contra de la construccion realizada. Este absurdo concluye la demostracion.

El reciproco del Teorema 3.5.3 es falso: $\mathbb{Z}[X]$ es un DFU que no es un DIP. Que no es DIP se sigue del Ejemplo 2.5.5. La demostracion de que $\mathbb{Z}[X]$ es DFU es bastante mas complicada y tambien es consecuencia de un resultado mas general. La veremos en el Capítulo 4.

Example 3.5.4

El anillo de los enteros $\mathbb{Z}$ es un DIP. Todo ideal de $\mathbb{Z}$ es de la forma (n) para algún $n \in \mathbb{Z}$.

Example 3.5.5

Si K es un cuerpo, entonces K es un DIP trivialmente, pues sus únicos ideales son (0) y (1).

Example 3.5.6

Si K es un cuerpo, entonces $K[[X]]$ es un DIP, pues sus ideales no nulos son de la forma (X^n) para algún $n \in \mathbb{N}$.

Proof

Sea K un cuerpo y sea $I \subseteq K[[X]]$.
En primer lugar, probaremos que las unidades de $K[[X]]$ son las series de potencias con primer término no nulo.

Proof

Claramente para ser invertible, una serie de potencias $f = \sum_{n=0}^{\infty} a_n X^n$ debe cumplir $a_0 \neq 0$, puesto que la serie con $a_1 = 1, a_n = 0$ si $n \neq 1$ no es invertible.
Por otro lado, si una serie verifica $a_0 \neq 0$ entonces la serie

$$\sum_{n=0}^{\infty} b_n X^n$$

construida haciendo $a_0 b_0 = 1, \sum_{k=0}^{n} a_k b_{n-k} = 0$, es decir,

$$b_0 = \frac{1}{a_0}, b_1 = \frac{a_1 b_0}{a_0}, \dots, b_n = \frac{\sum_{k=1}^{n} a_k b_{n-k}}{a_0}, \dots$$

verifica que

$$(\sum_{n=0}^{\infty} a_n X^n)(\sum_{n=0}^{\infty} b_n X^n) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n = 1.$$

Luego f es invertible.

Pasamos a demostrar el ejemplo. Si $I = (0)$ es principal. De igual manera, si existe alguna serie en I con $0 \neq a_0$ entonces la serie es invertible y por tanto $I = (X^0) = (1) = K[[X]]$, luego I es principal.
Supongamos por tanto que todas las series de I tienen $a_0 = 0$. Sean $m \in \mathbb{N}$ el menor número natural tal que existe una serie con $a_m = 0$ (este número ha de existir puesto que en caso contrario $I = (0)$). Entonces cualquier $f \in I$ es de la forma

$$f = X^m (\sum_{n=0}^{\infty} a_n X^n)$$

y finalmente $I = (X^m)$ como queríamos ver.

En la sección 3.6 estudiaremos los dominios euclídeos y probraremos que todo dominio euclídeo es un DIP, por tanto, todos los ejemplos de la siguiente sección valen también para esta.

3.6 Dominios euclídeos

Definition 3.6.1: Función euclídea

Una funcion euclidea en D es una aplicacion $\delta : D \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ que cumple las siguientes condiciones:

(DE1) Si $a, b \in D \setminus \{0\}$ verifican $a \mid b$ entonces $\delta(a) \leq \delta(b)$.

(DE2) Dados $a, b \in D$ con $b \neq 0$, existen $q, r \in D$ tales que $a = bq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(b)$.

Un dominio euclideo es un dominio que admite una funcion euclidea.

Example 3.6.2

El valor absoluto es una funcion euclidea en $\mathbb{Z}$. En efecto, si $a, b \in \mathbb{Z}$ con $b \neq 0$, existen $q, r \in \mathbb{Z}$ tales que $a = bq + r$ con $0 \leq r < |b|$, luego se cumple (DE2). Ademas, si $a \mid b$, $a, b \neq 0$ entonces

$$b = ax,\ x \neq 0 \implies |b| = |a||x|,\ |x| \geq 1 \implies |a| \leq |b|$$

luego se cumple (DE1).

Example 3.6.3

Si K es un cuerpo, entonces el grado define una función euclídea en $K[X]$. En efecto, la condicion (DE1) se verifica claramente.
Para demostrar que se verifica la condicion (DE2) tomamos $a, b \in K[X] \setminus \{0\}$ con $b \neq 0$. Si $a = 0$ tomando $q = r = 0$ se tiene que $a = bq + r$. Por tanto, suponemos que $a \neq 0$ y denotamos por n al grado de a y por m al grado de b.
Razonamos por inducción en n. Si $n < m$ podemos tomar $q = 0$ y $r = a$

$$a = r = 0 + r = bq + r$$

luego solo tenemos que estudiar los casos $m \leq n$.
Si $n = m = 0$ ambos polinomios son constantes, tomamos $q = ab^{-1}$ y $r = 0$ (recordemos que b es invertible al ser constante no nulo). Esto incluye el menor valor posible para n, o sea $n = 0$.
Ahora, para el caso n, por hipótesis de inducción se tiene que para todo polinomio c de grado menor que n existen q' y r' en $K[X]$ con $c = q'b + r'$ y o bien $r' = 0$ o r' tiene grado menor que b. Aplicamos esto a

$$c = a - \alpha\beta^{-1}X^{n-m}b,$$

donde α es el termino principal de a y β es el termino principal de b. Es facil ver que c tiene grado menor que a con lo que tenemos

$$a - \alpha\beta^{-1}X^{n-m}b = c = q'b + r' \implies a = (q' + \alpha\beta^{-1}X^{n-m})b + r'.$$

Tomando $q = q' + \alpha\beta^{-1}X^{n-m}$ se tiene que $a = qb + r$, como deseabamos.

Example 3.6.4

El cuadrado del modulo complejo define una funcion euclidea en el anillo $\mathbb{Z}[i]$. En efecto, si $x = a + bi$ con a y b numeros enteros entonces

$$\delta(x) = |x|^2 = a^2 + b^2 \in \mathbb{Z}^{\geq 0}.$$

Además, $\delta(x) = 0$ si y solo si $x = 0$ y $\delta(xy) = \delta(x)\delta(y)$ de donde facilmente se deduce que δ verifica (DE1).
Sean ahora $a = a_1 + a_2 i$ y $b = b_1 + b_2 i \neq 0$ con $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Sea

$$x = x_1 + x_2 i = \frac{a}{b}.$$

Elegimos dos numeros enteros q_1 y q_2 lo mas próximos posible a x_1 y x_2 respectivamente y ponemos $q = q_1 + q_2 i$. De la eleccion de los q_i tenemos que $|x_i - q_i| \leq \frac{1}{2}$. Sea $r = a - bq$, por tanto $a = bq + r$ y si $r \neq 0$

$$\delta(r) = |a - bq|^2 = |b|^2|x - q|^2 = \delta(b)((x_1 - q_1)^2 + (x_2 - q_2)^2) \leq \delta(b)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{\delta(b)}{2} < \delta(b).$$

Lemma 3.6.5

Sea δ una funcion euclidea en D, sea I un ideal de D y a un elemento de I diferente de 0. Entonces $I = (a)$ si y solo si para todo $x \in I$ se cumple $\delta(a) \leq \delta(x)$.

Proof

Supongamos que $I = (a)$ y sea $x \in I$. Entonces $x = ab \implies a \mid x$, luego de (DE1) deducimos que $\delta(a) \leq \delta(x)$.
Para demostrar el recíproco supongamos que para todo $x \in I$, $\delta(a) \leq \delta(x)$. Notemos que como $a \in I$ se tiene que $(a) \subseteq I$. Para probar el otro contenido imitamos la demostracion de que $\mathbb{Z}$ es DIP. Sea $x \in I$, por (DE2) existen $q, r \in D$ tales que $x = aq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(a)$. Entonces

$$r = x - aq \in I,$$

por tanto, $\delta(a) \leq \delta(r)$ por hipótesis. Finalmente ha de ser $r = 0$, con lo que $x \in (a)$. Esto demuestra que $I = (a)$.

Del Lema anterior se deduce de forma inmediata el siguiente resultado:

Theorem 3.6.6

Todo dominio euclideo es DIP.

Proof

Sea D un dominio euclideo con funcion euclidea δ, y sea I un ideal de D. Si $I = 0$, entonces $I = (0)$ es principal. Si $I \neq 0$, sea

$$\mathcal{A} = \{\delta(x) : x \in I \setminus \{0\}\} \subseteq \mathbb{Z}^{\geq 0}.$$

Por el principio de buena ordenación $\mathcal{A}$ tiene un mínimo, luego existe $a \in I \setminus \{0\}$ tal que $\forall x \in I \quad \delta(a) \leq \delta(x)$. Por el Lema 3.6.5, $I = (a)$, luego I es principal.

Lemma 3.6.7

Si δ es una funcion euclidea en D entonces las siguientes condiciones son equivalentes para $a \in D \setminus \{0\}$:

(1) a es una unidad de D.

(2) $\delta(a) = \delta(1)$.

(3) $\delta(a) \leq \delta(x)$, para todo $x \in D \setminus \{0\}$.

Proof

(1) $\Rightarrow$ (2): Si a es unidad, entonces

$$aa^{-1} = 1, a = 1a$$

luego $a \mid 1$ y $1 \mid a$, luego por (DE1) tenemos $\delta(a) = \delta(1)$.
(2) $\Rightarrow$ (3): Sea $x \in D \setminus \{0\}$. Como $1 \mid x$, por (DE1) tenemos $\delta(1) \leq \delta(x)$, luego $\delta(a) = \delta(1) \leq \delta(x)$.
(3) $\Rightarrow$ (1): Aplicando (DE2) a 1 y a, existen $q, r \in D$ tales que $1 = aq + r$ con $r = 0$ o $\delta(r) < \delta(a)$. Pero, por (3), $\delta(a) \leq \delta(r)$ si $r \neq 0$, luego necesariamente $r = 0$ y $1 = aq$, por lo que a es unidad.

Example 3.6.8

El anillo $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ es un dominio euclideo con la funcion $\delta(a + b\sqrt{2}) = |a^2 - 2b^2|$.

Proof

Si $x = a + b\sqrt{2}$ con $a, b \in \mathbb{Z}$, entonces

$$\delta(x) = |a^2 - 2b^2| \in \mathbb{Z}^{\geq 0}.$$

Además, $\delta(x) = 0$ si y solo si

$$a^2 = 2b^2 \iff a = b = 0$$

ya que si $b \neq 0$ entonces 2 sería un cuadrado perfecto en $\mathbb{Q}$. Por otro lado, si $x \mid y$ entonces

$$y = xz, \quad z \in \mathbb{Z}[\sqrt{2}]$$

Denotando $\bar{x} = a - b\sqrt{2}$ deducimos fácilmente que

$$\delta(y) = y\bar{y} = x\bar{x}z\bar{z} = \delta(x)\delta(z) \implies \delta(x) \leq \delta(y)$$

luego δ verifica (DE1).
Sean ahora $a = a_1 + a_2\sqrt{2}$ y $b = b_1 + b_2\sqrt{2} \neq 0$ con $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Sea

$$x = x_1 + x_2\sqrt{2} = (a_1 + a_2\sqrt{2}) \left(\frac{b_1 - b_2\sqrt{2}}{|b_1^2 - 2b_2^2|} \right).$$

Notemos entonces que

$$xb = (a_1 + a_2\sqrt{2}) \left(\frac{b_1^2 - 2b_2^2}{|b_1^2 - 2b_2^2|} \right) = \pm a$$

luego $a = by$, donde $y = \pm x$ según sea $xb = a$ o $xb = -a$.
Elegimos dos numeros enteros q_1 y q_2 lo mas próximos posible a y_1 y y_2 respectivamente y ponemos $q = q_1 + q_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. De la eleccion de los q_i tenemos que $|y_i - q_i| \leq \frac{1}{2}$. Sea $r = a - bq$, por tanto $a = bq + r$ y si $r \neq 0$

$$\delta(r) = \delta(a - bq) = \delta(by - bq) = \delta(b)\delta(y - q)$$

pero

$$\delta(y - q) = |(y_1 - q_1)^2 - 2(y_2 - q_2)^2| \leq (y_1 - q_1)^2 + 2(y_2 - q_2)^2 \leq \frac{1}{4} + \frac{1}{2} < 1$$

por tanto

$$\delta(r) < \delta(b)$$

lo que confirma que se verifica (DE2).

Example 3.6.9

El anillo $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$ es un dominio euclideo con la funcion $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$. La demostración es casi igual a la del ejemplo anterior.

Example 3.6.10

No todo DIP es euclideo. El anillo $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ es un DIP pero no es euclideo. La demostracion de este hecho es bastante técnica.

Remark. La definicion de dominio euclideo no requiere que la funcion euclidea satisfaga $\delta(ab) = \delta(a)\delta(b)$ *o* $\delta(ab) \geq \delta(a)$. *Estas propiedades se verifican en los ejemplos clasicos pero no son parte de la definicion.*

Remark. En algunos textos se exige que la funcion euclidea satisfaga $\delta(a) \leq \delta(ab)$ *para todo* $a, b \neq 0$. *Esta condicion es mas restrictiva pero muchas funciones euclideas naturales la satisfacen.*

3.7 El cuerpo de fracciones de un dominio

A lo largo de toda la sección D *es un dominio.*

Ya sabemos que todo subanillo de un cuerpo es un dominio. En esta sección vamos a ver que el recíproco es cierto, es decir, todo dominio D es un subanillo de un cuerpo. De hecho, existe un cuerpo que, en cierto sentido, es el menor cuerpo que contiene a D. Dicho cuerpo es único salvo isomorfismos y se llama el cuerpo de fracciones de D. Comenzaremos con la construcción de ese cuerpo, que es una traducción literal de la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$, y analizaremos entonces sus propiedades. La idea de la construcción es la de formar un cuerpo $Q(D)$ cuyos elementos sean «fracciones» del tipo a/b con $a, b \in D$ y $b \neq 0$. De este modo, D estara contenido en $Q(D)$ (identificando cada elemento a de D con la fraccion $a/1$), y los elementos no nulos de $Q(D)$ seran invertibles, pues si $a, b \in D \setminus \{0\}$, entonces b/a sera el inverso de a/b. Por supuesto, hay que definir con mas rigor las fracciones y hay que dotar a $Q(D)$ de una estructura de cuerpo. El primer problema que se presenta, si pensamos en el caso $D = \mathbb{Z}$ y $Q(D) = \mathbb{Q}$, es el hecho de que dos fracciones aparentemente distintas pueden representar el mismo elemento, como en el caso $10/15 = 2/3$. Esto se resuelve identificando ciertas fracciones mediante una relacion de equivalencia, y este sera el primer paso en nuestra construccion.

Definition 3.7.1: Cuerpo de fracciones

El cuerpo de fracciones o cuerpo de cocientes del dominio D es el cuerpo $Q(D)$ construido como el conjunto de clases de equivalencia de pares (a, s) con $a \in D$, $s \in D \setminus \{0\}$ bajo la relación $(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1$, con las operaciones:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \qquad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}.$$

Proposition 3.7.2

Las operaciones definidas sobre $Q(D)$ están bien definidas.

Proof

Supongamos que $a_1/s_1 = b_1/t_1$ y $a_2/s_2 = b_2/t_2$, por tanto

$$a_1 t_1 = b_1 s_1, \quad a_2 t_2 = b_2 s_2 \tag{$\star$}$$

veamos ahora ambas operaciones.

- Suma:
$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$$
$$\frac{b_1}{t_1} + \frac{b_2}{t_2} = \frac{b_1 t_2 + b_2 t_1}{t_1 t_2}$$
entonces
$$(a_1 s_2 + a_2 s_1, s_1 s_2) \sim (b_1 t_2 + b_2 t_1, t_1 t_2) \iff (a_1 s_2 + a_2 s_1) t_1 t_2 = (b_1 t_2 + b_2 t_1) s_1 s_2$$
para comprobar la igualdad del lado derecho basta usar ($\star$)
$$(a_1 s_2 + a_2 s_1) t_1 t_2 = a_1 t_1 s_2 t_2 + a_2 t_2 s_1 t_1 = b_1 s_1 s_2 t_2 + b_2 s_2 s_1 t_1 = (b_1 t_2 + b_2 t_1) s_1 s_2$$
por tanto la suma está bien definida.
- Producto:
$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$$

$$\frac{b_1}{t_1}+\frac{b_2}{t_2}=\frac{b_1b_2}{t_1t_2}$$

entonces

$$(a_1a_2, s_1s_2) \sim (b_1b_2, t_1t_2) \iff (a_1a_2)t_1t_2 = (b_1b_2)s_1s_2$$

para comprobar la igualdad del lado derecho basta usar ($\star$)

$$(a_1a_2)t_1t_2 = a_1t_1a_2t_2 = b_1s_1b_2s_2 = (b_1b_2)s_1s_2$$

por tanto el producto está bien definido.

Proposition 3.7.3

Si D es un dominio entonces $Q(D)$ es un cuerpo con la suma y multiplicación definidas anteriormente. Dados $a, b, s, t \in D$ con $s, t \neq 0$, se tiene:

(1) El cero de $Q(D)$ es $0/1$. Además, la igualdad $a/s = 0/1$ se verifica si y solo si $a = 0$.

(2) El uno de $Q(D)$ es $1/1$. Además, la igualdad $a/s = 1/1$ se verifica si y solo si $a = s$.

(3) $at/st = a/s$.

(4) La igualdad $a/s = b/s$ se verifica si y solo si $a = b$.

(5) La definición de suma se simplifica cuando hay "denominador común": $a/s + b/s = (a+b)/s$.

Proof

Probaremos las propiedades para después usarlas al justificar que $Q(D)$ es un cuerpo. En primer lugar, notemos que si $a = b \implies as = bs \implies \frac{a}{s} = \frac{b}{s}$, animamos al lector a fijarse en los pasos que usan este hecho.

(1) Claramente

$$\frac{a}{s}+\frac{0}{1}=\frac{a}{s}$$

y

$$\frac{a}{s}=\frac{0}{1} \iff a1 = s0 = 0 \iff a = 0.$$

(2)

$$\frac{a}{s}\cdot\frac{1}{1}=\frac{a}{s}$$

y

$$\frac{a}{s}=\frac{1}{1} \iff a1 = s1 \iff a = s.$$

(3)

$$(at)s = a(st) \iff (at, st) \sim (a, s) \iff \frac{at}{st}=\frac{a}{s}.$$

(4) Como $s \neq 0$ es cancelable (recordemos que D es un dominio)

$$\frac{a}{s}=\frac{b}{s} \iff as = bs \iff a = b$$

(5) Usando (3):
$$\frac{a}{s}+\frac{b}{s}=\frac{as+bs}{ss}=\frac{(a+b)s}{ss}=\frac{a+b}{s}.$$

Veamos ahora que $Q(D)$ es un anillo conmutativo con uno.

- $(Q(D),+)$ es un grupo. Tiene elemento neutro por (1). En cuanto a los simétricos, dado $\frac{a}{s}$ se tiene
$$\frac{a}{s}+\frac{-a}{s}=\frac{as-as}{ss}=\frac{0}{ss}=\frac{0}{1}$$
usando (1). Es fácil ver que además el grupo es abeliano por cómo está definida la suma
$$\frac{a}{s}+\frac{b}{t}=\frac{as+bt}{st}=\frac{bt+as}{ts}=\frac{b}{t}+\frac{a}{s}.$$
- $(Q(D),\cdot)$ es un monoide. El producto tiene neutro por (2), y es asociativo ya que
$$(\frac{a}{s}\frac{b}{t})\frac{c}{v}=\frac{ab}{st}\frac{c}{v}=\frac{abc}{stv}=\frac{a}{s}\frac{bc}{tv}=\frac{a}{s}(\frac{b}{t}\frac{c}{v}).$$
Que es conmutativo es inmediato por serlo D
$$\frac{a}{s}\frac{b}{t}=\frac{ab}{st}=\frac{ba}{ts}=\frac{b}{t}\frac{a}{s}.$$
- En cuanto a la propiedad distributiva:
$$\frac{a}{s}\left(\frac{b_1}{t_1}+\frac{b_2}{t_2}\right)=\frac{a}{s}\left(\frac{b_1t_2+b_2t_1}{t_1t_2}\right)=\frac{ab_1t_2+ab_2t_1}{st_1t_2}=\frac{ab_1}{st_1}+\frac{ab_2}{st_2}=\frac{a}{s}\frac{b_1}{t_1}+\frac{a}{s}\frac{b_2}{t_2}.$$

Para ver que es cuerpo solo necesitamos ver que $\frac{a}{s}\neq\frac{0}{1}$ tiene inverso, pero es obvio que como no es el cero entonces $a\neq 0$, luego
$$\frac{s}{a}\in Q(D),\quad \frac{a}{s}\frac{s}{a}=\frac{as}{sa}=\frac{1}{1}$$
usando (2).

Example 3.7.4

Obviamente, $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$.

Example 3.7.5

Supongamos que un anillo de polinomios $A[X]$ es un dominio (lo que ocurre si y solo si A es un dominio). Su cuerpo de fracciones se suele denotar por $A(X)$ y se llama el cuerpo de fracciones racionales sobre $A[X]$. Sus elementos son fracciones del tipo P/Q con $P, Q\in A[X]$ y $Q\neq 0$, que se suman y se multiplican de forma natural.

Usando la Proposición 3.7.3, es sencillo ver que la aplicación $u: D\to Q(D)$ dada por $u(a)=a/1$ es un homomorfismo inyectivo de anillos
$$u(a+b)=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=u(a)+u(b)$$
$$u(ab)=\frac{ab}{1}=\frac{a}{1}\frac{b}{1}=u(ab)$$

$$u(1) = \frac{1}{1}$$

$$u(a) = \frac{a}{1} = \frac{0}{1} \iff a = 0, \text{ luego } \ker u = 0$$

lo que nos permite ver a D como un subanillo de $Q(D)$ si identificamos cada elemento a de D con la fracción $a/1$ de $Q(D)$. El par $(Q(D), u)$ verifica una interesante propiedad:

Proposition 3.7.6: Propiedad Universal del Cuerpo de Fracciones

Sean D un dominio, $Q(D)$ su cuerpo de fracciones y $u : D \to Q(D)$ la aplicación dada por $u(a) = a/1$. Entonces:

(1) Para toda pareja (K, f) formada por un cuerpo K y un homomorfismo inyectivo de anillos $f : D \to K$, existe un único homomorfismo de cuerpos $\bar{f} : Q(D) \to K$ tal que $\bar{f} \circ u = f$. Se dice que $\bar{f}$ completa de modo único el diagrama

$$\begin{tikzcd} D \arrow[r, "f"] \arrow[d, "u"'] & K \\ Q(D) \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

(2) Si dos homomorfismos de cuerpos $g, h : Q(D) \to K$ coinciden sobre D entonces son iguales.

(3) Supongamos que existen un cuerpo F y un homomorfismo inyectivo de anillos $v : D \to F$ tales que, para todo cuerpo K y todo homomorfismo inyectivo de anillos $f : D \to K$, existe un único homomorfismo de cuerpos $\bar{f} : F \to K$ tal que $\bar{f} \circ v = f$. Entonces existe un isomorfismo $\phi : F \to Q(D)$ tal que $\phi \circ v = u$. Es decir, $Q(D)$ está determinado salvo isomorfismos por la Propiedad Universal.

Proof

(1) Sea $f : D \to K$ como en el enunciado. Si $\bar{f} : Q(D) \to K$ es un homomorfismo de cuerpos tal que $\bar{f} \circ u = f$ entonces, para todo $a/s \in Q(D)$, se verifica

$$\bar{f}(a/s) = \bar{f}(u(a)u(s)^{-1}) = (\bar{f} \circ u)(a)(\bar{f} \circ u)(s)^{-1} = f(a)f(s)^{-1}.$$

Esto prueba que el único homomorfismo de cuerpos $\bar{f} : Q(D) \to K$ que puede satisfacer $\bar{f} \circ u = f$ tiene que venir dado por

$$\bar{f}(a/s) = f(a)f(s)^{-1}.$$

Solo falta comprobar que la aplicación $\bar{f}$ así dada está bien definida y es un homomorfismo. Si $a_1/s_1 = a_2/s_2$ entonces $a_1s_2 = a_2s_1$, luego $f(a_1)f(s_2) = f(a_2)f(s_1)$ y, por tanto, $f(a_1)f(s_1)^{-1} = f(a_2)f(s_2)^{-1}$. Esto prueba que $\bar{f}$ está bien definido. La verificación de que es homomorfismo es directa.

(2) Si ponemos $f = g \circ u = h \circ u : D \to K$, los homomorfismos g y h completan el diagrama del apartado (1). Por la unicidad se tiene $g = h$.

(3) Sea $v : D \to F$ como en el enunciado. Aplicando (1) encontramos un homomorfismo $\bar{v} : Q(D) \to F$ tal que $\bar{v} \circ u = v$, y aplicando la hipótesis de (3) encontramos un homomorfismo $\bar{u} : F \to Q(D)$ tal que $\bar{u} \circ v = u$. Entonces la composición $\bar{u} \circ \bar{v} : Q(D) \to Q(D)$ verifica $(\bar{u} \circ \bar{v}) \circ u = \bar{u} \circ v = u$, y por (2) se obtiene $\bar{u} \circ \bar{v} = 1_{Q(D)}$. En particular $\bar{u}$ es supravectiva, y como es inyectiva por ser un homomorfismo de cuerpos, $\phi = \bar{u}$ es el isomorfismo que buscamos.

La Propiedad Universal permite afirmar que $Q(D)$ es «el menor cuerpo que contiene a D» en un sentido que se hace explícito en el siguiente resultado:

Proposition 3.7.7

Sea D un dominio. Si K es un cuerpo y $f : D \to K$ es un homomorfismo inyectivo de anillos, entonces K contiene un subcuerpo isomorfo a $Q(D)$.

Proof

Por la Propiedad Universal del Cuerpo de Fracciones existe un homomorfismo de cuerpos $\bar{f} : Q(D) \to K$, y como $\bar{f}$ es inyectiva, $\operatorname{Im} \bar{f}$ es un subcuerpo de K isomorfo a $Q(D)$.

Example 3.7.8: El cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$

Sea m un número entero que no es un cuadrado, y sea $f : \mathbb{Z}[\sqrt{m}] \to \mathbb{C}$ la inclusión. Si $\bar{f}$ es como en la demostración de la Proposición 3.7.7, entonces $\operatorname{Im} \bar{f}$ es isomorfo al cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$.
Un elemento genérico de $\operatorname{Im} \bar{f}$ es de la forma

$$x = \frac{a + b\sqrt{m}}{c + d\sqrt{m}},$$

con $a, b, c, d \in \mathbb{Z}$ y $c + d\sqrt{m} \neq 0$.
Notemos que $c - d\sqrt{m} \neq 0$ *(pregunta para el lector: ¿por qué?)*, luego

$$x = \frac{a + b\sqrt{m}}{c + d\sqrt{m}} = \frac{a + b\sqrt{m}}{c + d\sqrt{m}} \cdot \frac{c - d\sqrt{m}}{c - d\sqrt{m}} = \frac{(ac - bdm) + (bc - ad)\sqrt{m}}{c^2 - d^2 m} = \frac{r}{t} + \frac{s}{t}\sqrt{m}$$

donde $r, s, t \in \mathbb{Z}$, y por tanto $x \in \mathbb{Q}[\sqrt{m}]$. Esto demuestra que $\operatorname{Im} \bar{f} \subseteq \mathbb{Q}[\sqrt{m}]$, y el otro contenido es claro, pues un elemento genérico $\frac{a}{s} + \frac{b}{t}\sqrt{m}$ de $\mathbb{Q}[\sqrt{m}]$ se reescribe como $\frac{at+bs\sqrt{m}}{st}$.
En conclusión, el cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$ es isomorfo a $\mathbb{Q}[\sqrt{m}]$. De hecho abusaremos de la notación y diremos que el cuerpo de fracción de $\mathbb{Z}[\sqrt{m}]$ es $\mathbb{Q}[\sqrt{m}]$.

Un interesante corolario de la Proposición 3.7.7 es el siguiente:

Corollary 3.7.9

Todo cuerpo K posee un subcuerpo K', llamado el subcuerpo primo de K, que está contenido en cualquier otro subcuerpo de K (es decir, K' es «el menor subcuerpo de K»). Si la característica de K es un entero primo p, entonces K' es isomorfo a $\mathbb{Z}_p$; en caso contrario K' es isomorfo a $\mathbb{Q}$.

Proof

Si la característica es un primo p entonces el subanillo primo $\mathbb{Z}1$ de K (isomorfo a $\mathbb{Z}_p$) es ya un cuerpo, y contiene a cualquier subcuerpo (de hecho, a cualquier subanillo) de K.
En otro caso, al ser K un cuerpo, la característica es cero; es decir, el homomorfismo de anillos $f : \mathbb{Z} \to K$ es inyectivo. El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$, y el homomorfismo de cuerpos $\bar{f} : \mathbb{Q} \to K$ que nos da la Propiedad Universal viene dada por $\bar{f}(n/m) = f(n)f(m)^{-1}$.
Como $\bar{f}$ es inyectivo, $K' = \operatorname{Im} \bar{f}$ es un subcuerpo de K isomorfo a $\mathbb{Q}$, y ahora basta ver que K' está contenido en cualquier subcuerpo F de K. Dado un tal F, se tiene $f(m) \in F$ para

cada $m \in \mathbb{Z}$, y si $m \neq 0$ entonces $f(m) \neq 0$ y $f(m)^{-1} \in F$. Por tanto, para cada $n/m \in \mathbb{Q}$ se tiene $\bar{f}(n/m) = f(n)f(m)^{-1} \in F$, lo que demuestra que $K' \subseteq F$.

Remark. *La construcción del cuerpo de fracciones es análoga a la construcción de los números racionales a partir de los enteros. De hecho,* $\mathbb{Q}$ *es el caso particular cuando* $D = \mathbb{Z}$.

Remark. *Si* D *es ya un cuerpo, entonces* $Q(D)$ *es isomorfo a* D*, pues la aplicación* $a \mapsto a/1$ *es un isomorfismo.*

Chapter 4

Polinomios

4.1 Anillos de polinomios

En el resto del capítulo usaremos la siguiente notacion: $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Sea A un anillo. En el capítulo 1 definimos el anillo de polinomios $A[X]$ en una indeterminada con coeficientes en A como el conjunto de las expresiones del tipo

$$P = P(X) = p_0 + p_1 X + p_2 X^2 + \cdots + p_n X^n$$

donde n es un numero entero no negativo y $p_i \in A$ para todo i.

Los elementos $p_0, p_1, p_2, \ldots$ se llaman coeficientes de P. Más precisamente, $p_i X^i$ se llama monomio de grado i del polinomio P y p_i se llama coeficiente del monomio de grado i de P. Observese que P tiene infinitos coeficientes, aunque todos menos un numero finito son iguales a 0. Dos polinomios son iguales si sus coeficientes de los monomios del mismo grado son iguales. El polinomio cero o polinomio nulo es el polinomio que tiene todos los coeficientes iguales a 0.

La suma y el producto en $A[X]$ se definen

$$(a_0 + a_1 X + a_2 X^2 + \cdots) + (b_0 + b_1 X + b_2 X^2 + \cdots) = c_0 + c_1 X + c_2 X^2 + \cdots,$$

donde cada $c_n = a_n + b_n$, y

$$(a_0 + a_1 X + a_2 X^2 + \cdots) \cdot (b_0 + b_1 X + b_2 X^2 + \cdots) = d_0 + d_1 X + d_2 X^2 + \cdots,$$

donde cada $d_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0 = \sum_{i=0}^{n} a_i b_{n-i}$.

Sea A un anillo y sea $p = \sum_{i \in \mathbb{N}_0} p_i X^i \in A[X]$ un polinomio no nulo de $A[X]$. Entonces, por definicion de polinomio, el conjunto $\{i \in \mathbb{N}_0 : p_i \neq 0\}$ no es vacio y esta acotado superiormente. Por tanto ese conjunto tiene un maximo, al que llamamos grado del polinomio P y denotamos por $\text{gr}(p)$. Es decir,

$$\text{gr}(p) = \max\{i \in \mathbb{N}_0 : p_i \neq 0\}.$$

El coeficiente de mayor grado, $p_{\text{gr}(p)}$, se conoce como el coeficiente principal de P, y diremos que P es monico si su coeficiente principal es 1. Por convenio, consideramos que el polinomio 0 tiene grado $-\infty$ y coeficiente principal 0. Es claro que los polinomios de grado 0 son precisamente los polinomios constantes no nulos. A veces llamaremos lineales a los polinomios de grado 1, cuadraticos a los de grado 2, cubicos a los de grado 3, etcetera.

Lemma 4.1.1

Si P y Q son polinomios no nulos de $A[X]$ y sus términos principales son p y q respectivamente entonces se verifican las siguientes propiedades:

(1) $\mathrm{gr}(P+Q) \leq \max(\mathrm{gr}(P), \mathrm{gr}(Q))$, con la desigualdad estricta si y solo si $\mathrm{gr}(P) = \mathrm{gr}(Q)$ y $p+q=0$.

(2) $\mathrm{gr}(PQ) \leq \mathrm{gr}(P) + \mathrm{gr}(Q)$, con igualdad si y solo si $pq \neq 0$.

(3) Si p es regular (por ejemplo, si P es mónico, o si A es un dominio), entonces se tiene $\mathrm{gr}(PQ) = \mathrm{gr}(P) + \mathrm{gr}(Q)$.

(4) Las desigualdades de los apartados 1 y 2 pueden ser estrictas.

Proof

Supongamos que los coeficientes de P son $p_0, p_1, \ldots, p_n = p$ y los de Q son $q_0, q_1, \ldots, q_m = q$, luego $\mathrm{gr}(P) = n, \mathrm{gr}(Q) = m$. Podemos suponer además sin perder generalidad que $n \geq m$.

(1) Por la definición de grado

$$\mathrm{gr}(P+Q) = \max\{i \in \mathbb{N}_0 : p_i + g_i \neq 0\}.$$

Sabemos que si $i > n \geq m$ entonces $p_i = q_i = 0 \implies p_i + q_i = 0$, luego

$$\mathrm{gr}(P+Q) \leq n = \mathrm{gr}(P) = \max(\mathrm{gr}(P), \mathrm{gr}(Q)).$$

Además, la desigualdad es estricta si y solo si

$$p_n + q_n = 0 \iff p_n = -q_n$$

y como $p_n = p \neq 0$ debe ser $m = n$ y $q = -p$.

(2) Por definición

$$\mathrm{gr}(PQ) = \max\{i \in \mathbb{N}_0 : \sum_{k=0}^{i} p_k q_{i-k} \neq 0\}.$$

Sea $i > n+m$ entonces dado $0 \leq k \leq i$ tenemos $k > n \implies p_k = 0$ por lo que

$$\sum_{k=0}^{i} p_k q_{i-k} = \sum_{k=0}^{n} p_k q_{i-k}$$

pero $i - k > m \implies q_{i-k} = 0$ y esta condición es equivalente a

$$i - k \leq m \iff k \geq i - m > n$$

es decir, si $k > n$ los $q_{i-k} = 0$, por tanto nos queda

$$\sum_{k=0}^{n} p_k q_{i-k} = 0$$

esto prueba que

$$\mathrm{gr}(PQ) \leq n + m = \mathrm{gr}(P) + \mathrm{gr}(Q).$$

La igualdad se da si y solo si

$$0 \neq \sum_{k=0}^{n+m} p_k q_{(n+m)-k} = \sum_{k=n}^{n} p_k q_{(n+m)-k} = p_n q_m$$

es decir, si y solo si $pq \neq 0$.

(3) Supongamos que p es regular y que $pq = 0$, entonces, como p es regular $q = 0$, pero esto es imposible pues q es el término principal de Q. Por tanto

$$pq \neq 0 \implies \mathrm{gr}(PQ) = \mathrm{gr}(P) + \mathrm{gr}(Q)$$

por (2).

(4) Para el apartado (1) consideremos los polinomios

$$P = X + 1, Q = -X, \quad P, Q \in \mathbb{Z}[X],$$

claramente $\mathrm{gr}(P) = \mathrm{gr}(Q) = 1$ pero $P + Q = 1$, luego

$$\mathrm{gr}(P + Q) = 0 < \max(\mathrm{gr}(P), \mathrm{gr}(Q)) = 1.$$

En cuanto al apartado (2), sean

$$P = 2, Q = 2X + 1, \quad P, Q \in \mathbb{Z}_4[X],$$

entonces $\mathrm{gr}(P) = 0, \mathrm{gr}(Q) = 1$, pero $PQ = 4X + 2 = 2$, luego

$$\mathrm{gr}(PQ) = 0 < \mathrm{gr}(P) + \mathrm{gr}(Q) = 1.$$

Una consecuencia inmediata del Lema 4.1.1 es:

Corollary 4.1.2

Un anillo de polinomios $A[X]$ es un dominio si y solo si lo es el anillo de coeficientes A. En este caso se tiene $A[X]^* = A^*$, es decir, los polinomios invertibles de $A[X]$ son los polinomios constantes invertibles en A. En particular, los polinomios invertibles sobre un cuerpo son exactamente los de grado 0, y $A[X]$ nunca es un cuerpo.

Proof

Supongamos que $A[X]$ es un dominio, entonces

$$PQ = 0 \implies P = 0 \text{ o } Q = 0.$$

Sean $p, q \in A$ y supongamos que $pq = 0$, sean $P = p, Q = q$ polinomios en $A[X]$ con grado 0, que claramente cumplen $PQ = pq = 0$. Como $A[X]$ es un dominio debe ser entonces $P = 0$ o $Q = 0$, es decir, $p = 0$ o $q = 0$, luego A también es un dominio.
Para el recíproco, supongamos que A es un dominio. Sean $P, Q \in A[X]$ tales que $PQ = 0$, luego $\mathrm{gr}(PQ) = -\infty$. Por la parte (3) del Lema 4.1.1 sabemos que

$$-\infty = \mathrm{gr}(PQ) = \mathrm{gr}(P) + \mathrm{gr}(Q)$$

luego o bien $\mathrm{gr}(P) = -\infty$ o $\mathrm{gr}(Q) = -\infty$, es decir, $P = 0$ o $Q = 0$. Esto prueba que $A[X]$ es un dominio.
En cuanto a las unidades, es claro que $A^* \subseteq A[X]^*$ (abusamos del lenguaje identificando A como subanillo de $A[X]$). Sea ahora $P \in A[X]^*$, entonces existe Q tal que

$$PQ = 1 \implies 0 = \mathrm{gr}(PQ) = \mathrm{gr}(P) + \mathrm{gr}(Q) \implies \mathrm{gr}(P) = \mathrm{gr}(Q) = 0$$

es decir, $P, Q \in A \setminus \{0\}$, pero entonces P es una unidad en A, luego $P \in A^*$ como queríamos ver.

Hemos observado que un anillo A es un subanillo del anillo de polinomios $A[X]$, y por tanto la inclusión $u : A \to A[X]$ es un homomorfismo de anillos. También es claro que el subanillo de $A[X]$ generado por A y X es todo $A[X]$. Es decir, la indeterminada X y las constantes de A (las imágenes de u) generan todos los elementos de $A[X]$.

Proof

Ya sabemos que $(A \cup \{X\}) \subseteq A[X]$. Sea $P \in A[X]$, entonces

$$P = p_0 + p_1 X + \cdots + p_n X^n, \quad p_n \neq 0$$

agrupando términos

$$P = p_0 + X(p_1 + \cdots + p_n X^{n-1}) \in (A \cup \{X\})$$

luego $A[X] \subseteq (A \cup \{X\})$ como queríamos ver.

El siguiente resultado nos dice que $A[X]$ puede caracterizarse por una propiedad en la que solo intervienen X y u.

Proposition 4.1.3: Propiedad Universal del Anillo de Polinomios, PUAP

Sean A un anillo, $A[X]$ el anillo de polinomios con coeficientes en A en la indeterminada X y $u : A \to A[X]$ el homomorfismo de inclusión.

(1) Para todo homomorfismo de anillos $f : A \to B$ y todo elemento b de B existe un único homomorfismo de anillos $\overline{f} : A[X] \to B$ tal que $\overline{f}(X) = b$ y $\overline{f} \circ u = f$. Para expresar la última igualdad dice que $\overline{f}$ completa de modo único el diagrama

$$\begin{tikzcd} A \arrow[r, "u"] \arrow[dr, "f"'] & A[X] \arrow[d, "\overline{f}"] \\ & B \end{tikzcd}$$

(2) Si dos homomorfismos de anillos $g, h : A[X] \to B$ coinciden sobre A y en X entonces son iguales. Es decir, si $g \circ u = h \circ u$ y $g(X) = h(X)$ entonces $g = h$.

(3) $A[X]$ y u están determinados salvo isomorfismos por la PUAP. Explicitamente: supongamos que existen un homomorfismo de anillos $v : A \to P$ y un elemento $T \in P$ tales que, para todo homomorfismo de anillos $f : A \to B$ y todo elemento $b \in B$, existe un único homomorfismo de anillos $\overline{f} : P \to B$ tal que $\overline{f} \circ v = f$ y $\overline{f}(T) = b$. Entonces existe un isomorfismo $\phi : A[X] \to P$ tal que $\phi \circ u = v$ y $\phi(X) = T$.

Proof

(1) Sean $f : A \to B$ y $b \in B$ como en el enunciado. Si existe un homomorfismo $\overline{f} : A[X] \to B$ tal que $\overline{f} \circ u = f$ y $\overline{f}(X) = b$, entonces para un polinomio $P = \sum_{n=0}^{m} p_n X^n$, se tendra

$$\overline{f}(P) = \overline{f}\left(\sum_{n=0}^{m} u(p_n) X^n\right) = \sum_{n=0}^{m} f(p_n) b^n.$$

Por tanto, la aplicacion dada por $\overline{f}(P) = \sum_{n=0}^{m} f(p_n) b^n$ es la unica que puede cumplir tales condiciones.

Veamos que es un homomorfismo de anillos, dados $P, Q \in A[X]$

$$\overline{f}(P+Q) = \sum_{n\geq 0} f(c_n)b^n = \sum_{n\geq 0} f(p_n+q_n)b^n = \sum_{n\geq 0} f(p_n)b^n + \sum_{n\geq 0} f(q_n)b^n = \overline{f}(P)+\overline{f}(Q)$$

$$\overline{f}(PQ) = \sum_{n\geq 0} f(d_n)b^n = \sum_{n\geq 0} f(\sum_{i=0}^{n} p_i q_{n-i})b^n = \sum_{n\geq 0} \left(\sum_{i=0}^{n} f(p_i)f(q_{n-i})\right) b^n = \overline{f}(P)\overline{f}(Q)$$

$$\overline{f}(1) = f(1)b^0 = f(1) = 1.$$

Además, es elemental ver que satisface $\overline{f}(X) = b$ y $\overline{f} \circ u = f$.

(2) Si ponemos $f = g \circ u = h \circ u : A \to B$, los homomorfismos g y h completan el diagrama del apartado (1). Por la unicidad se tiene $g = h$.

(3) Sean $v : A \to P$ y $T \in P$ como en (3). Aplicando (1) y la hipotesis de (3) deducimos que existen homomorfismos $\overline{v} : A[X] \to P$ y $\overline{u} : P \to A[X]$ tales que que se verifican las siguientes igualdades:

$$\overline{v} \circ u = v, \quad \overline{v}(X) = T, \qquad \overline{u} \circ v = u, \quad \overline{u}(T) = X.$$

Entonces la composicion $\overline{u} \circ \overline{v} : A[X] \to A[X]$ verifica

$$(\overline{u} \circ \overline{v}) \circ u = \overline{u} \circ v = u \qquad \text{y} \qquad (\overline{u} \circ \overline{v})(X) = \overline{u}(T) = X,$$

y por (2) se obtiene $\overline{u} \circ \overline{v} = 1_{A[X]}$. De modo analogo, y observando que v y T verifican una condicion similar a (2), se demuestra que $\overline{v} \circ \overline{u} = 1_P$, con lo que $\overline{v}$ es el isomorfismo que buscamos.

La utilidad de la PUAP estriba en que, dado un homomorfismo $f : A \to B$, nos permite crear un homomorfismo $A[X] \to B$ que "respeta" a f y que "se comporta bien" sobre un elemento $b \in B$ que nos interese. Los siguientes ejemplos son aplicaciones de la PUAP a ciertos homomorfismos que aparecen con frecuencia y son importantes tanto en este capitulo como en algunos de los siguientes (y en otras muchas situaciones que no estudiaremos aqui).

Example 4.1.4: Aplicaciones de la PUAP (1)

Sean A un subanillo de B y $b \in B$. Aplicando la PUAP a la inclusion $A \hookrightarrow B$ obtenemos un homomorfismo $S_b : A[X] \to B$ que es la identidad sobre A (decimos a veces que fija los elementos de A) y tal que $S_b(X) = b$.
Se le llama el homomorfismo de sustitución (o de evaluación) en b. Dado $P \in A[X]$, escribiremos a menudo $P(b)$ en vez de $S_b(X)$. Podemos describir explicitamente la accion de S_b en un polinomio:

$$P(X) = \sum_{n\geq 0}^{A[X]} p_n X^n \rightsquigarrow S_b(P) = P(b) = \sum_{n\geq 0} p_n b^n.$$

Example 4.1.5: Aplicaciones de la PUAP (2)

Sean A un anillo y $a \in A$. Si en el ejemplo anterior tomamos $B = A[X]$ y $b = X + a$, obtenemos un homomorfismo $\phi : A[X] \to A[X]$ dado por

$$p(X) \mapsto p(X + a).$$

Este homomorfismo es un automorfismo cuyo inverso ψ viene dado por $p(X) \mapsto p(X - a)$. En efecto

$$\phi(\psi(p(X))) = \phi(p(X - a)) = p((X + a) - a) = p(x)$$

$$\psi(\phi(p(X))) = \psi(p(X + a)) = p((X - a) + a) = p(x).$$

Example 4.1.6: Aplicaciones de la PUAP (3)

Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo entre los correspondientes anillos de polinomios.
Aplicándole la PUAP a la composición de f con la inclusión $B \hookrightarrow B[X]$ obtenemos $\bar{f} : A[X] \to B[X]$ tal que $\bar{f}|_A = f$ y $\bar{f}(X) = X$. Explicitamente,

$$\bar{f}\left(\sum_{n\geq 0} p_n X^n\right) = \sum_{n\geq 0} f(p_n) X^n.$$

Es fácil ver que si f es inyectivo o suprayectivo, entonces lo es $\bar{f}$; como casos particulares de esta afirmación se obtienen los dos ejemplos siguientes.

Example 4.1.7: Aplicaciones de la PUAP (4)

Si A es un subanillo de B entonces $A[X]$ es un subanillo de $B[X]$.

Example 4.1.8: Aplicaciones de la PUAP (5)

Si I es un ideal del anillo A, la proyección $\pi : A \to A/I$ induce un homomorfismo suprayectivo $\bar{\pi} : A[X] \to (A/I)[X]$. Si ponemos $\bar{a} = a + I$, el homomorfismo $\bar{\pi}$ viene dado explícitamente por

$$\bar{\pi}\left(\sum_{n\geq 0} p_n X^n\right) = \sum_{n\geq 0} \overline{p_n} X^n.$$

A $\bar{\pi}$ se le llama el homomorfismo de reducción de coeficientes módulo I. Su núcleo, que es un ideal de $A[X]$, consiste en los polinomios con coeficientes en I, y lo denotaremos por $I[X]$. Del Primer Teorema de Isomorfía se tiene que $(A/I)[X] \simeq \frac{A[X]}{I[X]}$.

Example 4.1.9: Aplicaciones de la PUAP (6)

Sea A un subanillo de B y sea $S_b : A[X] \to B$ el homomorfismo de sustitución en cierto elemento b de B. Entonces Im S_b es el subanillo de B generado por $A \cup \{b\}$, y consiste en las "expresiones polinómicas en b con coeficientes en A"; es decir, en los elementos de la forma

$$\sum_{i=0}^{n} a_i b^i,$$

donde $n \geq 0$ y $a_i \in A$ para cada i. Este subanillo se suele denotar por $A[b]$ y es el menor subanillo de B que contiene a $A \cup \{b\}$.
Por ejemplo, si $A = \mathbb{Z}$, $B = \mathbb{C}$ y $b = \sqrt{m}$ para cierto $m \in \mathbb{Z}$, entonces la notación anterior es compatible con la que se usó anteriormente (es decir, $\mathbb{Z}[\sqrt{m}]$ representa el mismo subanillo atendiendo a cualquiera de las dos definiciones). Lo mismo ocurre si se toma $A = \mathbb{Q}$. Si además $m \equiv 1 \bmod 4$ entonces $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ es el anillo $A_m = \{\frac{a+b\sqrt{2}}{2} : a \equiv b \bmod 2\}$ y $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}\left[\frac{1+\sqrt{m}}{2}\right]$.

4.2 Raíces de polinomios

Empezaremos esta sección con el siguiente lema. Recuérdese que consideramos el polinomio cero como un polinomio de grado $-\infty$.

Lemma 4.2.1

Sea A un anillo y sean $f, g \in A[X]$. Si el coeficiente principal de g es invertible en A, entonces existen dos únicos polinomios $q, r \in A[X]$ tales que $f = gq + r$ y $\mathrm{gr}(r) < \mathrm{gr}(g)$. En esta situación, q y r se llaman cociente y resto de la división de f entre g.

Proof

Para la existencia usamos el argumento que vimos en el Ejemplo 3.6.3.
Sea $m = \mathrm{gr}(g)$ y sea b el coeficiente principal de g, que es invertible en A por hipótesis. Dado $f \in A[X]$ vamos a ver, por inducción en $n = \mathrm{gr}(f)$, que existen $q, r \in A[X]$ satisfaciendo las propiedades del Lema.
Si $n < m$ podemos tomar $q = 0$ y $r = f$. Supongamos pues que $n \geq m$ y que la propiedad se verifica si f se sustituye por un polinomio de grado menor. Si a es el término principal de f, es claro que el polinomio $f_1 = f - ab^{-1}X^{n-m}g \in A[X]$ tiene grado menor que el de f. Por hipótesis de inducción existen $q_1, r \in A[X]$ tales que $f_1 = gq_1 + r$ y $r = 0$ o $\mathrm{gr}(r) < m$. Entonces $f = g(q_1 + ab^{-1}X^{n-m}) + r$, lo que termina la demostración de la existencia de cociente y resto.
En cuanto a la unicidad, supongamos que $f = gq_1 + r_1 = gq_2 + r_2$ con $\mathrm{gr}(r_i) < \mathrm{gr}(g)$ para cada $i = 1, 2$. Como el término principal de g es regular, del Lema 4.1.1 se deduce que

$$\mathrm{gr}(g) + \mathrm{gr}(q_1 - q_2) = \mathrm{gr}(g(q_1 - q_2)) = \mathrm{gr}(r_2 - r_1) \leq \max\{\mathrm{gr}(r_2), \mathrm{gr}(r_1)\} < \mathrm{gr}(g).$$

Luego $\mathrm{gr}(q_1 - q_2) < 0$ y en consecuencia $q_1 = q_2$, de donde $r_1 = r_2$.

Proposition 4.2.2

Sean A un anillo, $a \in A$ y $f \in A[X]$. Entonces:

(1) (Teorema del Resto) El resto de la división de f entre $X - a$ es $f(a)$.

(2) (Teorema de Ruffini) $X - a$ divide a f si y solo si $f(a) = 0$. En tal caso se dice que a es una raíz de f.

Proof

Dividiendo f entre $X - a$ (podemos hacerlo puesto que el coeficiente principal de $X - a$ es 1) tenemos $f = q(X - a) + r$ con $\mathrm{gr}(r) < 1$, por lo que r es constante y así $r = r(a) = f(a) - q(a)(a - a) = f(a)$. Esto demuestra (1), y (2) es entonces inmediato.

Fijemos $a \in A$. Como, para cada $k \in \mathbb{N}_0$, el polinomio $(X - a)^k$ es monico de grado k, se tiene $\mathrm{gr}((X - a)^k q) = k + \mathrm{gr}(q)$ para cada $q \in A[X]$. Por tanto, para cada $f \in A[X]$ no nulo, existe un mayor $m \in \mathbb{N}_0$ tal que $(X - a)^m$ divide a f. Este entero m, que verifica $0 \leq m \leq \mathrm{gr}(f)$, se llama la multiplicidad de a en f. Por el Teorema de Ruffini, a es raíz de f precisamente si $m \geq 1$. Cuando $m = 1$ se dice que a es una raíz simple de f, y cuando $m > 1$ se dice que a es una raíz múltiple de f.

Lemma 4.2.3

Sean $a \in A$ y $f \in A[X]$. La multiplicidad de a en f es el único entero no negativo m tal que $f = (X-a)^m g$ para algún polinomio $g \in A[X]$ del que a no es raíz.

Proof

Sea n la multiplicidad de a en f. Entonces

$$f = (X-a)^n h$$

para un polinomio h, pero $(X-a)^{n+1}$ no divide a f. Si a es raíz de h, entonces $X-a$ divide a h y por tanto $(X-a)^{n+1}$ divide a f, que acabamos de decir que no pasa. Luego a no es raíz de h.
Recíprocamente, supongamos que

$$f = (X-a)^m g$$

con $g \in A[X]$ y $g(a) \neq 0$. Notemos que por tener multiplicidad n también tenemos $f = (X-a)^n h$. Por la definición de multiplicidad, $m \leq n$. Como $X-a$ es monico, también es cancelable en $A[X]$, y por tanto de

$$(X-a)^m g = (X-a)^n h$$

deducimos que $(X-a)^{n-m} h = g$. Si $n > m$ entonces $g(a) = 0$, en contra de la suposición. Luego $m = n$.

Cuando D es un dominio, del Teorema de Ruffini se deduce que $X-a$ es primo para cualquier $a \in D$. En efecto

$$(X-a) \mid fg \implies f(a)g(a) = 0 \implies f(a) = 0 \text{ ó } g(a) = 0 \implies (X-a) \mid f \text{ ó } (X-a) \mid g.$$

Esto es esencial en la demostración del siguiente resultado.

Proposition 4.2.4: Acotación de raíces

Sean D un dominio y $0 \neq f \in D[X]$. Entonces:

(1) Si $a_1, \ldots, a_n \in D$ son distintos dos a dos y $\alpha_1, \ldots, \alpha_n \geq 1$ son enteros con cada $(X-a_i)^{\alpha_i}$ dividiendo a f, entonces $(X-a_1)^{\alpha_1} \cdots (X-a_n)^{\alpha_n}$ divide a f. Por tanto $\sum_{i=1}^n \alpha_i \leq \mathrm{gr}(f)$.

(2) La suma de las multiplicidades de todas las raíces de f es menor o igual que $\mathrm{gr}(f)$. En particular, el número de raíces distintas de f es menor o igual que $\mathrm{gr}(f)$.

Proof

Es claro que basta con demostrar la primera afirmación de (1), cosa que hacemos por inducción en $s = \sum_{i=1}^n \alpha_i$. El caso $s = 1$ es inmediato, ya que por hipótesis $(X-a_1)_1^{\alpha}$ divide a f.
Cuando $s > 1$, por hipótesis $(X-a_1)^{\alpha_1}$ divide a f, y por hipótesis de inducción

$$(X-a_1)^{\alpha_1 - 1}(X-a_2)^{\alpha_2} \cdots (X-a_n)^{\alpha_n} \mid f$$

también. Por tanto, sabemos que existen polinomios g y h tales que

$$g(X-a_1)^{\alpha_1} = f = h(X-a_1)^{\alpha_1-1}(X-a_2)^{\alpha_2} \cdots (X-a_n)^{\alpha_n}.$$

Cancelando $(X - a_1)^{\alpha_1 - 1}$ y usando el hecho de que $X - a_1$ es primo y no divide a ningún otro $X - a_i$ (pues $a_1 \neq a_i$ para $i \geq 2$), deducimos que $X - a_1$ divide a h, y esto nos da el resultado.

Si D no es un dominio, siempre podemos encontrar un polinomio en $D[X]$ para el que falle la acotación de raíces (es decir, "con más raíces que grado"). En efecto, si $0 \neq a, b \in D$ y $ab = 0$, entonces aX es un polinomio de grado 1 con al menos 2 raíces, 0 y b. Otro ejemplo se obtiene considerando el polinomio $X^2 - 1$, que tiene 4 raíces en $\mathbb{Z}_8$.

El siguiente corolario evidente de la Proposición 4.2.4 se conoce como el principio de las identidades polinómicas. Ya hemos comentado que su segundo apartado falla sobre cualquier anillo finito.

Corollary 4.2.5: Principio de las identidades polinómicas

Sea D un dominio, y sean $f, g \in D[X]$. Entonces:

(1) Si las funciones polinomicas $f, g : D \to D$ coinciden en m elementos de D y se tiene que $m > gr(f)$ y $m > gr(g)$, entonces $f = g$ (como polinomios).

(2) Si D es infinito entonces dos polinomios distintos definen funciones polinomicas distintas en D.

Proof

(1) Si $f \neq g$, entonces $f - g \neq 0$ y tiene grado a lo sumo $\max\{gr(f), gr(g)\}$. Pero $f - g$ tiene al menos m raíces, lo que contradice la Proposición 4.2.4.

(2) Si f y g definen la misma función polinómica, entonces $f - g$ se anula en todo D, que es infinito, luego por (1) se tiene $f = g$.

La necesidad de la hipotesis de infinitud del dominio D en el Corolario anterior resulta obvia si observamos que si K es un cuerpo (recuerdese que todo dominio finito es un cuerpo) entonces hay infinitos polinomios con coeficientes en K pero solo un numero finito de aplicaciones de K en K.

Para un ejemplo explícito recordemos el Pequeño Teorema de Fermat que afirma que si p es primo, entonces $a^p \equiv a \bmod p$. Eso implica que todos los elementos del cuerpo $\mathbb{Z}/p\mathbb{Z}$ son raíces del polinomio no nulo $X^p - X$.

El siguiente concepto es útil para calcular multiplicidades.

Definition 4.2.6: Derivada de un polinomio

Sea A un anillo. La derivada de $P = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ se define como

$$D(P) = P' = a_1 + 2a_2 X + 3a_3 X^2 + \cdots + n a_n X^{n-1}.$$

Observese que la derivada no se ha definido a partir de ningún concepto métrico. Por ejemplo, no es cierto en general que un polinomio con derivada nula sea constante (considérese por ejemplo $X^n \in \mathbb{Z}_n[X]$). Sin embargo, esta derivada formal satisface las mismas propiedades algebraicas que la derivada del Análisis.

Lemma 4.2.7

Dados $a, b \in A$ y $P, Q \in A[X]$:

(1) $(aP + bQ)' = aP' + bQ'$.

(2) $(PQ)' = P'Q + PQ'$.

(3) $(P^n)' = nP^{n-1}P'$.

Proof

Sean
$$P = p_0 + p_1X + \cdots + p_nX^n, Q = q_0 + q_1X + \cdots + q_mX^m$$
y supongamos sin perder generalidad que $n \geq m$.

(1) Es inmediato que
$$aP + bQ = c_0 + c_1X + \cdots + c_nX^n$$
donde $c_k = ap_k + bq_k$. Entonces
$$(aP + bQ)' = c_1 + 2c_2X + \cdots + nc_nX^{n-1}$$
mientras que
$$P' = p_1 + \cdots + np_nX^{n-1}, \quad Q' = q_1 + \cdots + mq_mX^{m-1}$$
de donde es claro que $aP' + bQ'$ tiene coeficientes
$$ap_1 + bq_1, 2(ap_2 + bq_2), \ldots, n(ap_n + bq_n)$$
es decir, los mismos que $(aP + bQ)'$, como queríamos ver.

Las otras dos me dan pereza, quedan como ejercicio para el lector.

Proposition 4.2.8

Un elemento $a \in A$ es una raiz multiple de $P \in A[X]$ si y solo si $P(a) = P'(a) = 0$.

Proof

Ya sabemos que a es una raiz de P si y solo si $P(a) = 0$. Si a es raiz simple se tiene $P = (X - a)Q$ para cierto $Q \in A[X]$ con $Q(a) \neq 0$, por lo que, del Lema 4.2.7 tenemos que
$$P' = Q + (X - a)Q'$$
y asi $P'(a) = Q(a) \neq 0$.
Si a es raiz multiple se tiene $P = (X - a)^2Q$ para cierto $Q \in A[X]$, por lo que $P' = 2(X - a)Q + (X - a)^2Q'$ y asi $P'(a) = 0$.

En dominios de caracteristica cero, la idea de la demostracion anterior puede usarse para determinar la multiplicidad de a en P (no solo para decidir si a es simple o multiple). Para ello, necesitamos considerar las derivadas sucesivas de un polinomio: Para cada $n \geq 0$ se define la derivada n-esima $P^{(n)}$ de $P \in A[X]$, de forma recurrente, por las formulas:
$$P^{(0)} = P, \quad P^{(n+1)} = \left(P^{(n)}\right)'$$

Proposition 4.2.9

Sea D un dominio de característica 0, y sean $P \in D[X]$ y $a \in D$. Entonces la multiplicidad de a en P es el menor $m \in \mathbb{N}_0$ tal que $P^{(m)}(a) \neq 0$.

Proof

Haremos inducción en la multiplicidad m de a en P. Si $m = 0$ el resultado es inmediato puesto que a no es raíz de P, luego $P^{(0)}(a) = P(a) \neq 0$.
Supongamos ahora que se cumple para $m - 1$. Sea a raíz de P con multiplicidad m, entonces $P = (X - a)Q$ para cierto $Q \in D[X]$.Claramente, la multiplicidad de a en Q es $m - 1$, y por hipótesis de inducción para todo $i < m - 1$ se tiene $Q^{(i)}(a) = 0$ mientras que $Q^{(m-1)}(a) \neq 0$.
Además, usando el Lema 4.2.7 es fácil demostrar por inducción que para cada $t \geq 1$ se tiene

$$P^{(t)} = tQ^{(t-1)} + (X - a)Q^{(t)}.$$

Entonces es inmediato que para todo $i < m$

$$P^{(i)}(a) = iQ^{(i-1)}(a) + (a - a)Q^{(i)} = 0,$$

mientras que

$$P^{(m)}(a) = mQ^{(m-1)}(a) + (a - a)Q^{(i)} = mQ^{(m-1)}(a) \neq 0.$$

La hipótesis sobre la característica de D en la Proposición anterior es necesaria. Por ejemplo, si p es un número primo, $K = \mathbb{Z}_p$ y $P = X^p$, entonces $P' = 0$ y así $P^{(n)} = 0$ para todo n. No todos los polinomios con coeficientes en un anillo A tienen raíces en A. Por ejemplo, los polinomios de grado 0 no tienen ninguna raíz, y un polinomio lineal $aX + b$ (con $a \neq 0$) tiene una raíz en A si y solo si a divide a b. En particular, todo polinomio lineal sobre un cuerpo tiene una raíz, pero puede haber polinomios de grado positivo sin raíces: por ejemplo, $X^2 + 1$ no tiene raíces en $\mathbb{R}$, y para todo entero primo p y todo $n \geq 2$ el polinomio $X^n - p$ no tiene raíces en $\mathbb{Q}$.

4.3 Divisibilidad en anillos de polinomios

La siguiente proposición caracteriza cuándo un anillo de polinomios es un DIP o dominio euclídeo y cuáles son los irreducibles en tal caso.

Proposition 4.3.1

Para un anillo A, las condiciones siguientes son equivalentes:

(1) $A[X]$ es un dominio euclídeo.

(2) $A[X]$ es un dominio de ideales principales.

(3) A es un cuerpo.

En este caso, un polinomio $f \in A[X]$ es irreducible si y solo si es primo si y solo si $\operatorname{gr}(f) > 0$ y f no es producto de dos polinomios de grado menor; es decir, si una igualdad $f = gh$ en $A[X]$ implica que $\operatorname{gr}(g) = \operatorname{gr}(f)$ (y $\operatorname{gr}(h) = 0$) ó $\operatorname{gr}(h) = \operatorname{gr}(f)$ (y $\operatorname{gr}(g) = 0$).

Proof

- Ya sabemos que (1) implica (2) por el Teorema 3.6.6 y que (3) implica (1) por el Ejemplo 3.6.3.
- Para ver (2) implica (3) notemos que claramente el polinomio X es irreducible, con lo que si $A[X]$ es DIP entonces el ideal (X) es maximal. Si $a \in A \setminus \{0\}$ entonces $a \notin (X)$ con lo que de la maximalidad de (X) deducimos que $(a, X) = A[X]$ y por tanto $1 = aP + XQ$ para ciertos $P, Q \in A[X]$. Luego $1 = aP(0)$, con lo que a es invertible en A. Esto demuestra que A es un cuerpo.

En caso de que se verifiquen las equivalencias, por 3.5.2 $f \in A[X]$ es irreducible si y solo si es primo.
Para la otra caracterización recordemos que por el Corolario 4.1.2 $A[X]^* = A^*$, es decir, las únicas unidades son los polinomios de grado 0 (todos ellos ya que A es cuerpo).

- Supongamos que f es irreducible, entonces no puede ser 0 ni una unidad, luego $\operatorname{gr}(f) > 0$, pues si fuera $\operatorname{gr}(f) = 0$ entonces f sería una unidad. Además, si $f = gh$ entonces $g \in A[X]^*$ o $h \in A[X]^*$, es decir, g o h tienen grado 0, luego los grados verifican lo esperado.
- Supongamos por el contrario que f cumple las condiciones descritas. Como $\operatorname{gr}(f) > 0$ sabemos que $0 \neq f \in A \setminus A^*$. Además, si $f = gh$ entonces g o h tienen grado 0, es decir, uno de los dos es una unidad.

Obsérvese que si $a \in A$ y $f \in A[X]$ entonces

$$a \mid f \iff f = ag \iff f_0 + f_1 X + \cdots + f_n X^n = ag_0 + ag_1 X + \cdots + ag_n X^n \iff f_k = ag_k \iff a \mid f_k$$

es decir, $a \mid f$ si y solo si a divide a todos los coeficientes de f.

Lemma 4.3.2

Sea D un dominio y sea $p \in D$.

(1) p es irreducible en D si y solo si lo es en $D[X]$.

(2) Si p es primo en $D[X]$ entonces lo es en D.

(3) Si ademas D es un DFU entonces las condiciones siguientes son equivalentes:

  (a) p es irreducible en D.
  (b) p es irreducible en $D[X]$.
  (c) p es primo en D.
  (d) p es primo en $D[X]$.

Proof

(1) Es consecuencia del Corolario 4.1.2.

(2) Supongamos que $p \mid ab$ en D, entonces $p \mid ab$ en $D[X]$. Como p es primo en $D[X]$ podemos suponer sin perder generalidad que $p \mid a$, en tal caso

$$a = pf, \quad f \in D[X]$$

pero entonces comparando grados $0 = \mathrm{gr}(a) = \mathrm{gr}(p) + \mathrm{gr}(f) = \mathrm{gr}(f)$, luego $f \in D$ y por tanto $p \mid a$ en D.

(3) Por (1) sabemos que (a) y (b) son equivalentes. Además, por la Proposición 3.3.6 ser primo implica ser irreducible, luego (c) implica (a) y (d) implica (b) por otro lado, por el Lema 3.4.6 (a) implica (c). En resumen: (a), (b), (c) son equivalentes y (d) implica (b), luego solo falta ver que (c) implica (d).

Supongamos por tanto que p es primo en D, y veamos que lo es en $D[X]$. Para ello, sean

$$a = a_0 + \cdots + a_n X^n \qquad \text{y} \qquad b = b_0 + \cdots + b_m X^m$$

polinomios de $D[X]$ tales que $p \nmid a$ y $p \nmid b$, y veamos que $p \nmid ab$. Recordemos que p divide a un polinomio si y solo si divide a todos sus factores, luego por hipótesis, existen un menor indice i tal que $p \nmid a_i$, y un menor indice j tal que $p \nmid b_j$. El coeficiente de grado $i + j$ de ab es

$$c_{i+j} = a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0,$$

y las condiciones dadas implican que p divide a todos los sumandos excepto a $a_i b_j$, por lo que $p \nmid c_{i+j}$ y en consecuencia $p \nmid ab$.

4.3.1 Polinomios sobre dominios de factorización única

En el resto de la seccion D *sera un DFU y* K *su cuerpo de fracciones.*

Consideremos la funcion

$$\varphi : D \setminus \{0\} \to \mathbb{N}_0$$

que a cada $0 \neq a \in D$ le asocia el numero $\varphi(a)$ de factores irreducibles en la expresion de a como producto de irreducibles de D, contando repeticiones. Por ejemplo, si $D = \mathbb{Z}$ entonces $\varphi(12) = 3$ y $\varphi(-80) = 5$. Es claro que, si $a, b \in D \setminus \{0\}$, entonces

$$\varphi(ab) = \varphi(a) + \varphi(b) \qquad \text{y} \qquad \varphi(a) = 0 \Leftrightarrow a \in D^*.$$

Lemma 4.3.3

Si $a \in D$ y $f, g, h \in D[X]$ verifican $af = gh \neq 0$, entonces existen $g_1, h_1 \in D[X]$ tales que

$$f = g_1 h_1, \qquad gr(g_1) = gr(g), \qquad gr(h_1) = gr(h).$$

Proof

Razonamos por induccion en $\varphi(a)$. Si $\varphi(a) = 0$ podemos tomar $g_1 = a^{-1}g$ y $h_1 = h$.
Si $\varphi(a) > 0$, existen $p, b \in D$ tales que $a = pb$ y p es irreducible. Entonces $p \mid af = gh$ en $D[X]$ y, por el Lema 4.3.2, p es primo en $D[X]$ y por tanto podemos asumir que $p \mid g$ en $D[X]$. Es decir, existe $\overline{g} \in D[X]$ tal que $g = p\overline{g}$, de donde $gr(g) = gr(\overline{g})$.
Cancelando p en la igualdad

$$pbf = af = gh = p\overline{g}h$$

obtenemos $bf = \overline{g}h$. Como $\varphi(b) = \varphi(a) - 1 < \varphi(a)$, la hipotesis de induccion nos dice que existen $g_1, h_1 \in D[X]$ tales que $f = g_1h_1$, $gr(g_1) = gr(\overline{g}) = gr(g)$, y $gr(h_1) = gr(h)$, lo que nos da el resultado.

Example 4.3.4

Consideremos $D = \mathbb{Z}$

$$2 \in \mathbb{Z}, f = X^2 + X, g = X + 1, h = 2X$$

es inmediato que

$$2f = 2X^2 + 2X = gh$$

y $g_1 = X + 1, h_1 = X$ son los elementos que proporciona la proposición anterior.

El siguiente resultado relaciona la irreducibilidad de un polinomio sobre D con su irreducibilidad sobre K. Aunque su recíproco es falso en general: $2X$ no es irreducible como polinomio sobre $\mathbb{Z}$, pero sí en $\mathbb{Q}$ porque en ese caso 2 es unidad. Pronto veremos que el recíproco sí es válido con una condicion extra sobre el polinomio (Lema de Gauss 4.3.8).

Lemma 4.3.5

Si $f \in D[X] \setminus D$ es irreducible en $D[X]$, entonces es irreducible (y primo) en $K[X]$.

Proof

Supongamos que f no es irreducible en $K[X]$. Por la Proposición 4.3.1, existen $G, H \in K[X]$ tales que

$$f = GH, \qquad gr(G) > 0, \qquad gr(H) > 0.$$

Si $0 \neq b \in D$ es un multiplo comun de los denominadores de los coeficientes de G, se tiene

$g = bG \in D[X]$, y analogamente existe $0 \neq c \in D$ tal que $h = cH \in D[X]$. Aplicando el Lema 4.3.3 a la igualdad $(bc)f = gh$ obtenemos $g_1, h_1 \in D[X]$ tales que

$$f = g_1 h_1, \mathrm{gr}(g_1) = \mathrm{gr}(g) = \mathrm{gr}(G) > 0, \qquad \text{y} \qquad \mathrm{gr}(h_1) = \mathrm{gr}(h) = \mathrm{gr}(H) > 0,$$

lo que nos da una factorizacion no trivial de f en $D[X]$.

Podemos ya demostrar el resultado principal de esta seccion:

Theorem 4.3.6

D es un DFU si y solo si lo es $D[X]$.

Proof

Supongamos primero que $D[X]$ es un DFU. Entonces $D[X]$ es un dominio y por tanto D también, y cada $0 \neq a \in D \setminus D^*$ es producto de irreducibles de $D[X]$, que tendran grado 0 pues lo tiene a. Por el Lema 4.3.2, esa sera una factorizacion de a en irreducibles de D. Del mismo lema se deduce que todo irreducible de D es primo en D, por lo que D es un DFU.
Supongamos ahora que D es un DFU y veamos que lo es $D[X]$. Empezaremos demostrando que cada $a = a_0 + \cdots + a_n X^n \in D[X]$ (con $a_n \neq 0$) no invertible es producto de irreducibles, y lo haremos por induccion en $n + \varphi(a_n)$. Observese que a es invertible si y solo si $n + \varphi(a_n) = 0$. El caso $n + \varphi(a_n) = 1$ se resuelve facilmente. Supongamos pues que $n + \varphi(a_n) > 1$ y que a no es irreducible. Entonces existen

$$b = b_0 + \cdots + b_m X^m \quad (b_m \neq 0) \qquad \text{y} \qquad c = c_0 + \cdots + c_k X^k \quad (c_k \neq 0)$$

en $D[X]$, no invertibles, con $a = bc$ y b y c elementos de $D[X]$ que no son unidades de $D[X]$. Entonces

$$0 < m + \varphi(b_m), \quad 0 < k + \varphi(c_k) \quad \text{y} \quad n + \varphi(a_n) = m + k + \varphi(b_m) + \varphi(c_k).$$

En consecuencia, podemos aplicar la hipotesis de induccion a b y c, y pegando las factorizaciones asi obtenidas conseguimos una factorizacion en irreducibles de a.
Por la Proposición 3.4.8, solo falta demostrar que todo irreducible f de $D[X]$ es primo, y por el Lema 4.3.2 podemos suponer que $\mathrm{gr}(f) \geq 1$. Sean pues $g, h \in D[X]$ tales que $f \mid gh$ en $D[X]$, y veamos que $f \mid g$ o $f \mid h$ en $D[X]$. Obviamente, $f \mid gh$ en $K[X]$, y como f es primo en $K[X]$ por el Lema 4.3.5, podemos asumir que $f \mid g$ en $K[X]$. Es decir, existe $G \in K[X]$ tal que $g = fG$, y si demostramos que $G \in D[X]$ habremos terminado. Para ello, tomando $a \in D$ con $aG \in D[X]$ y $\varphi(a)$ mínimo, basta ver que $\varphi(a) = 0$. Supongamos que $\varphi(a) > 0$ y sean $p, b \in D$ con $a = pb$ y p primo. Entonces, en $D[X]$, se tiene $p \mid ag = f(aG)$. Como p es primo en $D[X]$ (Lema 4.3.2) y $p \nmid f$ (pues f es irreducible y $\mathrm{gr}(f) \geq 1$), deducimos que $p \mid aG$ en $D[X]$. Si $g_1 \in D[X]$ verifica $aG = pg_1$ entonces $bG = g_1 \in D[X]$, contra la minimalidad de $\varphi(a)$, y esta contradiccion termina la demostracion.

De la Proposición 4.3.1 y el Teorema 4.3.6 se deduce que $\mathbb{Z}[X]$ es un DFU pero no un DIP, lo que muestra que el reciproco del Teorema 3.5.3 no es cierto.

4.3.2 Contenido de un polinomio

Definimos una relacion de equivalencia $\sim$ en K de la siguiente forma para $x, y \in K$:

$$x \sim y \Leftrightarrow y = ux \text{ para algun } u \in D^*.$$

Claramente la clase de equivalencia que contiene a x es $xD^* = \{xu : u \in D^*\}$. En particular, si $x \in D$ entonces la clase de equivalencia que contiene a x está formada por los elementos que son asociados de x en D. Por ejemplo, $0D^* = \{0\}$, $1D^* = D^*$. Observese que $xyD^* = \{xa : a \in yD^*\} = x(yD^*)$.

Podemos definir una multiplicacion de elementos de K por elementos de $K/\sim$ poniendo

$$a(bD^*) = (ab)D^*.$$

Esto esta bien definido pues si $b_1 \sim b_2$ entonces $ab_1 \sim ab_2$. Ademas se verifica $a(b(cD^*)) = (ab)(cD^*)$.

Vamos a definir una aplicacion

$$c : K[X] \to K/\sim$$

Empezamos definiendo $c(p)$ para $p \in D[X]$ como la clase que contiene a un maximo comun divisor de los coeficientes de p, o sea, si $p = \sum_{i \geq 0} p_i X^i$ entonces

$$c(p) = \text{mcd}\{p_i : i \geq 0\}D^*.$$

Para definir $c(p)$ para un elemento $p \in K[X]$ elegimos $a \in D \setminus \{0\}$ con $ap \in D[X]$ y definimos

$$c(p) = a^{-1}c(ap).$$

Donde $a^{-1} \in K$. Esto esta bien definido pues si $a_1p, a_2p \in D[X]$ entonces $c(a_1a_2p) = a_1c(a_2p) = a_2c(a_1p)$ con lo que $a_1^{-1}c(a_1p) = a_2^{-1}c(a_2p)$.

Si $c(p) = aD^*$, entonces decimos que a es el contenido y abusaremos de la notacion escribiendo $a = c(p)$. En realidad deberiamos decir "un contenido" pero estamos abusando de la notacion, de la misma forma que lo haciamos al hablar "del maximo comun divisor" o "el mínimo comun multiplo". En todos los casos se trata de un concepto que es unico salvo multiplicacion por unidades de D.

Observese que si $a \in D$ y $p \in D[X]$ entonces las notaciones $a \mid c(p)$ y $c(p) \mid a$ no son ambiguas pues todos los valores posibles para $c(p)$ son asociados.

Veamos ahora algunas propiedades del contenido.

Proposition 4.3.7

Sean D un DFU y K su cuerpo de fracciones. Sean $a \in K$ y $p \in K[X]$.

(1) Si $a \in D$ y $p \in D[X]$ entonces $a \mid p$ en $D[X]$ si y solo si $a \mid c(p)$ en D.

(2) $c(ap) = ac(p)$.

(3) $p \in D[X]$ si y solo si $c(p) \in D$.

Proof

Pongamos $b = c(p)$.

(1) Si $a \mid p$ en $D[X]$ entonces $\forall i \geq 0,\ a \mid p_i$. Por tanto, por definición de mcd, $b = ax \implies a \mid b$ en D. Por el contrario, si $a \mid b$ entonces a es un divisor común de todos los p_i, por lo que divide a p.

(2) Sea $d \in D \setminus \{0\}$ tal que $dap, dp \in D[X]$, entonces

$$c(ap) = d^{-1}c(dap), \quad c(p) = d^{-1}c(dp).$$

Por tanto, basta probar que

$$\mathrm{mcd}(ap_0, ap_1, \ldots, ap_n) = a\,\mathrm{mcd}(p_0, p_1, \ldots, p_n).$$

En efecto, si $d = \mathrm{mcd}(p_0, p_1, \ldots, p_n)$ entonces dado $i \geq 0$ sabemos que $d \mid p_i$, por lo que $ad \mid ap_i$ y ad es divisor común de los ap_i. Si

$$c = \mathrm{mcd}(ap_0, ap_1, \ldots, ap_n)$$

entonces $ad \mid c$. Además, como d es el mcd de los p_i existen a_i tales que

$$d = a_1p_1 + \cdots + a_np_n \implies ad = aa_1p_1 + \cdots + aa_np_n$$

y como $c \mid ap_i \implies c \mid aa_ip_i$, por tanto

$$c \mid \sum_i aa_ip_i = ad$$

y finalmente $c = ad$ como queríamos ver.

(3) Pendiente

(3) Obviamente si $p \in D[X]$ entonces $b \in D$. Para demostrar la otra implicación ponemos $p = \sum_{i=0}^{k} s_iX^i$ donde cada s_i es una fracción reducida, entendiendo que si $r_i = 0$ entonces $s_i = 1$. Supongamos que $p \notin D[X]$. Eso implica que algún s_i no es unidad de D con lo que es divisible por un irreducible q y por tanto q no divide a r_i. Ponemos $s_i = q^{n_i}h_i$ con q no divide a h_i para cada i y tomamos n = $\max(n_0, n_1, \ldots, n_k) \geq 1$ y m = $\mathrm{mcm}(s_0, \ldots, s_k)$. Entonces m = q^nh con h $\in$ D y q no divide a h en D. Además $mp \in D[X] y c(mp) = mbD^*$. Pero $ms_ir_i = \frac{hr}{h_i}$ es el coeficiente de X^i en mp, que es un elemento de D que no es múltiplo de q. Luego mb, que es el máximo común divisor de los coeficientes de mp, no es múltiplo de q en D. Pero m es un elemento de D que sí es múltiplo de q en D. Por tanto b $\notin$ D.

Diremos que un polinomio es primitivo si c(p) = 1. Es decir p $\in$ D[X] es primitivo si los únicos divisores de p en D[X] que tienen grado 0 son las unidades de D[X]. Obsérvese que para todo 0 $\neq$ p $\in$ D[X] se tiene que $p/c(p)$ es primitivo y de hecho c = c(p) si y solo si p = cp1 con p1 $\in$ D[X], primitivo.

Lemma 4.3.8: Lema de Gauss

Si f, g $\in$ K[X], entonces c(fg) = c(f)c(g). En particular, si f y g son primitivos entonces fg es primitivo y si además f, g $\in$ D[X] entonces se verifica el recíproco.

Proof

Tenemos f = c(f)f1 y g = c(g)g1 con f1 y g1 primitivos. Por tanto fg = c(f)c(g)f1g1, luego para demostrar que c(fg) = c(f)c(g) basta probar que f1g1 es primitivo. En caso contrario c(f1g1) tendría un divisor irreducible p en D. Eso implica que p|f1g1. Por el Lema 3.14, p es primo en D[X] y por tanto p|f1 ó p|g1, lo que implica que p|c(f1) ó p|c(g1), en contra de que c(f1) = c(g1) = 1.

Proposition 4.3.9

Para un polinomio primitivo $f \in D[X] \setminus D$, las condiciones siguientes son equivalentes:

(1) f es irreducible en $D[X]$.

(2) f es irreducible en $K[X]$.

(3) Si $f = GH$ con $G, H \in K[X]$ entonces $gr(G) = 0$ ó $gr(H) = 0$.

Corollary 4.3.10

Si D es un DFU y K es su cuerpo de fracciones, entonces los irreducibles de $D[X]$ son los irreducibles de D y los polinomios primitivos de $D[X] \setminus D$ que son irreducibles en $K[X]$.

Appendix A

Teoría de conjuntos

A.1 Conjuntos y clases

Introducimos de manera informal en esta sección la teoría de conjuntos de von Neumann-Bernays-Gödel (denotada NBG). Para más información consultar [**?**]. Las nociones primitivas en esta teoría son las de clase, pertenencia e igualdad. Intuitivamente consideramos que una clase es una colección A de objetos tal que dado un objeto cualquiera x podemos determinar si este pertenece a la clase $(x \in A)$ o no $(x \notin A)$.

Los axiomas de la teoría se formulan en terminos de estas nociones primitivas y del cálculo de predicados lógicos de primer orden (es decir, las afirmaciones construidas usando conectores de tipo *y, o, negación, implica*, y cuantificadores $\forall, \exists$). Por ejemplo, se asume que la igualdad tiene las siguientes propiedades para cualesquiera clases A, B, C:

$$A = A, \quad A = B \implies B = A, \quad (A = B) \wedge (B = C) \implies A = C, \quad (A = B) \wedge (x \in A) \implies x \in B.$$

Por otro lado, el **axioma de extensionalidad** afirma que dos clases con los mismos elementos son iguales:

$$(x \in A \iff x \in B) \implies A = B.$$

Una clase A es un conjunto si y solo si existe una clase B tal que $A \in B$. Por tanto, un conjunto es un tipo particular de clase. Una clase que no es un conjunto se llama una clase propia. Informalmente un conjunto es una clase «pequeña», mientras que una clase propia es «grande». El **axioma de formación** de clases asegura que para cualquier enunciado $P(y)$ de primer orden involucrando a la variable y existe una clase A tal que

$$x \in A \iff (x \text{ es un conjunto} \wedge x \text{ es verdadero})$$

en tal caso denotamos a la clase A como $\{x : P(x)\}$, llamada clase de todos los x tal que se cumple $P(x)$. En ocasiones podemos describir una clase listando sus elementos: $\{a, b, c\}$.

Example A.1.1: Construcción de una clase propia

Consideremos la clase $M = \{X : X \text{ es un conjunto y } X \notin X\}$. La afirmación $X \notin X$ tiene sentido como predicado, de hecho muchos conjuntos la satisfacen (por ejemplo, el conjunto de todos los libros no es un libro). Veamos que M es una clase propia. En efecto, si M fuera un conjunto, entonces tendríamos que $M \in M$ o $M \notin M$. Pero por la definición de M, $M \in M$ implica $M \notin M$ y $M \notin M$ implica $M \in M$. Así, en ambos casos, la suposición de que M es un conjunto lleva a una contradicción: $M \in M$ y $M \notin M$.

Una clase A es una subclase de una clase B, $A \subset B$ si

$$\forall x \in A, x \in A \implies x \in B$$

por el axioma de extensionalidad y las propiedades de la igualdad tenemos

$$A = B \iff (A \subset B) \wedge (B \subset A).$$

Una subclase A de un conjunto B es un conjunto en sí misma, y en tal caso decimos que es un subconjunto.

El conjunto vacío $\emptyset$ es el conjunto sin elementos, es decir, $\forall x, x \notin \emptyset$. Como la afirmación $x \in \emptyset$ es siempre falsa tenemos de manera trivial que $\emptyset \subset B$ para cualquier clase B. Se dice entonces que A es una subclase propia de B si $A \subset B$ pero $A \neq \emptyset, A \neq B$.

El **axioma de partes** establece que para cualquier conjunto A la clase $\mathcal{P}(A)$ de todos sus subconjuntos es ella misma un conjunto, que usualmente llamamos las partes de A.

A.2 Uniones, intersecciones, complementos

Una familia de conjuntos indexada por una clase (no vacía) I es una colección de conjuntos $\{A_i : i \in I\}$. Dada una familia su unión e intersección son las clases:

$$\cup_{i \in I} A_i = \{x : x \in A_i \text{ para algún } i \in I\}$$
$$\cap_{i \in I} A_i = \{x : x \in A_i \text{ para todo } i \in I\}$$

Si I es un conjunto entonces las construcciones anteriores son conjuntos.

Si A y B son clases su diferencia es la subclase de B

$$B \setminus A = \{x : x \in B, x \notin A\}.$$

A.3 Aplicaciones

Dadas dos clases A, B la definición de aplicación es idéntica a la ya conocida para conjuntos. Se dan por conocidos los conceptos ya conocidos de dominio, rango, restricciones, etc. Dos aplicaciones son iguales si tienen el mismo dominio, rango y asignan el mismo valor a cada elemento de su dominio común.

Dada una clase A la aplicación identidad en A (denotada $1_A : A \to A$) es la aplicación dada por $a \mapsto a$. Si $S \subseteq A$, la aplicación $1_A|_S : S \to A$ se llama la aplicación inclusión de S en A.

Sean $f : A \to B$ y $g : B \to C$ aplicaciones. La composición de f y g es la aplicación $A \to C$ dada por

$$a \mapsto g(f(a)), \quad a \in A.$$

La aplicación compuesta se denota $g \circ f$ o simplemente gf. Si $h : C \to D$ es una tercera aplicación, es fácil verificar que $h(gf) = (hg)f$. Si $f : A \to B$, entonces $f \circ 1_A = f = 1_B \circ f : A \to B$.

Un diagrama:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"'] & B \arrow[dl, "g"] \\ C & \end{tikzcd}$$

se dice que es conmutativo si $gf = h$. De manera similar, el diagrama:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"'] & B \arrow[d, "g"] \\ C \arrow[r, "k"'] & D \end{tikzcd}$$

es conmutativo si $kh = gf$. Frecuentemente se trabaja con diagramas más complicados compuestos por varios triángulos y cuadrados como los anteriores. Tal diagrama se dice conmutativo si todo triángulo y cuadrado en él es conmutativo.

Las nociones de inyectividad y sobreyectividad son las usuales. Una aplicación $f : A \to B$ se dice inyectiva si

$$\forall a, a' \in A, \quad a \neq a' \implies f(a) \neq f(a').$$

Una aplicación f es sobreyectiva si $f(A) = B$; es decir,

$$\forall b \in B, \quad b = f(a) \text{ para algún } a \in A.$$

Una aplicación f se dice biyectiva si es a la vez inyectiva y sobreyectiva. Se sigue inmediatamente de estas definiciones que, para cualquier clase A, la aplicación identidad $1_A : A \to A$ es biyectiva.

Enunciamos ahora el siguiente teorema que permite caracterizar las nociones anteriores en aplicación de inversas por la derecha e izquierda.

Theorem A.3.1

Sea $f : A \to B$ una aplicación, con $A \neq \emptyset$.

(1) f es inyectiva si y solo si existe una aplicación $g : B \to A$ tal que $gf = 1_A$.

(2) Si A es un conjunto, entonces f es sobreyectiva si y solo si existe una aplicación $h : B \to A$ tal que $fh = 1_B$.

La aplicación g del teorema anterior se llama una inversa por la izquierda de f, y h se llama una inversa por la derecha de f. Si una aplicación $f : A \to B$ tiene inversas por ambos lados entonces

$$g = g1_B = g(fh) = (gf)h = 1_A h = h$$

y la aplicación $g = h$ se llama la inversa de f. Este argumento también muestra que la inversa de una aplicación (si existe) es única. Por el Teorema A.3.1, si A es un conjunto y $f : A \to B$ una aplicación, entonces

$$f \text{ es biyectiva} \iff f \text{ tiene inversa por ambos lados}$$

La única inversa de una biyección f se denota f^{-1}; claramente f es una inversa de f^{-1}, por lo que f^{-1} también es una biyección.

Remark. La caracterización de biyectividad como existencia de una inversa es válida incluso cuando A es una clase propia

A.4 Relaciones

El **axioma de formación de pares** establece que para dos conjuntos (elementos) a, b, existe un conjunto $P = \{a, b\}$ tal que $x \in P$ si y solo si $x = a$ o $x = b$; si $a = b$, entonces P es el conjunto unitario $\{a\}$. El par ordenado (a, b) se define como el conjunto $\{\{a\}, \{a, b\}\}$; su primera componente es a y su segunda componente es b. Es fácil verificar que $(a, b) = (a', b')$ si y solo si $a = a'$ y $b = b'$. El producto cartesiano de las clases A y B es la clase

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Nótese que $A \times \emptyset = \emptyset = \emptyset \times B$.

Una subclase R de $A \times B$ se llama una relación en $A \times B$. Por ejemplo, si $f : A \to B$ es una aplicación, el grafo de f es la relación $R = \{(a, f(a)) : a \in A\}$. Como f es una aplicación, R tiene la propiedad especial:

$$\text{cada elemento de } A \text{ es la primera componente de uno y solo un par ordenado en } R. \qquad (*)$$

Recíprocamente, cualquier relación R en $A \times B$ que satisfaga $(*)$ determina una única aplicación $f : A \to B$ cuyo grafo es R (definiendo $f(a) = b$, donde (a, b) es el único par ordenado en R

con primera componente a). Por esta razón es habitual identificar una aplicación con su grafo, es decir, definir una aplicación como una relación que satisface $(*)$.

Otra ventaja de este enfoque es que permite definir funciones con dominio vacío. Dado que $\emptyset \times B = \emptyset$ es el único subconjunto de $\emptyset \times B$ y satisface trivialmente $(*)$, existe una única aplicación $\emptyset \to B$. También es claro por $(*)$ que solo puede haber una aplicación con rango vacío si el dominio también es vacío.

A.5 Productos

En esta sección solo tratamos con conjuntos. No hay clases propias involucradas.

Consideremos el producto cartesiano de dos conjuntos $A_1 \times A_2$. Un elemento de $A_1 \times A_2$ es un par (a_1, a_2) con $a_i \in A_i$, $i = 1, 2$. Así, el par (a_1, a_2) determina una aplicación $f : \{1, 2\} \to A_1 \cup A_2$ mediante: $f(1) = a_1$, $f(2) = a_2$. Recíprocamente, toda aplicación $f : \{1, 2\} \to A_1 \cup A_2$ con la propiedad de que $f(1) \in A_1$ y $f(2) \in A_2$ determina un elemento $(a_1, a_2) = (f(1), f(2))$ de $A_1 \times A_2$. Por lo tanto, no es difícil ver que hay una correspondencia biyectiva entre el conjunto de todas las aplicaciones de este tipo y el conjunto $A_1 \times A_2$. Este hecho nos lleva a generalizar la noción de producto cartesiano como sigue.

Definition A.5.1: Producto

Sea $\{A_i : i \in I\}$ una familia de conjuntos indexada por un conjunto (no vacío) I. El producto (cartesiano) de los conjuntos A_i es el conjunto de todas las aplicaciones $f : I \to \bigcup_{i \in I} A_i$ tales que $f(i) \in A_i$ para todo $i \in I$. Se denota $\prod_{i \in I} A_i$.

Si $I = \{1, 2, \dots, n\}$, el producto $\prod_{i \in I} A_i$ a menudo se denota por $A_1 \times A_2 \times \cdots \times A_n$ y se identifica con el conjunto de todas las n-tuplas ordenadas $(a_1, a_2, \dots, a_n)$, donde $a_i \in A_i$ para $i = 1, 2, \dots, n$, como en el caso mencionado anteriormente donde $I = \{1, 2\}$. Una notación similar es a menudo conveniente cuando I es infinito. A veces denotaremos la aplicación $f \in \prod_{i \in I} A_i$ por $(a_i)_{i \in I}$ o simplemente (a_i), donde $f(i) = a_i \in A_i$ para cada $i \in I$.

Si algún $A_i = \emptyset$, entonces $\prod_{i \in I} A_i = \emptyset$, ya que no puede haber una aplicación $f : I \to \bigcup A_i$ tal que $f(i) \in A_i$. Si $\{A_i : i \in I\}$ y $\{B_i : i \in I\}$ son familias de conjuntos tales que $B_i \subset A_i$ para cada $i \in I$, entonces toda aplicación $I \to \bigcup B_i$ puede considerarse como una aplicación $I \to \bigcup_{i \in I} A_i$. Por lo tanto, consideramos $\prod_{i \in I} B_i$ como un subconjunto de $\prod_{i \in I} A_i$.

A.5.1 Caracterización del producto

Sea $\prod_{i \in I} A_i$ un producto cartesiano. Para cada $k \in I$, definamos una aplicación $\pi_k : \prod_{i \in I} A_i \to A_k$ mediante $f \mapsto f(k)$, o en la otra notación, $(a_i) \mapsto a_k$. π_k se llama la proyección canónica del producto sobre su k-ésima componente. Se deja como ejercicio probar que si cada A_i es no vacío, entonces cada π_k es sobreyectiva.

El producto $\prod_{i \in I} A_i$ y sus proyecciones son precisamente lo que necesitamos para el siguiente teorema

Theorem A.5.2: Propiedad universal del producto

Sea $\{A_i : i \in I\}$ una familia de conjuntos indexada por I. Entonces existe un conjunto D, junto con una familia de aplicaciones $\{\pi_i : D \to A_i : i \in I\}$, con la siguiente propiedad: para cualquier conjunto C y familia de aplicaciones $\{\varphi_i : C \to A_i : i \in I\}$, existe una única aplicación $\varphi : C \to D$ tal que $\pi_i \varphi = \varphi_i$ para todo $i \in I$. Además, D está determinado de manera única salvo biyección.

La última frase significa que si D' es un conjunto y $\{\pi_i' : D' \to A_i : i \in I\}$ una familia de aplicaciones que tienen la misma propiedad que D y $\{\pi_i\}$, entonces existe una biyección $D \to D'$.

Proof

(Existencia) Sea $D = \prod_{i \in I} A_i$ y sean las aplicaciones π_i las proyecciones sobre las i-ésimas componentes. Dado C y las aplicaciones φ_i, definamos $\varphi : C \to \prod_{i \in I} A_i$ por $c \mapsto f_c$, donde $f_c(i) = \varphi_i(c) \in A_i$. Se sigue inmediatamente que $\pi_i \varphi = \varphi_i$ para todo $i \in I$. Para mostrar que φ es única, supongamos que $\varphi' : C \to \prod_{i \in I} A_i$ es otra aplicación tal que

$\pi_i\varphi' = \varphi_i$ para todo $i \in I$ y demostremos que $\varphi = \varphi'$. Para ello, debemos mostrar que para cada $c \in C$, $\varphi(c)$ y $\varphi'(c)$ son el mismo elemento de $\prod_{i\in I} A_i$, es decir, $\varphi(c)$ y $\varphi'(c)$ coinciden como funciones en I: $(\varphi(c))(i) = (\varphi'(c))(i)$ para todo $i \in I$. Pero por hipótesis y la definición de π_i, tenemos para todo $i \in I$:

$$(\varphi'(c))(i) = \pi_i\varphi'(c) = \varphi_i(c) = f_c(i) = (\varphi(c))(i).$$

(Unicidad) Supongamos que D' (con aplicaciones $\pi_i' : D' \to A_i$) tiene la misma propiedad que $D = \prod_{i\in I} A_i$. Si aplicamos esta propiedad (para D) a la familia de aplicaciones $\{\pi_i' : D' \to A_i\}$ y también la aplicamos (para D') a la familia $\{\pi_i : D \to A_i\}$, obtenemos (únicas) aplicaciones $\varphi : D' \to D$ y $\psi : D \to D'$ tales que los siguientes diagramas son conmutativos para cada $i \in I$:

$$\begin{tikzcd} D \arrow[r, dashed, "\psi"] \arrow[dr, "\pi_i"'] & D' \arrow[d, "\pi_i'"] \\ & A_i \end{tikzcd}$$

$$\begin{tikzcd} D' \arrow[r, dashed, "\varphi"] \arrow[d, "\pi_i'"'] & D \arrow[dl, "\pi_i"] \\ A_i & \end{tikzcd}$$

Combinando estos, obtenemos para cada $i \in I$ un diagrama conmutativo:

$$\begin{tikzcd} D \arrow[r, "\varphi\psi"] \arrow[d, "\varphi_i"'] & D \arrow[dl, "\pi_i"] \\ A_i & \end{tikzcd}$$

Así, $\varphi\psi : D \to D$ es una aplicación tal que $\pi_i(\varphi\psi) = \pi_i$ para todo $i \in I$. Pero por la demostración anterior, hay una única aplicación con esta propiedad. Como la aplicación $1_D : D \to D$ también satisface $\pi_i 1_D = \pi_i$ para todo $i \in I$, debemos tener $\varphi\psi = 1_D$ por unicidad. Un argumento similar muestra que $\psi\varphi = 1_D$. Por lo tanto, φ es una biyección por (13), y $D = \prod_{i\in I} A_i$ está determinado de manera única salvo biyección.

Nótese que el enunciado del Teorema A.5.2 no menciona elementos; involucra solo conjuntos y aplicaciones. Establece que el producto $\prod_{i\in I} A_i$ se caracteriza por una cierta propiedad universal que cumplen todas las aplicaciones. Esta propiedad se resume en el siguiente diagrama conmutativo:

$$\begin{tikzcd} C \arrow[r, dashed, "\varphi"] \arrow[dr, "\varphi_i"'] & D \arrow[d, "\pi_i"] \\ & A_i \end{tikzcd}$$