Álgebra I

Versión 2.2 [1]

Cursos 2019/2022 [2]

José Gómez Torrecillas
Departamento de Álgebra
Universidad de Granada

[1] Versión revisada de [**2**], en particular se corrigen erratas. El Capítulo I ha sido reestructurado. También se incluyen nuevos ejercicios.

[2] versión: 10 de abril de 2022

Índice general

Capítulo 1

Fundamentos

1.1. Conjuntos

Es notorio que una cualidad fundamental de las Mátemáticas es la precisión de sus enunciados. Para conseguir aquélla, hay que aceptar unas nociones primitivas a partir de las cuales definir las demás. La opción más extendida (casi universalmente entre los matemáticos) es admitir la noción de *conjunto* y de *elemento* como conceptos primitivos o indefinibles, y definir las demás nociones a partir de ellos. La relación entre ambos conceptos primitivos está regulada por la *pertenencia* según las siguientes reglas. En las mismas, podemos entender que el significado de la palabra "objeto" es "objeto matemático".

R1. Dado un conjunto X y cualquier objeto a, o bien a pertenece a X, o bien a no pertenece a X. Simbólicamente, escribiremos $a \in X$ o $a \notin X$. Ambas opciones son excluyentes. Si $a \in X$, diremos que a es un *elemento* de X o, también, que X *contiene al elemento* a.

R2. Un conjunto X está completamente determinado por sus elementos. Dicho de otra forma, dados conjuntos X, Y, se considerarán iguales si para todo objeto a la afirmación $a \in X$ es equivalente a la afirmación $a \in Y$.

R3. Un objeto no puede ser elemento de sí mismo. Es decir, está **prohibido** admitir "$a \in a$" cualquiera sea el objeto a.

R4. Dado un objeto a, podemos formar el conjunto $\{a\}$ definido por la siguiente propiedad: $a \in \{a\}$ pero $b \notin \{a\}$ para todo otro objeto b distinto de a.

R5. Admitimos que existe el conjunto vacío $\emptyset$ definido por la propiedad $a \notin \emptyset$ para todo objeto a.

OBSERVACIÓN 1.1. La Regla 3 impide considerar el conjunto cuyos elementos son todos los conjuntos.

EJEMPLO 1.2. En matemáticas se usan palabras del lenguaje natural (en nuestro caso, el español) para designar objetos o conceptos que no coinciden con los designados por el uso común. Por ejemplo, si menciono el conjunto de "todas las buenas personas", está claro que no estoy definiendo un conjunto desde el punto de vista matemático, ya que la regla R1 no puede aplicarse por lo difuso del concepto "buena persona".

En contraste, el conjunto de todas las personas que tienen un pasaporte a su nombre vigente a fecha de hoy expedido por el Reino de España, sí parece más cercano a un conjunto en el sentido matemático[1].

[1] Otra cosa es la dificultad para aplicar efectivamente la regla R1, ya que las personas pueden mentir, tener un pasaporte falsificado, haberlo tirado a la basura, etc. Esto quiere decir que el conjunto que hemos definido es más bien el de los pasaportes vigentes a día de hoy expedidos por el Reino de España, como abstracción de una "propiedad" que una persona puede tener o no.

Admitiremos que conocemos el conjunto $\mathbb{N}$ cuyos elementos son todos los números naturales. Sus elementos, que son los números “que sirven para contar”, es decir, el cero, el uno, el dos, etcétera, podrían construirse formalmente a partir de las reglas que nos hemos dado, pero esto nos llevaría un tiempo del que no disponemos. Nos limitamos pues a aceptar que, de acuerdo con nuestras reglas, estamos diciendo que, dado un objeto, dicho objeto pertenece a $\mathbb{N}$ o no, nada menos... Reiteremos que, en nuestra exposición, $0 \in \mathbb{N}$.

Unión de conjuntos. Con las reglas enunciadas, ya podemos comenzar a construir conjuntos a partir de objetos matemáticos dados (incluyendo otros conjuntos). Con tal fin, las definiciones son cruciales. Aquí está la primera.

DEFINICIÓN 1.3. Dados conjuntos X, Y, definimos su *unión* como el conjunto $X \cup Y$ determinado por los objetos a tales que $a \in X$ o bien $a \in Y$. Observemos que $X \cup Y = Y \cup X$.

EJEMPLO 1.4. Si a y b son objetos, podemos formar, de acuerdo con la Regla 4, los conjuntos $\{a\}$ y $\{b\}$. Y ahora podemos formar $\{a\} \cup \{b\}$. Si se piensa qué dice la Definición 1.3, es razonable usar la notación $\{a, b\} = \{a\} \cup \{b\}$. Observemos que $\{a, b\} = \{b, a\}$. También merece la pena darse cuenta de que $\{a, b\} = \{a\}$ si, y sólo si, $a = b$.

EJEMPLO 1.5. La notación introducida en el Ejemplo 1.4 se generaliza a la llamada definición por *extensión* de un conjunto. Esto consiste en que, partiendo de una lista de objetos $a, b, c, \dots$, formamos el conjunto $\{a, b, c, \dots\}$ cuyos elementos son los objetos de la lista. Tomemos, por ejemplo, la lista de números $1, 1, 2, 3$. Podemos formar el conjunto $\{1, 1, 2, 3\}$. Observemos que, como consecuencia de la Regla 2, $\{1, 1, 2, 3\} = \{1, 2, 3\}$, lo que indica una diferencia clara entre lista y conjunto.

Normalmente, los conjuntos definidos por extensión suelen ser finitos. Pero hay excepciones: por ejemplo, se suele escribir $\mathbb{N} = \{0, 1, 2, \dots\}$.

EJEMPLO 1.6. De acuerdo con las reglas 5 y 4, podemos formar el conjunto $\{\emptyset\}$. Y ahora, según el Ejemplo 1.4, podemos formar el conjunto $\{\emptyset, \{\emptyset\}\}$. Éste ya tiene dos elementos distintos, ¿verdad?.

EJERCICIO 1. Sea X un conjunto. Demostrar que $X \cup \{\emptyset\} = X$ si, y sólo si, $\emptyset \in X$.

DEFINICIÓN 1.7. La noción de unión de subconjuntos se extiende para familias de más de dos conjuntos. De hecho, si Γ es un conjunto cuyos elementos son conjuntos, entonces la unión $\bigcup_{Y \in \Gamma} Y$ es el conjunto formado por los elementos a tales que $a \in Y$ para algún $Y \in \Gamma$.

EJERCICIO 2. Sea $\Gamma = \{\{0, 1\}, \{1, 2\}, \{1, 3, 5\}\}$. Calcular $\bigcup_{Y \in \Gamma} Y$.

Es muy común definir un conjunto A mediante la descripción de los objetos que satisfacen una propiedad P. Así, se usa la notación

$$A = \{a \mid a \text{ satisface } P\}.$$

Así, por ejemplo, si X e Y son conjuntos, entonces podemos poner

$$X \cup Y = \{a \mid a \in X \text{ o } a \in Y\}.$$

Inclusión, intersección, diferencia y potencia de conjuntos. La segunda definición fundamental es la de subconjunto.

DEFINICIÓN 1.8. Sean X e Y conjuntos. Diremos que X es un *subconjunto* de Y si para todo objeto a, la condición $a \in X$ implica que $a \in Y$. Escribiremos entonces $X \subseteq Y$. También se dice que X *está incluido* en Y.

OBSERVACIÓN 1.9. Observemos que, de acuerdo con la Regla 2, tener que $X \subseteq Y$ e $Y \subseteq X$ es lo mismo que decir que $X = Y$.

OBSERVACIÓN 1.10. Usando la regla lógica llamada *contra-recíproco*, vemos que afirmar que $X \subseteq Y$ es equivalente a afirmar que la condición $a \notin Y$ implica que $a \notin X$. Deducimos fácilmente que $\emptyset \subseteq X$ cualquiera sea el conjunto X.

EJERCICIO 3. Sean X, Y conjuntos. Demostrar que $X \cup Y = Y$ si, y sólo si, $X \subseteq Y$.

EJERCICIO 4. Mostrar tres conjuntos X, Y, Z que verifiquen que $X \in Y \in Z$ y, al mismo tiempo, $X \subseteq Y \subseteq Z$.

DEFINICIÓN 1.11. Dados dos conjuntos X, Y, definimos su *intersección* como el conjunto $X \cap Y$ determinado por los objetos a tales que $a \in X$ y $a \in Y$. Brevemente,

$$X \cap Y = \{a \mid a \in X \text{ y } a \in Y\}.$$

Es perfectamente posible que $X \cap Y = \emptyset$. En tal caso, diremos que X e Y son *disjuntos*.

EJERCICIO 5. Si X, Y son conjuntos, demostrar que $X \cap Y = Y$ si, y sólo si, $Y \subseteq X$.

OBSERVACIÓN 1.12. Como ya observamos en el caso de la unión, la definición de intersección puede extenderse a familias de más de dos conjuntos. Concretamente, si Γ es un conjunto cuyos elementos son conjuntos, podemos definir $\bigcap_{Y \in \Gamma} Y$ como el conjunto cuyos elementos son aquellos objetos a tales que $a \in Y$ para todo $Y \in \Gamma$.

DEFINICIÓN 1.13. Dados conjuntos X, Y, definimos el conjunto *diferencia* entre Y y X como

$$Y \setminus X = \{a \mid a \in Y \text{ y } a \notin X\}.$$

Es también usual utilizar la siguiente forma abreviada de definir el mismo conjunto:

$$Y \setminus X = \{a \in Y \mid a \notin X\}.$$

Por último, cuando, por el contexto, es claro quién es Y, y $X \subseteq Y$ se suele escribir $\overline{X}$ para referirse a $Y \setminus X$. En este caso, $\overline{X}$ se llama *complemento* de X en Y.

Dado un conjunto X, definimos su *conjunto potencia* o *conjunto de las partes de* X como

$$\mathcal{P}(X) = \{A \mid A \subseteq X\}$$

EJEMPLO 1.14. Observemos que $\mathcal{P}(\emptyset) = \{\emptyset\}$ y, por tanto[2], $\mathcal{P}(\emptyset) \neq \emptyset$. ¿Cuántos elementos tiene $\mathcal{P}(\mathcal{P}(\emptyset))$?.

[2]Es fundamental entender esto.

1.2. Correspondencias y relaciones

En esta sección, vamos a introducir construcciones básicas de la Matemática, como son el producto cartesiano, las correspondencias, y varios tipos de relaciones (preorden, orden y equivalencia).

Producto cartesiano y correspondencias. Dados conjuntos X, Y, para cada par de elementos $x \in X$, $y \in Y$, admitiremos como objeto matemático el *par ordenado* (x, y). Construimos el conjunto $X \times Y$ llamado *producto cartesiano de* X *e* Y, como el conjunto de todos estos pares ordenados, es decir,

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}.$$

Observemos que, en general, $(x, y) \neq (y, x)$ (por eso hablamos de par **ordenado**). También se tiene que $X \times Y \neq Y \times X$ salvo que $X = Y$.

EJERCICIO 6. Razonar que $\emptyset \times X = \emptyset = X \times \emptyset$, cualquiera sea el conjunto X.

EJERCICIO 7. Sean $I = \{\emptyset\}, II = I \cup \{I\}$. Describir por extensión $II \times II$.

DEFINICIÓN 1.15. Dados conjuntos X e Y, llamaremos *correspondencia de* X *a* Y a todo subconjunto C de $X \times Y$. Cuando $(x, y) \in C$ se escribe a veces xCy y se lee "x se corresponde con y", o terminologías similares.

Nota: En algunos textos, se usa la palabra "relación" para referirse a una correspondencia. Nosotros reservaremos la palabra "relación" en un sentido más restrictivo, de acuerdo con la Definición 1.17.

El *dominio* de una correspondencia C de X a Y se define como

$$\mathrm{Dom}(C) = \{x \in X \mid xCy \text{ para algún } y \in Y\}.$$

La *imagen* de C se define como

$$\mathrm{Im}(C) = \{y \in Y \mid xCy \text{ para algún } x \in X\}.$$

EJERCICIO 8. Consideremos la correspondencia C de $\{1, 2, 3\}$ a $\{0, 2\}$ definida por aCb si $a > b$, para $a \in \{1, 2, 3\}$, $b \in \{0, 2\}$. Dar por extensión C, el dominio de C y la imagen de C.

EJERCICIO 9. Sonia, Carlos y Belén son amigos y usan servicios de mensajería instantánea. Concretamente, Sonia es usuaria de *Rauda* y *Vitesse*, Carlos de *Veloz* y Belén de *Vitesse* y *Veloz*. Pongamos

$$X = \{S, C, B\},$$

donde cada amigo está simbolizado por la inicial de su nombre. Sea

$$Y = \{R, V_1, V_2\},$$

donde R simboliza el servicio *Rauda*, en tanto que V_1 simboliza *Vitesse* y V_2, *Veloz*.

Definir una correspondencia de X a Y que sirva de modelo para la situación descrita.

La construcción de pares ordenados, y la consecuente definición de producto cartesiano, puede extenderse sin dificultades a un mayor número de componentes, de acuerdo con la siguiente definición.

DEFINICIÓN 1.16. Sea n un número natural distinto del cero, y $X_1, \dots, X_n$ conjuntos. Dados elementos $x_1 \in X_1, \dots, x_n \in X_n$, podemos formar la n-*tupla* $(x_1, \dots, x_n)$. El *producto cartesiano de* $X_1, \dots, X_n$ se define como

$$X_1 \times \cdots \times X_n = \{(x_1, \dots, x_n) \mid x_i \in X_i \text{ para } 1 \leq i \leq n\}$$

Por ejemplo,

$$X_1 \times X_2 \times X_3 = \{(x_1, x_2, x_3) \mid x_1 \in X_1, x_2 \in X_2, x_3 \in X_3\}.$$

Observemos que una n–tupla no es sino una lista ordenada de elementos escogidos de una lista ordenada, y de igual longitud, de conjuntos.

Para un conjunto X, el producto cartesiano de n copias de X se denotará por X^n.

Vamos a suponer en lo que sigue que se tiene cierta familiaridad con el conjunto $\mathbb{R}$ de los números reales, siquiera informalmente. También asumimos algunos conocimientos de Geometría en el plano (triángulos, círculos, y figuras de este tipo).

EJERCICIO 10. Sea $\triangle$ el conjunto de los triángulos en el plano. Definimos la correspondencia C de $\triangle$ a $\mathbb{R}^3$ declarando, para $x \in \triangle$ y $(\alpha, \beta, \gamma) \in \mathbb{R}^3$, que $xC(\alpha, \beta, \gamma)$ si los valores α, β, γ miden los ángulos de x. Calcular $\mathrm{Im}(C)$.

Relaciones. Las relaciones[3] no son más que correspondencias de un conjunto a sí mismo, de acuerdo con la siguiente definición.

DEFINICIÓN 1.17. Sea X un conjunto. Una *relación en* X es, por definición, una correspondencia de X a X, esto es, un subconjunto del producto cartesiano $X \times X$.

EJERCICIO 11. En el conjunto II definido en el Ejercicio 7, definimos la relación $R \subseteq \mathrm{II} \times \mathrm{II}$ dada por xRy si, y sólo si, $x \in y$. Describir explícitamente todos los pares ordenados que pertenecen a R.

Si el conjunto X es suficientemente pequeño para poder representar gráficamente sus elementos como, por ejemplo, puntos, podemos representar una relación R en X gráficamente como sigue: trazaremos una flecha de x a x', donde $x, x' \in X$, si $(x, x') \in R$. Esta representación gráfica se llama *grafo*[4] de la relación R, y los elementos de X adquieren el nombre de *vértices* del grafo.

EJEMPLO 1.18. Cinco ciudadanos mantienen páginas web personales. El cuadro 1 recoge información sobre los enlaces de unas páginas a otras en este grupo de personas.

CUADRO 1. Enlaces entre páginas personales.

	Ana	Bob	Clark	Dana	Emma
Ana	0	1	1	0	0
Bob	0	0	0	1	0
Clark	1	1	0	1	1
Dana	1	0	0	0	1
Emma	1	0	1	0	0

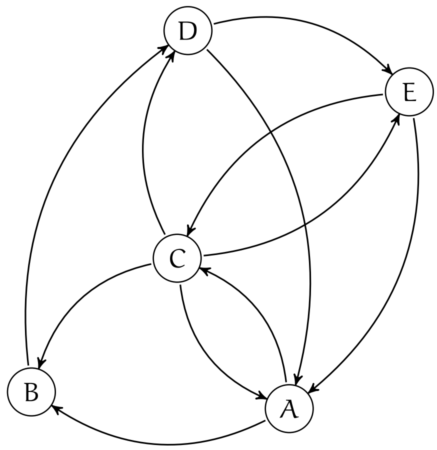
Interpretemos la primera línea del cuadro: Pensamos que la página de Ana tiene enlaces a las de Bob y Clark, por lo que ponemos un 1 las casillas correspondientes, pero no los tiene a las de Dana ni Emma, con lo que asignamos un 0.

[3]Estrictamente hablando, vamos a considerar sólo relaciones binarias
[4]Más específicamente, obtenemos un grafo dirigido.

Para construir un modelo matemático de la información recogida en el Cuadro 1, formamos un conjunto P con las iniciales de los dueños de las páginas personales, esto es

$$P = \{A, B, C, D, E\}.$$

En P definimos la relación R dada por pRp' si la página de p tiene un enlace a la página de p', donde $p, p' \in P$. El siguiente es el grafo de la relación R.



1.3. Pre-órdenes, órdenes y relaciones de equivalencia

En Matemáticas, se han demostrado útiles relaciones que satisfacen ciertas propiedades. Algunas de estas propiedades fundamentales están recogidas en la siguiente definición.

DEFINICIÓN 1.19. Sea R una relación en un conjunto no vacío X. Diremos que R es

1. *reflexiva* si xRx para todo $x \in X$.
2. *transitiva* si para todo $x, y, z \in X$, si xRy e yRz, entonces xRz.
3. *simétrica* si para todo $x, y \in X$, la condición xRy implica yRx.
4. *antisimétrica* si para todo $x, y \in X$, si xRy e yRx, entonces $x = y$.

EJEMPLO 1.20. La relación descrita en el Ejemplo 1.18 no es reflexiva, ni transitiva, ni simétrica, ni antisimétrica[5]. Esto significa que, para estudiar relaciones como ésa (es decir, grafos) se necesitan técnicas que no vamos estudiar en este curso, sino en Álgebra II.

EJERCICIO 12. Si R es una relación en un conjunto X entonces, para cada subconjunto $S \subseteq X$, tenemos la relación en S dada por $R \cap (S \times S)$, que se llama *relación inducida* en S por R o *restricción de* R *a* S. Comprobar que cada una de las propiedades listadas en la Definición 1.19 se heredan en las relaciones inducidas.

Pre-órdenes y órdenes. Comencemos con la definición de pre-orden.

DEFINICIÓN 1.21. Una relación se llama un *pre-orden* si es reflexiva y transitiva.

Un ejemplo fundamental de pre-orden es el dado por la relación “implicación” en un conjunto de afirmaciones. Veamos un ejemplo.

[5]Explicar por qué.

EJEMPLO 1.22. Consideremos las siguientes afirmaciones sobre un número natural n mayor que 3.

P1 n es par.
P2 El único divisor primo de n es 2.
P3 El resto de dividir n entre 6 es 2.
P4 n es una potencia de 2.
P5 n es un múltiplo de 4.

En el conjunto

$$X = \{P1, P2, P3, P4, P5\}$$

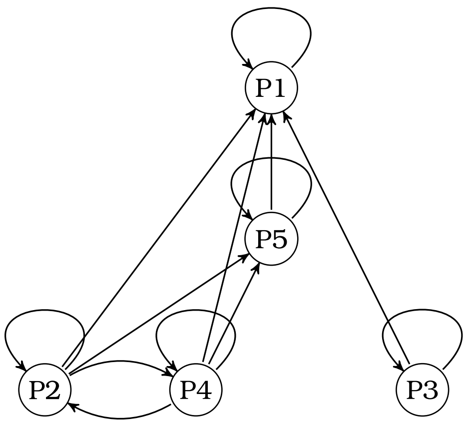
definimos la relación $\Rightarrow$ dada, para $p, q \in X$, por $p \Rightarrow q$ si p implica q.

Las reglas básicas de la lógica nos dicen que $\Rightarrow$ es reflexiva y transitiva, así que se trata de un pre-orden[6] en X.

La comprensión de la siguiente observación es crucial para tu futuro como estudiante de matemáticas: la veracidad de la afirmación "p implica q" no depende del valor concreto del número natural n, sino de que siempre que n satisfaga p, necesariamente ha de satisfacer q.

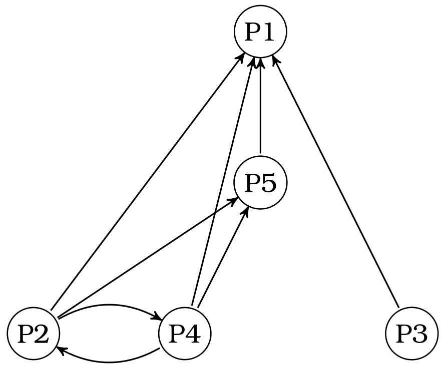
Como hay una cantidad infinita de valores que n puede tomar, para verificar si $p \Rightarrow q$ no queda más remedio que buscar una demostración, para afirmarlo, o algún argumento para descartarlo. Es claro que decidir cada implicación depende de cuánto sepamos sobre los números naturales.

Bien, en el caso que nos ocupa, el grafo de la relación $\Rightarrow$ en X es

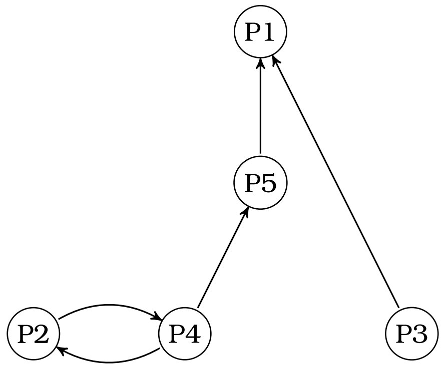


La información contenida en el anterior grafo puede presentarse de manera más simplificada usando las propiedades de la relación $\Rightarrow$. Por ejemplo, los bucles que adornan cada vértice expresan que la relación es reflexiva, luego pueden entenderse implícitamente y, por tanto, eliminarse sin perder información. El resultado es

[6] Obviamente, esto sería cierto para cualquier conjunto de afirmaciones bien definidas en que definamos la relación "implicación".



Puesto que la relación $\Rightarrow$ es transitiva, podemos condensar aún más la información, de la manera siguiente:



Esta representación gráfica del pre-orden $\Rightarrow$ en X se llama *diagrama de Hasse*[7]. A partir del mismo, usando las propiedades reflexiva y transitiva, puede reconstruirse completamente la relación.

OBSERVACIÓN 1.23. Dado cualquier conjunto X de afirmaciones no ambiguas sobre objetos matemáticos, podemos definir el pre-orden $\Rightarrow$ en X dado por la implicación.

EJERCICIO 13. Calcular el diagrama de Hasse del pre-orden $\Rightarrow$ que obtendríamos en X si, en el Ejemplo 1.22, suponemos que n es un número natural mayor que 1. ¿Qué ha cambiado? ¿Por qué?

Órdenes. Un *orden* o *relación de orden* es un pre-orden que satisface la propiedad antisimétrica. Explícitamente, se tiene la siguiente definición.

DEFINICIÓN 1.24. Un *orden* en un conjunto X es una relación en X que es reflexiva, transitiva y antisimétrica. Es tradición denotar por símbolos como $\preceq$ a las relaciones de orden. Si $\preceq$ es una relación de orden en X, diremos que $(X, \preceq)$ es un *conjunto ordenado*.

No obstante la tradición mencionada en la anterior definición para la notación, nuestro primer ejemplo no la respeta.

[7]Esta definición se suele dar para conjuntos ordenados, pero es útil extenderla para pre-órdenes

EJEMPLO 1.25. En $\mathbb{N}$ definimos la relación $\mid$ como sigue: dados $a, b \in \mathbb{N}$, establecemos que $a \mid b$ si existe $c \in \mathbb{N}$ tal que $b = ac$. Aquí, la yuxtaposición indica el producto de números naturales. Esto es, $a \mid b$ si a es un divisor de b, equivalentemente, si b es un múltiplo de a. Es fácil comprobar que $(\mathbb{N}, \mid)$ es un conjunto ordenado.

El segundo ejemplo es el más natural.

EJEMPLO 1.26. En $\mathbb{N}$ consideramos la relación $\leq$ dada, para $a, b \in \mathbb{N}$, por $a \leq b$ si $a < b$ o bien $a = b$. Equivalentemente, $a \leq b$ si, y sólo si, existe $c \in \mathbb{N}$ tal que $b = a + c$. Claramente, $(\mathbb{N}, \leq)$ es un conjunto ordenado.

DEFINICIÓN 1.27. Una relación de orden $\preceq$ en un conjunto X se dirá *total* si para todo $x, y \in X$ se tiene que $x \preceq y$ o bien $y \preceq x$. Diremos entonces que $(X, \preceq)$ es un *conjunto totalmente ordenado*.

EJEMPLO 1.28. El orden natural en $\mathbb{N}$ (ver Ejemplo 1.26) es total, en tanto que el orden establecido en el mismo conjunto en el Ejemplo 1.25 no es total.

A veces, para recalcar que un orden no se supone total, se dice que es un orden parcial.

Concluimos poniendo de manifiesto que la inclusión da conjuntos ordenados.

EJEMPLO 1.29. Si X es un conjunto, entonces $(\mathcal{P}(X), \subseteq)$ es un conjunto ordenado. Este orden no es total si X tiene, al menos, dos elementos.

Relaciones de equivalencia. Un pre-orden que verifica la propiedad simétrica se llama relación de equivalencia, de acuerdo con la siguiente definición.

DEFINICIÓN 1.30. Sea R una relación en un conjunto X. Diremos que la relación R es *de equivalencia* si es reflexiva, simétrica y transitiva.

EJEMPLO 1.31. Si X es un conjunto, entonces la relación *identidad*, definida por

$$\mathrm{id}_X = \{(x, x) : x \in X\}$$

es de equivalencia. Según esta relación, dos elementos de X están relacionados si, y sólo si, son iguales.

EJEMPLO 1.32. Definimos en $\mathbb{N}$ la relación R dada para $a, b \in \mathbb{N}$ por aRb si $a + b$ es par (es decir, un mútiplo de 2; obsérvese que 0 es par). Se trata de una relación de equivalencia.

En efecto, es reflexiva, puesto que, para todo $a \in \mathbb{N}$, $a + a = 2a$ y, por tanto, aRa.

También es claramente simétrica ya que, si aRb para ciertos $a, b \in \mathbb{N}$, entonces $a + b$ es par. Pero $a + b = b + a$, luego bRa.

Comprobemos por último que es transitiva: dados $a, b, c \in \mathbb{N}$ satisfaciendo aRb y bRc, tenemos que existen $k, k' \in \mathbb{N}$ tales que $a + b = 2k$ y $b + c = 2k'$. De esta manera, $a + b + b + c = 2k + 2k'$. Esto implica que $a + c + 2b = 2(k + k')$. Por tanto[8], $a + c$ ha de ser par, lo que prueba que aRc.

Llegamos a un punto crucial, la definición de clase de equivalencia.

[8]Esto podría considerarse evidente. Quien crea que, en este momento, no es así, puede consultar el Lema 1.70.

DEFINICIÓN 1.33. Sea R una relación de equivalencia en un conjunto no vacío X, y $x \in X$. La *clase de equivalencia de* x *bajo (o con respecto de)* R es el siguiente subconjunto de X:

$$[x]_R = \{y \in X \mid xRy\}.$$

Un subconjunto $\mathcal{C}$ de X se dirá una clase de equivalencia bajo R si es de la forma $\mathcal{C} = [x]_R$ para algún $x \in X$. El elemento x se llama *representante* de la clase de equivalencia $\mathcal{C}$.

Una destreza fundamental para un matemático es saber decidir cuando dos clases de equivalencia, dadas por dos representantes distintos, son realmente distintas.

PROPOSICIÓN 1.34. *Sea* R *una relación de equivalencia en* X, $x, y \in X$. *Las siguientes condiciones son equivalentes*[9]*.*

(a) xRy*;*
(b) $y \in [x]_R$*;*
(c) $x \in [y]_R$*;*
(d) $[x]_R \cap [y]_R \neq \emptyset$*;*
(e) $[x]_R = [y]_R$*.*

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Por definición de $[x]_R$.
(b) $\Rightarrow$ (c). Como $y \in [x]_R$, tenemos que xRy. Al ser R simétrica, deducimos que yRx, lo que da que $x \in [y]_R$.
(c) $\Rightarrow$ (d). Como R es reflexiva, tenemos que $x \in [x]_R$. Así que, si $x \in [y]_R$, deducimos que $x \in [x]_R \cap [y]_R$.
(d) $\Rightarrow$ (e). Demostremos que $[x]_R \subseteq [y]_R$. Sea $t \in [x]_R$ Por hipótesis, existe $z \in [x]_R \cap [y]_R$. Así, xRz y, por la propiedad simétrica, deducimos que zRx. Pero también tenemos que yRz, de donde, por la propiedad transitiva, yRx. Por último, xRt, así que la propiedad transitiva garantiza que yRt. Esto es, $t \in [y]_R$, y hemos demostrado que $[x]_R \subseteq [y]_R$. La inclusión recíproca se demuestra igual, intercambiando los papeles de x e y.
(e) $\Rightarrow$ (a). Como R es reflexiva, $y \in [y]_R$. Así, $y \in [x]_R$, lo que da xRy. $\square$

Llegamos al delicado punto de definir qué es un conjunto cociente bajo una relación de equivalencia. La idea es muy sencilla: cada clase de equivalencia se convierte en un elemento del conjunto cociente.

DEFINICIÓN 1.35. Sea R una relación de equivalencia en un conjunto no vacío X. El *conjunto cociente de* X *bajo* R se define como

$$X/R = \{[x]_R \mid x \in X\}.$$

Es de mayor importancia comprender que los elementos de X/R **no** son elementos de X, sino subconjuntos de X. Dicho de otro modo, X/R es un subconjunto de $\mathcal{P}(X)$.

EJEMPLO 1.36. Vamos a calcular $\mathbb{N}/R$, donde R es la relación de equivalencia definida en el Ejemplo 1.32. Recordemos que, para $a, b \in \mathbb{N}$, aRb si $a + b$ es par. Por ejemplo, $0Rb$ es lo mismo que decir que $0 + b = b$ es par. Por tanto,

$$[0]_R = \{b \in \mathbb{N} \mid b \text{ es par}\}.$$

[9]Es meta-divertido pensar que, en verdad, lo que probamos es que la relación implicación es de equivalencia en el conjunto de las afirmaciones enunciadas, resultando una única clase de equivalencia ahí.

O sea, $[0]_R$ es el conjunto de los números naturales pares. Observemos que, de la Proposición 1.34, deducimos que

$$[0]_R = [2]_R = [4]_R = \cdots$$

Tenemos que

$$[1]_R = \{b \in \mathbb{N} \mid 1 + b \text{ es par}\} = \{b \in \mathbb{N} \mid b \text{ es impar}\}.$$

Así que

$$[1]_R = [3]_R = [5]_R = \cdots$$

Además, puesto que $0 \notin [1]_R$, deducimos de la Proposición 1.34 que $[0]_R \neq [1]_R$. Por otra parte, todo número natural es par o impar, por lo que no hay más clases de equivalencia. Así, en virtud de la Regla 2,

$$\mathbb{N}/R = \{[0]_R, [1]_R\},$$

un conjunto de dos elementos. Insistamos en que estos elementos son el conjunto de los números naturales pares y el conjunto de los números naturales impares.

Atención, la igualdad

$$\mathbb{N}/R = \{[291384512394588]_R, [459724527]_R\}$$

es perfectamente correcta.

EJERCICIO 14. Pongamos $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. En $\mathbb{N} \times \mathbb{N}_+$ definimos la relación R dada, para $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}_+$, por

$$(a, b)R(c, d) \quad \text{si } ad = bc.$$

Demostrar que R es una relación de equivalencia. El conjunto cociente

$$\mathbb{Q}_+ = (\mathbb{N} \times \mathbb{N}_+)/R$$

captura la noción de razón entre dos números naturales. Sus elementos son los números racionales positivos. Normalmente, se escribe

$$[(a, b)]_R = \frac{a}{b}.$$

Así, por ejemplo, la igualdad $1/2 = 2/4$ no es más que la igualdad $[(1, 2)]_R = [(2, 4)]_R$.

Orden construido desde un pre-orden. Seguidamente, vamos a definir una relación de equivalencia en cualquier conjunto pre-ordenado que hace que el conjunto cociente resulte ordenado de manera natural.

PROPOSICIÓN 1.37. *Sea $(X, \propto)$ un conjunto pre-ordenado.*

1. *La relación R definida en X declarando, para $x, y \in X$, que xRy si $x \propto y$ e $y \propto x$, es de equivalencia.*
2. *La relación $\preceq$ en X/R, dada, para $[x]_R, [y]_R \in X/R$, por $[x]_R \preceq [y]_R$ si $x \propto y$, está bien definida y es un orden.*

DEMOSTRACIÓN. 1. Comprobar que R es de equivalencia es bastante fácil y se deja como ejercicio.

2. Comprobemos que $\preceq$ está bien definida. Esto significa que hemos de demostrar que, dados $x, x', y, y' \in X$, si $[x]_R = [x']_R$, $[y]_R = [y']_R$ y $x \propto y$, entonces $x' \propto y'$. Pero esto es consecuencia de la propiedad transitiva de $\propto$: en efecto, las hipótesis sobre x, x', y, y' implican que $x' \propto x$, $x \propto y$ e $y \propto y'$, de donde $x' \propto y'$.

También se deja como ejercicio comprobar que $\preceq$ es un orden en X/R. $\square$

EJEMPLO 1.38. Consideremos un conjunto de afirmaciones P con el pre-orden $\Rightarrow$ definido por la implicación lógica. Aquí, la relación de equivalencia dada en P por la Proposición 1.37 es la equivalencia lógica o doble implicación, es decir, la relación "si, y sólo si". La denotaremos por $\Leftrightarrow$. Los elementos del conjunto cociente $P/\Leftrightarrow$ son los subconjuntos de P compuestos por afirmaciones lógicamente equivalentes entre sí.

EJERCICIO 15. En el conjunto $\mathbb{N} \times \mathbb{N}_+$ definimos la relación $\propto$ dada para $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}_+$ por $(a, b) \propto (c, d)$ si $ad \leq bc$. Demostrar que $\propto$ es un preorden. La relación de equivalencia dada por este pre-orden no es sino la del Ejercicio 14. Observar que el orden en el conjunto cociente correspondiente coincide con el orden entre fracciones que nos enseñaron en el cole.

1.4. Aplicaciones

Antes que nada, digamos que una aplicación (o función) no es sino un tipo especial de correspondencia, que quiere capturar la idea de transformación, dada sin ambigüedad, de un conjunto a otro.

Noción de aplicación.

DEFINICIÓN 1.39. Una *aplicación* de un conjunto X a un conjunto Y es una correspondencia $f \subseteq X \times Y$ tal que para todo $x \in X$ existe un único $y \in Y$ satisfaciendo que $(x, y) \in f$. Escribiremos $y = f(x)$, en lugar de la notación general xfy, y diremos que y es la *imagen* de x por (o bajo) f. También diremos que f *asigna* y a x

La notación casi universalmente aceptada para denotar una aplicación es escribir $f : X \to Y$, o su variante $X \xrightarrow{f} Y$. El conjunto X es denominado *dominio* de f, en tanto que Y se denomina *codominio* de f. Vamos a distinguir el codominio de f de la *imagen* de f, definida como

$$\mathrm{Im}(f) = \{f(x) \mid x \in X\}.$$

En algunos textos se usa la palabra "función" como sinónimo de "aplicación".

EJEMPLO 1.40. La correspondencia identidad id_X para cualquier conjunto X es una aplicación. En este contexto, escribimos $id_X : X \to X$, que viene definida por $id_X(x) = x$ para todo $x \in X$.

EJERCICIO 16. Sea X un conjunto. ¿Cuántas aplicaciones hay de $\emptyset$ a X? ¿Cuántas aplicaciones hay de X a $\emptyset$?

DEFINICIÓN 1.41. Una aplicación $f : X \to Y$ se dice *inyectiva* si para todo $x, x' \in X$ la condición $f(x) = f(x')$ implica $x = x'$. La aplicación f se llama *sobreyectiva* si para todo $y \in Y$ existe $x \in X$ tal que $y = f(x)$. Observemos que f es sobreyectiva si, y sólo si, $\mathrm{Im}(f) = Y$.

Observemos que si X es un subconjunto de Y, la propia inclusión $X \subseteq Y$ puede entenderse como una aplicación inyectiva.

EJERCICIO 17. Poner un ejemplo de aplicación inyectiva que no sea sobreyectiva, y otro de aplicación sobreyectiva que no sea inyectiva.

EJEMPLO 1.42. Sea X el conjunto de los círculos en el plano. Se tiene la aplicación $f : X \to \mathbb{R}$ que asigna a cada círculo la longitud de su radio. ¿Quién es $\mathrm{Im}(f)$?

EJEMPLO 1.43. Sea $\triangle$ el conjunto de los triángulos en el plano. Se tiene la aplicación $f : \triangle \to \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ que asigna a cada triángulo la terna (α, β, γ) de sus ángulos, medidos en grados sexagesimales, ordenados de menor a mayor, es decir, $\alpha \leq \beta \leq \gamma$. ¿Quién es $\mathrm{Im}(f)$?.

Composición y biyecciones. Una propiedad fundamental de las aplicaciones es que se pueden componer, siempre que sus co-dominios y dominios casen bien, como especifica la siguiente definición.

DEFINICIÓN 1.44. Dadas aplicaciones

$$X \xrightarrow{f} Y \xrightarrow{g} Z,$$

definimos su *composición*

$$X \xrightarrow{g \circ f} Z$$

por la regla $(g \circ f)(x) = g(f(x))$ para todo $x \in X$.

Hagamos algunas observaciones sobre la notación. Es muy usual abreviar $g \circ f$ como gf, cuando el contexto lo permite. Aceptaremos, así, las siguiente notación abreviada:

$$(g \circ f)(x) = gf(x), \qquad (x \in X).$$

EJERCICIO 18. Poner un ejemplo que demuestre que la composición de dos aplicaciones no siempre es posible.

Si $f : X \to Y$ es una aplicación y $Z \subseteq X$ es un subconjunto, entonces podemos considerar la *restricción* de f a Z, denotada por $f_{|Z} : Z \to Y$ y dada por $f_{|Z}(z) = f(z)$ para todo $z \in Z$. Esta restricción puede concebirse como la composición de la aplicación dada por la inclusión $Z \subseteq X$ y la propia f.

PROPOSICIÓN 1.45. *Sean* $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$ *aplicaciones. Entonces* $(h \circ g) \circ f = h \circ (g \circ f)$.

DEMOSTRACIÓN. Se deja como ejercicio. $\square$

DEFINICIÓN 1.46. Una aplicación se dice *biyectiva* si es inyectiva y sobreyectiva.

PROPOSICIÓN 1.47. *Una aplicación* $f : X \to Y$ *es biyectiva si, y sólo si, existe una aplicación* $g : Y \to X$ *tal que* $g \circ f = id_X$ *y* $f \circ g = id_Y$.

DEMOSTRACIÓN. Expondremos una demostración por “doble implicación”. Así, supongamos primero que $f : X \to Y$ es biyectiva y demostramos que entonces existe g en las condiciones descritas. Para ello, definimos una correspondencia de Y a X por

$$g = \{(y, x) \in Y \times X \mid y = f(x)\}.$$

Veamos que g es una aplicación. Dado $y \in Y$, por ser f sobreyectiva, existe $x \in X$ tal que $y = f(x)$. Así que $(y, x) \in g$. Si $x' \in X$ es tal que $(y, x') \in g$, entonces $f(x) = y = f(x')$. Como f es inyectiva, $x = x'$. Hemos probado que g es una aplicación de Y a X según la Definición 1.39.

Ahora, si $y \in Y$, tengo que, por definición, $g(y) = x$ para $x \in X$ tal que $f(x) = y$ Así, $f(g(y)) = f(x) = y$. Esto demuestra que $f \circ g = id_Y$.

Si $x \in X$, entonces $g(f(x)) = z$ para $z \in X$ tal que $f(z) = f(x)$. Al ser f inyectiva, $z = x$. Esto demuestra que $g \circ f = id_X$. Esto acaba la prueba de la implicación “directa”.

Para razonar la implicación “recíproca” o “inversa”, supongamos dada $g : Y \to X$ tal que $g \circ f = id_X$ y $f \circ g = id_Y$. Puesto que, para $y \in Y$, tenemos que $f(g(y)) = y$, deducimos que f es sobreyectiva.

Por último, si $x, x' \in X$ son tales que $f(x) = f(x')$ entonces, aplicando g, obtenemos $x = g(f(x)) = g(f(x')) = x'$. Así, f es inyectiva y hemos terminado la demostración. □

OBSERVACIÓN 1.48. Dada una aplicación biyectiva (o biyección) $f : X \to Y$, la aplicación $g : Y \to X$ proporcionada por la Proposición 1.47 está determinada de manera única por f. En efecto, si $g, h : Y \to X$ verifican $g \circ f = id_X = h \circ f$ y $f \circ g = id_Y = f \circ h$, entonces, usando la Proposición 1.45, obtenemos

$$h = id_X \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ id_Y = g.$$

DEFINICIÓN 1.49. La aplicación $g : Y \to X$ dada por la Proposición 1.47 para una aplicación biyectiva $f : X \to Y$ se llama *recíproca* o *inversa* de f, y se denota por $g = f^{-1}$ (ver la Observación 1.48) . Advertimos que la palabra “inversa”se usa en Cálculo también para otro tipo de funciones (las inversas multiplicativas), y nada tiene que ver con lo definido aquí.

COROLARIO 1.50. *Si* $f : X \to Y$ *es una biyección, entonces* $f^{-1} : Y \to X$ *es una biyección y* $(f^{-1})^{-1} = f$.

DEMOSTRACIÓN. Las ecuaciones

$$f \circ f^{-1} = id_Y, f^{-1} \circ f = id_X,$$

miradas a la luz de la Proposición 1.47 desde la perspectiva de f^{-1}, indican que ésta es una biyección. Por otra parte, como la inversa de una biyección es única según la Observación 1.48, de nuevo las ecuaciones anteriores implican que $(f^{-1})^{-1} = f$. □

Particiones. Descomposición canónica de una aplicación. Queremos explicar una forma alternativa de ver una relación de equivalencia, a través de la noción de partición.

DEFINICIÓN 1.51. Sea X un conjunto no vacío. Una *partición de* X es un subconjunto $\Gamma \subseteq \mathcal{P}(X)$ tal que

1. $\emptyset \notin \Gamma$.
2. $X = \bigcup_{Y \in \Gamma} Y$.
3. $Y \cap Z = \emptyset$ para todo $Y, Z \in \Gamma$ con $Y \neq Z$.

EJERCICIO 19. Sea $X = \{1, 2, 3\}$. Calcular todas las particiones de X.

Cada relación de equivalencia en X da una partición de X, a saber, el conjunto cociente X/R. Enunciemos esto explícitamente.

PROPOSICIÓN 1.52. *Dada una relación de equivalencia* R *en un conjunto no vacío* X*, consideremos la aplicación* $p_R : X \to \mathcal{P}(X)$ *definida por* $p_R(x) = [x]_R$ *para todo* $x \in X$*. Entonces* $\mathrm{Im}(p_R) = X/R$ *es una partición de* X*.*

DEMOSTRACIÓN. Ninguna clase de equivalencia es vacía, por tanto, $\emptyset \notin X/R$. Dado $x \in X$, tenemos que $x \in [x]_R = p_R(x) \in \mathrm{Im}(p_R)$. Esto garantiza la condición 2 en la Definición 1.51. Supongamos ahora $\mathcal{C}, \mathcal{D} \in \mathrm{Im}(p_R)$ con $\mathcal{C} \neq \mathcal{D}$. Por definición, existen $x, y \in X$ tales que $\mathcal{C} = p_R(x) = [x]_R$, $\mathcal{D} = p_R(y) = [y]_R$. En virtud de la Proposición 1.34, $\emptyset = [x]_R \cap [y]_R = \mathcal{C} \cap \mathcal{D}$. □

La aplicación "co-restricción" de p_R, que sólo cambia el codominio por su imagen, se llama *proyección canónica*. Denotaremos a ésta por

$$\pi_R : X \to X/R,$$

definida, pues, por $\pi_R(x) = [x]_R$ para $x \in X$.

Hemos visto que una relación de equivalencia da una partición. Veamos que cada partición da una relación de equivalencia. Hagamos primero una definición más general.

DEFINICIÓN 1.53. Sea $f : X \to Z$ una aplicación. Definimos en X la relación $\sim_f$ dada por $x \sim_f y$ si $f(x) = f(y)$, para $x, y \in X$. Es muy fácil ver que $\sim_f$ es de equivalencia, y se llama *relación de equivalencia determinada por* f.

DEFINICIÓN 1.54. Dada una partición Γ de X, definimos la aplicación $p^\Gamma : X \to \Gamma$ que asigna a $x \in X$ el único $Y \in \Gamma$ tal que $x \in Y$. La relación $\sim_{p^\Gamma}$ es de equivalencia y se llama *relación de equivalencia definida por* Γ, y la denotaremos por $\sim^\Gamma$. Observemos que, para $x, y \in X$, $x \sim^\Gamma y$ si, y sólo si, existe $Y \in \Gamma$ tal que $x, y \in Y$.

La siguiente proposición muestra que dar una relación de equivalencia en un conjunto contiene la misma información que dar una partición.

PROPOSICIÓN 1.55. *Sea* X *un conjunto no vacío. Dada una partición* Γ *de* X*, tenemos que* $X/{\sim^\Gamma} = \Gamma$*. Dada una relación de equivalencia* R *en* X *tenemos que* $\sim^{X/R} = R$.

DEMOSTRACIÓN. Ejercicio. □

Concluimos esta sección con la llamada descomposición canónica de una aplicación.

PROPOSICIÓN 1.56. *Sea* $f : X \to Y$ *una aplicación. Denotemos por*

$$p : X \to X/{\sim_f}$$

la proyección canónica, y por

$$i : \mathrm{Im}(f) \to Y$$

la aplicación dada por la inclusión. Existe una única aplicación

$$X/{\sim_f} \xrightarrow{\widetilde{f}} \mathrm{Im}(f)$$

tal que $f = i \circ \widetilde{f} \circ p$*. Dicha aplicación* $\widetilde{f}$ *es biyectiva.*

DEMOSTRACIÓN. Demostraremos primero la unicidad mediante la siguiente estrategia: supondremos que tenemos $g : X/{\sim_f} \to \mathrm{Im}(f)$ tal que $f = i \circ g \circ p$, y demostraremos que g sólo tiene una definición posible. De hecho, dada una clase de equivalencia $[x]_{\sim_f}$ con representante $x \in X$, tenemos que

$$g([x]_{\sim_f}) = g(p(x)) = i(g(p(x)) = (i \circ g \circ p)(x) = f(x).$$

Observemos que la segunda igualdad viene garantizada porque $g(p(x)) \in \mathrm{Im}(f)$. Así que hemos demostrado que la única definición posible de $\widetilde{f}$ es

$$\widetilde{f}([x]_{\sim_f}) = f(x),$$

para $[x]_{\sim_f} \in X/{\sim_f}$. Comprobemos que esta definición es consistente, es decir, que si $[x]_{\sim_f} = [x']_{\sim_f}$ para ciertos $x, x' \in X$, entonces $\widetilde{f}([x]_{\sim_f}) = \widetilde{f}([x']_{\sim_f})$. En efecto,

$$\widetilde{f}([x]_{\sim_f}) = f(x) = f(x') = \widetilde{f}([x']_{\sim_f}),$$

donde la segunda igualdad se da porque $x \sim_f x'$.

Que $\widetilde{f}$ satisface la ecuación $f = i \circ \widetilde{f} \circ p$ es también una consecuencia casi inmediata de las definiciones involucradas, así como el hecho de que $\widetilde{f}$ es inyectiva y sobreyectiva. □

EJEMPLO 1.57. Consideremos la aplicación del Ejercicio 1.43. La aplicación $\widetilde{f} : \triangle/\sim_f \to \mathrm{Im}(f)$ expresa de manera sintética el hecho de que cada terna (α, β, γ) de números reales tales $0 < \alpha \leq \beta \leq \gamma < 180$ y $\alpha + \beta + \gamma = 180$ determina una única clase de triángulos en el plano semejantes entre sí. Aquí, estamos usando el hecho de que dos triángulos son semejantes si, y sólo si, tienen ángulos iguales.

EJERCICIO 20. Dada una aplicación cualquiera $f : X \to Y$, definimos $f_* : \mathcal{P}(X) \to \mathcal{P}(Y)$ por

$$f_*(A) = \{f(a) : a \in A\}, \qquad \text{para } A \in \mathcal{P}(X).$$

También podemos definir $f^* : \mathcal{P}(Y) \to \mathcal{P}(X)$ por

$$f^*(B) = \{a \in X \mid f(a) \in B\}, \qquad \text{para } B \in \mathcal{P}(Y).$$

Sean $X_1, X_2 \in \mathcal{P}(X), Y_1, Y_2 \in \mathcal{P}(Y)$. Demostrar que

1. Si $X_1 \subseteq X_2$, entonces $f_*(X_1) \subseteq f_*(X_2)$.
2. Si $Y_1 \subseteq Y_2$, entonces $f^*(Y_1) \subseteq f^*(Y_2)$.
3. $f_*(X_1 \cup X_2) = f_*(X_1) \cup f_*(X_2)$.
4. $f^*(Y_1 \cup Y_2) = f^*(Y_1) \cup f^*(Y_2)$.
5. $f_*(X_1 \cap X_2) \subseteq f_*(X_1) \cap f_*(X_2)$.
6. $f^*(Y_1 \cap Y_2) = f^*(Y_1) \cap f^*(Y_2)$.
7. $X_1 \subseteq f^*(f_*(X_1))$.
8. $f_*(f^*(Y_1)) \subseteq Y_1$.

EJERCICIO 21. Demostrar que una aplicación $f : X \to Y$ es sobreyectiva si, y sólo si, existe $g : Y \to X$ tal que $f \circ g = id_Y$.

EJERCICIO 22. Demostrar que una aplicación $f : X \to Y$ es inyectiva si, y sólo si, existe $g : Y \to X$ tal que $g \circ f = id_X$.

EJERCICIO 23. Sea X un conjunto no vacío e $Y \in \mathcal{P}(X)$. Definimos la aplicación $f : X \to \mathcal{P}(X)$ por $f(x) = Y \cup \{x\}$, para $x \in X$, y consideramos la la relación de equivalencia $\sim_f$ asociada a f (según la Definición 1.53). Describir el conjunto cociente $X/\sim_f$. Si X es finito y tiene n elementos e Y tiene m elementos, calcular el cardinal (o sea, el número de elementos) de $X/\sim_f$.

1.5. Monoides. Los números naturales

Hemos admitido que conocemos el conjunto $\mathbb{N} = \{0, 1, 2, \dots\}$ de los números naturales. Sus elementos, que son los números "que sirven para contar", podrían construirse formalmente a partir de las reglas que nos hemos dado, y también podríamos definir a partir de esa construcción las operaciones usuales de suma y producto de números naturales, pero esto nos llevaría un tiempo del que no disponemos. Nos limitamos, pues, a aceptar que, de acuerdo con nuestras reglas, estamos diciendo que, si nos presentan un objeto, sabemos decir si dicho objeto pertenece a $\mathbb{N}$ o no... Nada menos.

La primera observación que hemos de hacer es que los elementos de $\mathbb{N}$ no se pueden listar explícitamente, porque su cantidad es infinita. Una manera de entender esto es aceptar que para cada $n \in \mathbb{N}$, existe un "siguiente", a saber, $n + 1$.

Operaciones binarias, semigrupos y monoides. Tal y como lo hemos expresado, estamos aceptando que sabemos sumar números naturales. Podemos expresar esto en lenguaje de conjuntos diciendo que conocemos una aplicación

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N},$$

llamada "suma". Como es usual, dado $(n, m) \in \mathbb{N}$, su imagen por $+$ se denotará como $n + m$.

Vamos a aprovechar el modelo de la suma de números naturales para dar la noción de operación binaria.

DEFINICIÓN 1.58. Sea X un conjunto no vacío. Toda aplicación

$$\bullet : X \times X \to X$$

se llamará *operación binaria interna* en X. Eludiremos el adjetivo "interna" en lo que sigue.

Las propiedades de las operaciones binarias de las que nos vamos a ocupar, en un contexto asociativo, requieren, para su manejo, de una simplificación en la notación general que usamos para las aplicaciones. Concretamente, si $\bullet : X \times X \to X$ es una operación binaria, entonces, dado $(a, b) \in X \times X$, su imagen por $\bullet$ habría de ser denotada por $\bullet((a, b))$.

Una primera simplificación, en la que no perdemos información, es prescindir de dos paréntesis, y escribir $\bullet(a, b)$ en lugar $\bullet((a, b))$. Pero, ya puestos, podemos suprimir, sin menguar la información, los paréntesis e incluso la coma, y escribir $a \bullet b$ en lugar de $\bullet((a, b))$. Eso sí, tenemos que tener cuidado de no confundir esta notación abreviada con la que se usa en las correspondencias... pero esto estará claro por el contexto en cada caso. Usar notaciones ambiguas sin caer en ambigüedad es una de las características más notables de la Matemática.

En fin, podemos definir ahora lo que es un semigrupo con comodidad.

DEFINICIÓN 1.59. Un *semigrupo* es un par $(S, \bullet)$, donde S es un conjunto no vacío y $\bullet : S \times S \to S$ es una aplicación (una operación binaria) tal que

$$s \bullet (t \bullet u) = (s \bullet t) \bullet u, \qquad \text{para todo } s, t, u \in S. \tag{1.1}$$

La propiedad (1.1) se llama *propiedad asociativa*.

DEFINICIÓN 1.60. Un semigrupo $(S, \bullet)$ es un *monoide* si existe un *elemento neutro* para $\bullet$, esto es, existe $e \in S$ tal que $e \bullet a = a = a \bullet e$ para todo $a \in S$. Diremos que $(S, \bullet, e)$ es un monoide.

EJEMPLO 1.61. Dado un conjunto no vacío X, denotamos por $\mathrm{Map}(X, X)$ al conjunto de todas las aplicaciones de X a X. Es claro que

$$(\mathrm{Map}(X, X), \circ, \mathrm{id}_X)$$

es un monoide.

EJERCICIO 24. Demostrar que, en un monoide, el elemento neutro es único.

DEFINICIÓN 1.62. Un semigrupo $(S, \bullet)$ se dice *conmutativo* si $a \bullet b = b \bullet a$ para todo $a, b \in S$.

EJEMPLO 1.63. $(\mathbb{N}, +, 0)$ es un monoide conmutativo.

Si denotamos por $\cdot$ el producto de $\mathbb{N}$, tenemos:

EJEMPLO 1.64. $(\mathbb{N}, \cdot, 1)$ es un monoide conmutativo. Usaremos la extendida costumbre de denotar el producto $a \cdot b$ de dos números naturales a, b, cuando el contexto lo permita, mediante yuxtaposición, esto es, $ab = a \cdot b$.

EJERCICIO 25. Demostrar que en el conjunto cociente $\mathbb{Q}_+$ definido en el Ejercicio 14 existe una operación suma que verifica que

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

para todo $a/b, c/d \in \mathbb{Q}_+$. Comprobar que, con esta operación, $\mathbb{Q}_+$ es un monoide conmutativo.

EJERCICIO 26. Demostrar que en el conjunto cociente $\mathbb{Q}_+$ definido en el Ejercicio 14 existe una operación producto que verifica que

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

para todo $a/b, c/d \in \mathbb{Q}_+$. Comprobar que, con esta operación, $\mathbb{Q}_+$ es un monoide conmutativo.

Hay muchos ejemplos de monoides conmutativos, aquí van dos más.

EJEMPLO 1.65. Dado X un conjunto, $(\mathcal{P}(X), \cup, \emptyset)$ y $(\mathcal{P}(X), \cap, X)$ son monoides conmutativos.

Hechos fundamentales sobre los números naturales. Volvamos con los números naturales. Es difícil poner un límite sobre qué podemos suponer conocido o qué no sobre los mismos. Los ejemplos 1.63 y 1.64 son asunciones que estamos haciendo sobre las operaciones básicas de suma y producto de números naturales. También podemos aceptar la propiedad distributiva, esto es, la igualdad $(n + m)k = nk + mk$ para todo $n, m, k \in \mathbb{N}$. Y que los elementos de $\mathbb{N}$ se pueden ordenar en el sentido usual, es decir $n < m$ si existe $k \in \mathbb{N} \setminus \{0\}$, tal que $m = n + k$. Todas estos hechos nos parecen bastante obvias. Vamos a aceptar también una propiedad que, para algunas personas, puede no parecer tan obvia.

1.66. **Principio de inducción.** *Sea* $X \subseteq \mathbb{N}$ *tal que* $0 \in X$ *y disfruta de la propiedad de que siempre que* $n \in X$ *entonces* $n + 1 \in X$*. Entonces* $X = \mathbb{N}$.

El siguiente es un ejemplo tradicional de cómo se usa el principio de inducción en una demostración.

EJEMPLO 1.67. Sea n un número natural, entonces

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{1.2}$$

Vamos a hacer una demostración “por inducción”. Primero, tomemos

$$X = \{n \in \mathbb{N} \mid n \text{ satisface (1.2)}\}.$$

Claramente, $0 \in X$. Ahora, dado $n \in X$ tenemos que

$$0+1+\cdots+n+(n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Por tanto, $n + 1 \in X$ y, por el principio de inducción, $X = \mathbb{N}$.

El siguiente ejemplo de uso del principio de inducción es tan importante que lo hemos elevado a la categoría de teorema.

TEOREMA 1.68 (Buena ordenación de los naturales). *Todo conjunto no vacío de números naturales tiene mínimo*[10]*. Esto es, si* $X \subseteq \mathbb{N}$ *verifica que* $X \neq \emptyset$*, entonces existe* $m \in X$ *tal que* $m \leq x$ *para todo* $x \in X$*.*

DEMOSTRACIÓN. Vamos a hacer una demostración por reducción al absurdo, esto es, supondremos que lo afirmado en el enunciado es falso, y llegaremos a una contradicción flagrante, todo ello mediante el uso de un razonamiento correcto, claro.

La idea subyacente a una demostración por reducción al absurdo es que, si añadimos a una serie de enunciados verdaderos un enunciado nuevo que lleva a deducir un enunciado falso, es porque el enunciado añadido es falso.

Vayamos con esta demostración. Tomemos

$$U = \{m \in \mathbb{N} \mid m \leq x \ \forall x \in X\}.$$

Demostremos que, si X no tiene mínimo, entonces $U = \mathbb{N}$. Usamos el principio de inducción.

Que $0 \in U$ es claro, ya que, de hecho, $0 \leq n$ para todo $n \in \mathbb{N}$. Ahora, dado $m \in U$ tenemos que, para todo $x \in X$, $x \geq m$. Pero $m \notin X$ (ya que hemos supuesto que X no tiene mínimo), luego $x > m$ para todo $x \in X$. Por tanto, $x \geq m+1$ para todo $x \in X$. Hemos demostrado, pues, que $m+1 \in U$. Así que, por el principio de inducción, $U = \mathbb{N}$.

Llegamos a la siguiente contradicción: dado que $X \neq \emptyset$, existe algún $x \in X$. Como $x+1 \in \mathbb{N} = U$, deducimos que $x \geq x+1$, lo que es falso. □

Infinidad de los números primos. Un número natural n es *primo* si $n \neq 1$ y sólo admite como divisores 1 y n. Con esta definición, 0 no es primo.

Un número natural distinto de $0, 1$ es *compuesto* si no es primo. El número 1 ni es primo ni es compuesto, y lo mismo para el 0.

Euclides demostró hace 2.300 años que existe una cantidad infinita de números primos. Vamos a dar la demostración de Euclides en términos modernos, claro. Como es típico en matemáticas, parte del argumento de desgajará en dos lemas previos, que son de interés independiente.

LEMA 1.69. *Todo número natural distinto de* 0 *y* 1 *tiene al menos un divisor primo.*

DEMOSTRACIÓN. Sea $n \in \mathbb{N}$, con $n \neq 0, 1$. Tomemos el conjunto

$$X = \{m \in \mathbb{N} \mid m \neq 1 \text{ y } m \text{ divide a } n\},$$

que es no vacío, ya que $n \in X$. Sea p el mínimo de X, que existe en virtud del Teorema 1.68. Veamos que p es primo. Si $p = qr$, con $q, r \neq 1$, entonces $q \in X$ y $q < p$. Esto contradice que p es el mínimo de X. Por tanto, p es primo. □

LEMA 1.70. *Sean* $a, b, c \in \mathbb{N}$ *tales que* $a = b + c$*. Si* $0 \neq d \in \mathbb{N}$ *es tal que divide a dos de los elementos de* $\{a, b, c\}$*, entonces los divide a todos.*

DEMOSTRACIÓN. Hay dos casos esencialmente distintos. El primero es que d sea divisor de b y c. Entonces $b = db', c = dc'$ para $b', c' \in \mathbb{N}$ adecuados. Así, $a = db' + dc' = d(b' + c')$, luego d es un divisor de a.

El otro caso se da cuando d es divisor de a y b. De nuevo, existen $a', b' \in \mathbb{N}$ tales que $a = da', b = db'$. Por tanto, $da' = db' + c \geq db'$. Así que

[10] con respecto del orden natural, claro

$a' \geq b'$, lo que significa que existe $k \in \mathbb{N}$ tal que $a' = b' + k$. Pero esto da $db' + dk = db' + c$, de donde $dk = c$. Por tanto, d divide a c. $\square$

TEOREMA 1.71. *Existe una cantidad infinita de números primos.*

DEMOSTRACIÓN. Haremos esta demostración por reducción al absurdo. Así, supongamos que hubiese una cantidad finita de números primos, digamos que son $p_1, \dots, p_n$. Formemos el número $N = p_1 \cdots p_n + 1$. Observemos que $N \neq 0, 1$, luego, de acuerdo con el Lemma 1.69, N tiene un divisor primo p. Dicho divisor estará la lista completa anterior, luego también es un divisor de $p_1 \cdots p_n$. Por el Lema 1.70, p es un divisor de 1. Esta contradicción demuestra que $p_1, \dots, p_n$ no puede ser una lista completa de todos los números primos. Luego hay infinitos. $\square$

El Teorema Fundamental de la Aritmética. El siguiente lema aparece enunciado en los Elementos de Euclides. En Teoría de Números se suele llamar *Lema de Euclides*.

LEMA 1.72 (Euclides). *Sea p un número primo, y $a, b \in \mathbb{N}$. Si p divide a ab, entonces p divide a a o bien p divide a b.*

DEMOSTRACIÓN. Diremos que $x \in \mathbb{N}$ satisface la propiedad $P(x)$ si dada cualquier factorización $x = ab$ con $a, b \in \mathbb{N}$ el hecho de que un número primo p divida a ab implica que divide al menos a uno de los factores a o b. Definamos el siguiente conjunto

$$X = \{n \in \mathbb{N} \mid \text{ se satisface } P(x) \text{ para todo } x \leq n\}.$$

Queremos demostrar que $X = \mathbb{N}$. Que $0 \in X$ y, por tanto, X es no vacío, es fácil de ver usando que $ab = 0$ para $a, b \in \mathbb{N}$ implica que $a = 0$ o bien $b = 0$.

Supongamos ahora $n \in X$. Hemos de demostrar que $n + 1 \in X$ para completar la inducción.

En el caso de que $n = 0$, tendremos que comprobar que $1 \in X$. Pero esto es obvio, ya que si $1 = ab$, entonces $a = b = 1$.

Discutamos ahora el caso $n \neq 0$. De este modo, $n + 1 \geq 2$. Tomamos $x \leq n + 1$. Si $x < n + 1$, entonces $x \leq n$ y satisface $P(x)$ por hipótesis de inducción (ya que $n \in X$). Nos concentramos, pues, en el caso $x = n + 1$. Dados a, b naturales tales que $n + 1 = ab$ y un primo p que divide a ab razonamos como sigue. Queremos demostrar que p divide a a o bien p divide a b. Podemos suponer que $a \neq 1$ y $b \neq 1$, para razonar un caso no trivial.

Llegados a este punto, escribamos $ab = pq$, para $q \in \mathbb{N}$ adecuado. Puesto que ab no es primo, $q \neq 1$, ya que p sí lo es. En virtud del Lema 1.69, podemos tomar un divisor primo p' de q. Escribimos, pues, $q = q'p'$ para q' adecuado.

De ser p' un un divisor de a, escribimos $a = a'p'$ y deducimos que

$$a'p'b = pq'p',$$

de donde $a'b = pq'$. Así, p es un divisor de $a'b < ab$. Por hipótesis de inducción, p divide a a' (y, por tanto, a a) o bien p divide a b. Análogamente se razona si p' es un divisor de b.

Veamos, por último, que admitir que p' no es divisor ni de a ni de b, lleva a una contradicción. Ciertamente, tenemos que $p' < a$ o bien $p' < b$. Bastará con discutir el primer caso. Tomamos k natural no nulo tal que $a = p' + k$. Tenemos que $(p' + k)b = ab = p'q'p$ Por el Lema 1.70, p' divide a kb. Como $kb < ab = n + 1$, podemos usar inducción para deducir que p' divide a k o bien p' divide a b. El segundo caso está descartado por hipótesis. Del primero deducimos, de nuevo por el Lema 1.70, que p' divide a a. Contradicción. □

El Teorema 1.75 tiene como consecuencia la existencia de números irracionales, que, según la leyenda, inquietó mucho a los pitagóricos.

TEOREMA 1.73. *Si* p *es un número natural primo, entonces no existe ningún número racional* r *tal que* $r^2 = p$.

DEMOSTRACIÓN. Supongamos, razonando por reducción al absurdo, que $r^2 = p$ para un racional r. Podemos escribir $r = a/b$, para a mínimo entre los posibles numeradores de todas las fracciones equivalentes. Entonces a y b no tienen ningún divisor primo común. Esto es porque, de tener a y b un divisor común, podemos simplificar la fracción para obtener una equivalente a a/b pero con numerador más pequeño.

Tenemos, pues, que $a^2 = b^2p$. Del Lema 1.72 deducimos que p es un divisor de a. Tenemos, pues, que $a = pc$ para cierto $c \in \mathbb{N}$. Pero, así, $p^2c^2 = b^2p$, de donde $pc^2 = b^2$. De nuevo el Lema 1.72 implica que p es un divisor de b. Así que p resulta ser un divisor común de a y b, lo que es una contradicción. □

OBSERVACIÓN 1.74. El Teorema 1.73, junto con el Teorema 1.71, muestra que existen infinitos números irracionales, ya que la raíz cuadrada de cualquier número primo no es racional.

Nuestro próximo objetivo es demostrar el llamado Teorema Fundamental de la Aritmética.

TEOREMA 1.75 (Fundamental de la Aritmética). *Todo número natural distinto de* 0 *y* 1 *es producto de números primos. Esta factorización es única salvo reordenación de los factores primos.*

DEMOSTRACIÓN. Supongamos que el conjunto

$$X = \{n \in \mathbb{N} \mid n \geq 2 \text{ y } n \text{ no es producto de primos }\}$$

fuese no vacío. Entonces tendría un mínimo, digamos m. Por el Lema 1.69, m tiene un divisor primo, digamos p. Así, $m = ap$ para cierto $a \in \mathbb{N}$. Como $m \neq 0$, tenemos que $a \neq 0$. Ahora, $a \neq 1$ ya que, de lo contrario, m sería primo. Por tanto $a \neq 0, 1$. Como $a < m$, tenemos que admitir que $a \notin X$, luego a es un producto de primos. Pero, claro, $m = ap$ es entonces un producto de primos. Así que, en cualquier caso, $m \notin X$, lo que es una contradicción. Por tanto, X es vacío, y todo número natural distinto de 0 y 1 es producto de números primos.

Para ver la unicidad, supongamos que existe un número natural con dos factorizaciones distintas, y tomemos n mínimo con esta propiedad. Así, tendremos dos factorizaciones distintas $n = p_1 \cdots p_r = q_1 \cdots q_s$, para $p_1, \ldots, p_r, q_1, \ldots, q_s$ primos. Por aplicación reiterada del Lema 1.72, p_1 ha de ser divisor de algún q_j, para algún j. Al ser éste primo, $p_1 = q_j$. Reordenando los factores q_j, podemos suponer que $j = 1$, esto es, $p_1 = q_1$. Deducimos así que $p_2 \cdots p_r = q_2 \cdots q_s$. Pero este número es estrictamente menor que n, por lo que su factorización en primos es única. Así que $r = s$ y, tras reordenación, $p_i = q_i$ para $i = 2, \ldots, r$. Pero, de esta forma, hemos visto que las factorizaciones distintas de n son la misma. Contradicción. □

EJERCICIO 27. Si un número natural no es el cuadrado de ningún otro número natural, entonces no es el cuadrado de ningún número racional.

División Euclidiana. Aquí va otro teorema que aparece en los Elementos de Euclides.

TEOREMA 1.76 (División Euclidiana de números naturales). *Dados* $a, b \in \mathbb{N}$ *con* $b \neq 0$, *existen* $q, r \in \mathbb{N}$ *tales que* $r < b$ *y* $a = qb + r$.

DEMOSTRACIÓN. Esta demostración también la haremos por inducción. Por conveniencia, dado $0 \neq b \in \mathbb{N}$, diremos que $a \in \mathbb{N}$ admite una división con resto entre b si existen $q, r \in \mathbb{N}$ con $r < b$ y $a = qb + r$.

Dado $b \neq 0$, consideremos el conjunto

$$X = \{n \in \mathbb{N} \mid \forall a \in \mathbb{N} \text{ con } a \leq n, a \text{ admite una división con resto entre } b\}.$$

Obviamente, $0 \in X$, ya que $0 = 0b + 0$. Supongamos que $n \in X$. Tomemos $a \leq n + 1$. Pueden darse dos casos.

Si $a < b$, entonces $a = 0b + a$, tomando $q = 0$, $r = a$ tenemos la división con resto.

Si $a \geq b$, entonces $a = b + k$ para cierto $k \in \mathbb{N}$. Observemos que $k < a \leq n + 1$. Luego $k \leq n$ y, como $n \in X$, existen $q, r \in \mathbb{N}$ tales que $r < b$ y $k = qb + r$. Para concluir, observemos que

$$a = b + k = b + qb + r = (q + 1)b + r$$

da la división con resto deseada. Por inducción, $X = \mathbb{N}$. □

OBSERVACIÓN 1.77. Es posible demostrar[11] que los números naturales q, r que aparecen en en el Teorema 1.76 están determinados de manera única por a, b. De acuerdo a la tradición, q se llama *cociente* y r se llama *resto* de la división de a entre b. Usaremos la notación

$$q = \mathrm{quot}(a, b), \qquad r = \mathrm{rem}(a, b).$$

OBSERVACIÓN 1.78. Seguro que recordáis cómo se calcula en primaria el máximo común divisor de dos naturales a, b, con $a > b > 0$. Aquí sugiero un método que, lo mismo, no conocéis: Si realizamos una división con resto, tendremos que $a = qb + r$, para $q, r \in \mathbb{N}$ con $r < b$. Según el Lema 1.70, los divisores comunes de a y b son los mismos que los divisores comunes de b y r. ¿Ves cómo aprovechar esto para calcular el máximo común divisor de a y b sin conocer sus factores primos?

EJERCICIO 28. Sea $n \in \mathbb{N}$, $n \neq 0$. Para cada $a \in \mathbb{N}$, escribamos $\mathrm{rem}(a, n)$ para denotar el resto de la división de a entre n. Definimos la relación mod_n en $\mathbb{N}$ por la condición $a \ \mathrm{mod}_n \ b$ si $\mathrm{rem}(a, n) = \mathrm{rem}(b, n)$ para $a, b \in \mathbb{N}$. Demostrar que mod_n una relación de equivalencia. El respeto a la tradición sugiere que escribamos $a \equiv b \pmod n$ para indicar $a \ \mathrm{mod}_n \ b$. Describir el conjunto cociente $\mathbb{N}/\mathrm{mod}_n$.

EJERCICIO 29. En un monoide $(A, *, e)$, podemos definir, para $n \in \mathbb{N}$, y $a \in A$, el elemento a^n como sigue. Para $n = 0$, definimos $a^0 = e$ y, supuesto definido a^m para cierto $m \in \mathbb{N}$, definimos $a^{m+1} = a^m * a$. Demostrar que $a^{k+m} = a^k * a^m$ y $(a^k)^l = a^{kl}$ para todo $k, l \in \mathbb{N}$.

[11] Usando números enteros (positivos y negativos), es bastante fácil. Si sólo nos permitimos, en este momento, números naturales, la demostración es algo más sutil. Puedes intentarlo.

Capítulo 2

Anillos

En este capítulo vamos a introducir dos estructuras fundamentales, la de grupo y la de anillo. Nuestro ejemplo básico será el anillo de los números enteros, del cual se derivarán otros ejemplos básicos como los anillos de clases de congruencia, cuya utilidad quedará clara por su aplicación a la aritmética modular. En capítulos posteriores, tras la construcción de los anillos de polinomios, el catálogo de ejemplos se ampliará considerablemente.

2.1. Nociones de grupo y anillo. El anillo de los enteros.

Ahora nos disponemos a construir formalmente el conjunto $\mathbb{Z}$ de los números enteros a partir de $\mathbb{N}$. Esto es un buen banco de pruebas para afianzar la noción de relación de equivalencia.

Construcción de los enteros. Si $n, m \in \mathbb{N}$ con $m \geq n$, entonces existe un único $k \in \mathbb{N}$ tal que $n + k = m$. Este número k se llama *diferencia* entre m y n. Es universalmente admitido escribir entonces $k = m - n$.

Los números enteros se inventan para dar sentido a la diferencia $n-m$, que, cuando $m > n$, no tiene sentido en $\mathbb{N}$. Estos nuevos números han de contener a los naturales, poseer un orden y operaciones artiméticas (suma y producto) que extiendan a las de $\mathbb{N}$ y que disfruten de propiedades adecuadas.

Vamos a construir el conjunto de los números enteros como aplicación de la Proposición 1.37. Comenzaremos definiendo un pre-orden en $\mathbb{N} \times \mathbb{N}$, que quiere establecer cuándo una diferencia va a ser menor que otra, en términos puramente de números naturales (¡sin signo!).

LEMA 2.1. *Definamos la relación $\propto$ en $\mathbb{N} \times \mathbb{N}$ estableciendo, para*

$$(n, m), (n', m') \in \mathbb{N} \times \mathbb{N},$$

que

$$(n, m) \propto (n'm') \textit{ si } n + m' \leq m + n'.$$

La relación $\propto$ es un pre-orden.

DEMOSTRACIÓN. Se trata de una relación obviamente reflexiva, así que sólo hemos de probar la propiedad transitiva. Tomemos

$$(n, m), (n', m'), (n'', m'') \in \mathbb{N} \times \mathbb{N}$$

tales que

$$(n, m) \propto (n', m') \text{ y } (n', m') \propto (n'', m'').$$

Entonces

$$n + m' \leq m + n' \text{ y } n' + m'' \leq m' + n''.$$

Sumando los miembros al mismo lado de cada desigualdad, obtenemos

$$n + m' + n' + m'' \leq m + n' + m' + n''.$$

De donde[1] $n + m'' \leq m + n''$, esto es, $(n, m) \propto (n'', m'')$. □

Estamos en condiciones de construir los números enteros.

PROPOSICIÓN 2.2. *El conjunto cociente*

$$\mathbb{Z} = \frac{\mathbb{N} \times \mathbb{N}}{R}$$

bajo la relación de equivalencia R *definida por*

$$(n, m)R(n'm') \text{ si } n + m' = m + n',$$

para $(n, m), (n', m') \in \mathbb{N} \times \mathbb{N}$, *está totalmente ordenado por la relación de orden* $\leq$ *definida por*

$$[(n, m)]_R \leq [(n', m')]_R \text{ si } n + m' \leq m + n'.$$

DEMOSTRACIÓN. Se obtiene por aplicación directa de la Proposición 1.37 al pre-orden dado en el Lema 2.1. □

DEFINICIÓN 2.3. El conjunto ordenado $(\mathbb{Z}, \leq)$ definido en la Proposición 2.2 se llama *conjunto de los números enteros*.

OBSERVACIÓN 2.4. Observemos que

$$[(3, 1)]_R = \{(2, 0), (3, 1), (4, 2), \dots\}.$$

Fijémonos en que los elementos de esta clase de equivalencia son todas las formas de obtener 2 como diferencia de dos números naturales. O sea, de alguna forma, $[3, 1]_R$ es el número 2. Lo interesante es que la clase

$$[(1, 3)]_R = \{(0, 2), (1, 3), (2, 4), \dots\}$$

contiene todas las formas de obtener -2 como diferencia de dos números naturales. Es decir, $[1, 3]_R$ es el número negativo -2.

Vamos a ver que el conjunto $\mathbb{N}$ se puede identificar, como conjunto ordenado, con un subconjunto de $\mathbb{Z}$.

PROPOSICIÓN 2.5. *La aplicación* $\iota : \mathbb{N} \to \mathbb{Z}$ *definida por* $\iota(n) = [(n, 0)]_R$ *para todo* $n \in \mathbb{N}$ *es inyectiva. Además, para* $n, m \in \mathbb{N}$*, se tiene que* $n \leq m$ *si, y sólo si,* $\iota(n) \leq \iota(m)$.

DEMOSTRACIÓN. Veamos primero que ι es inyectiva: si $a, b \in \mathbb{N}$ son tales que $\iota(a) = \iota(b)$, entonces $[(a, 0)]_R = [(b, 0)]_R$. Según la Proposición 1.34, $(a, 0)R(b, 0)$, de donde $a + 0 = 0 + b$, esto es, $a = b$.

Supongamos ahora que $m, n \in \mathbb{N}$. Es bastante obvio que $n \leq m$ si, y sólo si, $\iota(n) \leq \iota(m)$. □

La Proposición 2.5 permite ver $\mathbb{N}$ como un subconjunto de $\mathbb{Z}$, de manera que el orden usual de $\mathbb{N}$ se extiende a un orden en $\mathbb{Z}$. El siguiente paso es extender adecuadamente las operaciones suma y producto de $\mathbb{N}$ a $\mathbb{Z}$.

---

[1]Estamos suponiendo que sabemos que si $a, b, c \in \mathbb{N}$ verifican que $a + c \leq b + c$, entonces $a \leq b$. Esto se puede probar a partir de hechos aún más "evidentes" sobre $\mathbb{N}$, **sin necesidad de usar números negativos**, pero no nos vamos a entretener en ello.

Noción de grupo. Los enteros como grupo aditivo. Como veremos, un anillo combina dos estructuras de monoide. Una de ellas disfruta, además, de una propiedad adicional que lo hace un grupo. Como los grupos son objetos fundamentales en Matemáticas, definamos esta noción.

DEFINICIÓN 2.6. Un monoide $(A, *, e)$ es un *grupo* si para cada $a \in A$, existe $\overline{a} \in A$ tal que $a * \overline{a} = e = \overline{a} * a$. El grupo es *conmutativo* si lo es como monoide, esto es, $a * b = b * a$ para todo $a, b \in A$.

EJERCICIO 30. Demostrar que, para un grupo $(A, *, e)$, y cada $a \in A$, el elemento $\overline{a}$ está determinado de manera única por a. El elemento $\overline{a}$ se llama *simétrico* de a.

OBSERVACIÓN 2.7. En muchos contextos, cuando se tiene un grupo conmutativo, se suele usar la llamada "notación aditiva". Esto significa que la operación de monoide se representa por el signo $+$, el elemento neutro por 0 y, para cada a en el grupo, $-a$ denota el elemento simétrico de a, que verifica que $-a + a = 0$. Se suele llamar *opuesto* de a.

Se usará la notación abreviada $a-b$ para $a+(-b)$. Éste va a ser el caso de $\mathbb{Z}$, como veremos más abajo, o de la "suma" en un espacio vectorial, como habréis visto en Álgebra Lineal.

OBSERVACIÓN 2.8. En general, para un grupo cualquiera A, se suele usar la "notación multiplicativa" a^{-1} para denotar el simétrico de $a \in A$. En tal caso, el elemento a^{-1} se llama *inverso* de a. En este contexto, la yuxtaposición ab de dos elementos $a, b \in A$ denota su producto, esto es, $ab = a * b$.

DEFINICIÓN 2.9. Sea $(A, *, e)$ un monoide, y $B \subseteq A$. Diremos que B es un submonoide de A si $e \in B$ y, para cada $b, c \in B$, se tiene que $b * c \in B$. Obsérvese que, en tal caso, la restricción de la operación binaria $*$ a $B \times B$, hace que $(B, *, e)$ sea, a su vez, un monoide.

EJEMPLO 2.10. Dado un conjunto X, consideremos

$$Sym(X) = \{f : X \to X \mid f \text{ biyectiva } \}.$$

Es claro que $(Sym(X), \circ, id_X)$ es un submonoide de $(Map(X, X), \circ, id_X)$. Se deduce de la Proposición 1.47 que $Sym(X)$ es un grupo, llamado *grupo de permutaciones* de X.

TEOREMA 2.11. *Existe un grupo conmutativo* $(\mathbb{Z}, +, 0)$ *que contiene a* $(\mathbb{N}, +, 0)$ *como submonoide de manera que*

$$\mathbb{Z} = -\mathbb{N} \cup \mathbb{N},$$

donde

$$-\mathbb{N} = \{-k \mid k \in \mathbb{N}\}.$$

El grupo $(\mathbb{Z}, +, 0)$ *está totalmente ordenado por la relación* $n \leq m$ *si, y sólo si, existe* $k \in \mathbb{N}$ *tal que* $n + k = m$, *para* $n, m \in \mathbb{Z}$.

DEMOSTRACIÓN. Consideremos la relación de equivalencia R en $\mathbb{N} \times \mathbb{N}$ proporcionada por la Proposición 2.2. El conjunto cociente es

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R.$$

Vamos a usar notación aditiva para la operación de grupo en $\mathbb{Z}$. Definimos, pues, para $[(a, b)]_R, [(c, d)]_R \in \mathbb{Z}$,

$$[(a, b)]_R + [(c, d)]_R = [(a + c, b + d)]_R. \tag{2.1}$$

Hemos de comprobar que esta definición no depende de los representantes de las clases de equivalencia escogidos. Así, supongamos que

$$[(a,b)]_R = [(a',b')]_R \text{ y } [(c,d)]_R = [(c',d')]_R.$$

Usando las propiedades conmutativa y asociativa de la operación $+$ en $\mathbb{N}$, tenemos que

$$(a+c)+(b'+d') = (a+b')+(c+d') = (a'+b)+(c'+d) = (a'+c')+(b+d).$$

Por tanto,

$$(a+c,b+d)R(a'+c',b'+d'),$$

de donde

$$[(a+c,b+d)]_R = [(a'+c',b'+d')]_R.$$

La asociatividad de la nueva operación $+$ se sigue fácilmente de la de $+$ en $\mathbb{N}$. Además, el elemento neutro es, claramente, $0 = [(0,0)]_R$. Tenemos, pues, un monoide $(\mathbb{Z},+,0)$, claramente conmutativo.

Veamos que se trata de un grupo: dado $[(a,b)]_R \in \mathbb{Z}$, tenemos que

$$[(a,b)]_R + [(b,a)]_R = [(a+b,b+a)]_R = [(0,0)]_R = 0.$$

Vamos a representar los elementos de $\mathbb{Z}$ de manera más familiar. La Proposición 2.5 da una aplicación inyectiva $\iota : \mathbb{N} \to \mathbb{Z}$ que permitía identificar $\mathbb{N}$ con

$$\mathrm{Im}(\iota) = \{[(n,0)]_R \mid n \in \mathbb{N}\}$$

como conjunto ordenado. Concretamente, vamos a identificar cada $n \in \mathbb{N}$ con la clase $[(n,0)]_R$.

Vemos fácilmente que, de esta forma, $\mathbb{N}$ resulta ser un submonoide de $\mathbb{Z}$: para $n,m \in \mathbb{N}$, tenemos

$$[(n,0)]_R + [(m,0)]_R = [(n+m,0)]_R.$$

Si ahora escribimos, para $n \in \mathbb{N}$, $-n = [(0,n)]_R$, consideremos

$$-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}.$$

Demostremos que $\mathbb{Z} = -\mathbb{N} \cup \mathbb{N}$. En efecto, dado $[(a,b)]_R \in \mathbb{Z}$, se tiene que, o bien $a \geq b$, o $a \leq b$. En el primer caso, existe $k \in \mathbb{N}$ tal que $a = b+k$, por lo que

$$[(a,b)]_R = [(b+k,b)]_R = [(k,0)]_R = k \in \mathbb{N}.$$

En el segundo, para $k \in \mathbb{N}$ tal que $b = a+k$, tenemos

$$[(a,b)]_R = [(a,a+k)]_R = [(0,k)] = -k \in -\mathbb{N}.$$

Veamos, por último, cómo se caracteriza ahora el orden en $\mathbb{Z}$ que introdujimos en la Proposición 2.5. Recordemos que $[(a,b)]_R \leq [(c,d)]_R$ si, y sólo si, $a+d \leq b+c$. Esto es, existe $k \in \mathbb{N}$ tal que $b+c = k+a+d$. Esta condición es equivalente a decir que

$$[(a,b)]_R + [(k,0)]_R = [(c,d)]_R.$$

Es decir, hemos demostrado que, dados $x,y \in \mathbb{Z}$, $x \leq y$ si, y sólo si, existe $k \in \mathbb{N}$ tal que $x+k = y$. Observemos que no hemos tenido que preocuparnos de los “signos”... explícitamente. □

EJERCICIO 31. Con la notación del Ejercicio 29, supongamos ahora que A es un grupo. Usamos notación multiplicativa en A (ver Observación 2.8). Para $n \in \mathbb{Z}$ con $n < 0$, definimos $a^n = (a^{-1})^{-n}$. Demostrar que $a^{x+y} = a^x a^y$ para todo $x,y \in \mathbb{Z}$.

El Teorema 2.11 es el instrumento que permite, en lo que respecta al orden y la suma, no volver a usar que los elementos de $\mathbb{Z}$ son clases de equivalencia.

Noción de anillo. Los enteros como anillo. Nos proponemos ahora extender la multiplicación de $\mathbb{N}$ a $\mathbb{Z}$ de manera adecuada. Este producto en $\mathbb{Z}$ gozará de unas propiedades que permitirán operar en $\mathbb{Z}$ de manera sencilla. Dichas propiedades son compartidas con otros sistemas algebraicos relevantes, así que merecen una definición abstracta como la que sigue.

DEFINICIÓN 2.12. Un *anillo* es un grupo conmutativo $(A, +, 0)$ dotado además de una estructura de monoide $(A, \cdot, 1)$ tal que se verifica la propiedad distributiva, esto es, para todo $a, b, c \in A$, se tiene que

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

Se usa la notación $(A, +, 0, \cdot, 1)$, pero también diremos simplemente que "A es un anillo". La operación $+$ se suele llamar *suma de* A, en tanto que $\cdot$ es el *producto* o *multiplicación* de A. El elemento 0 se llama *cero de* A, y 1 es el *uno de* A. El anillo es *conmutativo* si $(A, \cdot, 1)$ es un monoide conmutativo.

EJERCICIO 32. Demostrar que, en todo anillo A, se tiene que $a \cdot 0 = 0 = 0 \cdot a$ para todo $a \in A$. Deducir que, en un anillo con al menos dos elementos, $0 \neq 1$.

EJERCICIO 33. Sean $x, y \in A$, donde A es un anillo. Demostrar que $(-x) \cdot y = -x \cdot y = x \cdot (-y)$. Deducir que $(-x) \cdot (-y) = x \cdot y$.

EJERCICIO 34. Sean A, B anillos. En el producto cartesiano $A \times B$ definimos las operaciones

$$(a, b) + (a', b') = (a + a', b + b') \text{ y } (a, b) \cdot (a', b') = (a \cdot a', b \cdot b').$$

Demostrar que, con estas operaciones, $A \times B$ es un anillo, llamado *anillo producto* de A y B.

EJERCICIO 35. Para un anillo A, consideremos en $A \times A$ las siguientes operaciones: $(a, a') + (b, b') = (a + b, a' + b')$ y $(a, a') \cdot (b, b') = (a \cdot b, a \cdot b' + a' \cdot b)$. Demostrar que $A \times A$, con estas operaciones, es un anillo.

TEOREMA 2.13. *El grupo conmutativo $(\mathbb{Z}, +, 0)$ admite una estructura adicional de monoide $(\mathbb{Z}, \cdot, 1)$ que lo hace un anillo conmutativo. El producto $\cdot$ está dado por*

$$[(a, b)]_R \cdot [(c, d)]_R = [(ac + bd, ad + bc)]_R, \qquad ([(a, b)]_R, [(c, d)]_R \in \mathbb{Z}), \tag{2.2}$$

y, por tanto, es una extensión del producto de $\mathbb{N}$.

DEMOSTRACIÓN. Comencemos demostrando que el producto dado en (2.2) está bien definido. Así, supongamos que $(a, b) R (a', b')$ y $(c, d) R (c', d')$. Se tiene entonces que $a + b' = a' + b$ y $c + d' = c' + d$. De estas identidades se obtienen fácilmente las siguientes:

$$\begin{array}{rcl} ac + b'c & = & a'c + bc \\ a'd + bd & = & ad + b'd \\ a'c + a'd' & = & a'c' + a'd \\ b'c' + b'd & = & b'c + b'd' \end{array}$$

Sumando los términos al mismo lado, y cancelando sumandos iguales en la identidad resultante, se obtiene que

$$ac + bd + a'd' + b'c' = ad + bc + a'c' + b'd'.$$

Así, $(ad+bd, ad+bc)R(a'd'+b'd', a'd'+b'c')$, lo que muestra que el producto dado en (2.2) está bien definido.

Claramente, $\cdot$ es conmutativo y extiende al producto en $\mathbb{N}$. La comprobación de las propiedades asociativa y distributiva son cálculos rutinarios que se dejan como ejercicio. Es claro que $1 \in \mathbb{N}$ es neutro para el producto definido en $\mathbb{Z}$. $\square$

OBSERVACIÓN 2.14. En virtud del Teorema 2.11, cada elemento de $\mathbb{Z}$ es de la forma n o $-n$ para algún n. Ahora, el Teorema 2.13, junto con el Ejercicio 33, permite así multiplicar dos números enteros sabiendo multiplicar números naturales, mediante las reglas usuales de manejo de los signos bajo la multiplicación.

¿Cuál es el sentido del Teorema 2.13? Bueno, si no supiéramos que $\mathbb{Z}$ es un anillo, y prefiriéramos definir su producto a partir del de $\mathbb{N}$ con arreglo a las reglas de los signos (como en la escuela elemental, o sea, "más por menos es menos", "menos por menos es más", etcétera), tendríamos que demostrar que se trata de un producto asociativo y distributivo con respecto de la suma. Esto da una cantidad de casos posibles en los signos de los números involucrados en las identidades que comprobar bastante desagradable, aunque, si uno se empeña, puede hacerlo así...

EJERCICIO 36. Con la notación del Ejercicio 31, demostrar que $(a^x)^y = a^{xy}$ para todo $x, y \in \mathbb{Z}$.

OBSERVACIÓN 2.15. Se suele representar el producto de números enteros mediante yuxtaposición. Es decir, si $a, b \in \mathbb{Z}$, entonces escribimos $ab = a \cdot b$. De hecho, esta notación se hace extensiva a cualquier anillo.

Subgrupos de $\mathbb{Z}$. El conocimiento de los subgrupos de $\mathbb{Z}$ proporciona una herramienta fundamental para una aproximación moderna a las aritméticas entera y modular. Como la noción de subgrupo es también relevante en Matemáticas, comencemos con la definición general.

DEFINICIÓN 2.16. Sea $(A, *, e)$ un grupo y $B \subseteq A$ un submonoide. Diremos que B es un *subgrupo* si $(B, *, e)$ es un grupo.

El siguiente ejercicio da una caracterización de subgrupo que, en no pocos textos, se da como definición.

EJERCICIO 37. Sea $(A, *, e)$ un grupo y $B \subseteq A$ un subconjunto no vacío. Demostrar que B es un subgrupo de A si, y sólo si, para todo $b, c \in B$ se tiene que $b * \overline{c} \in B$.

TEOREMA 2.17. *Para cada $n \in \mathbb{N}$, el conjunto $n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$ es un subgrupo de $(\mathbb{Z}, +, 0)$. Todo subgrupo de $(\mathbb{Z}, +, 0)$ es de esa forma.*

DEMOSTRACIÓN. Si $a, b \in n\mathbb{Z}$, entonces $a = nq$, $b = nk$, para ciertos $q, k \in \mathbb{Z}$. Por tanto, $a - b = nq - nk = n(q-k) \in n\mathbb{Z}$. De acuerdo con el Ejercicio 37, $n\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$.

Supongamos, recíprocamente, que I es un subgrupo de $\mathbb{Z}$. Si $I = \{0\}$, entonces, claramente, $I = 0\mathbb{Z}$.

Supongamos que $I \neq \{0\}$. Eso significa que existe $x \in I$ con $x \neq 0$. Como I es subgrupo, tenemos que $-x \in I$. Por el Teorema 2.11, tenemos que, o bien $x \in \mathbb{N}$, o bien $-x \in \mathbb{N}$. Esto es, el conjunto $I \cap \mathbb{N}_+$ es no vacío. Por la buena ordenación de $\mathbb{N}$ (ver Teorema 1.68), podemos tomar el mínimo n de $I \cap \mathbb{N}_+$.

Comencemos razonando que $n\mathbb{Z} \subseteq I$. En efecto, dado $q \in \mathbb{Z}$, hemos de ver que $nq \in I$. Si $q \in \mathbb{N}$, entonces

$$nq = n + \overset{(q)}{\cdots} + n,$$

donde esta notación significa “sumar q veces n.” Como $n \in I$, se deduce de aquí que $nq \in I$. En caso de que $-q \in \mathbb{N}$, tenemos que

$$nq = (-n)(-q) = (-n) + \overset{(-q)}{\cdots} + (-n).$$

Como $-n \in I$, volvemos a obtener que $nq \in I$.

Para demostrar la inclusión $I \subseteq n\mathbb{Z}$, tomemos $a \in I$. Si $a \in \mathbb{N}$, entonces, por la División Euclidiana en $\mathbb{N}$, tenemos que $a = qn + r$ para $q, r \in \mathbb{N}$ con $r < n$. Pero, entonces, $r = a - qn \in I$, lo que implica que $r = 0$, por ser n mínimo entre los números naturales no nulos de I. Esto es, $a = qn \in n\mathbb{Z}$. La otra opción es que $-a \in \mathbb{N}$. Encontramos de nuevo $k, s \in \mathbb{N}$ tales que $-a = kn + s$ y $s < n$. De nuevo, $s = -a - kn \in I$, lo que implica que $s = 0$. Así, $a = -kn \in n\mathbb{Z}$, lo que concluye la demostración. □

Un punto clave de la demostración del Teorema 2.17 es el uso de la división euclidiana en $\mathbb{N}$, convenientemente adaptada a números enteros. Si la acomodamos completamente, obtenemos el siguiente resultado fundamental de la aritmética entera. Introducimos primero la noción de valor absoluto.

DEFINICIÓN 2.18. Dado $x \in \mathbb{Z}$, definimos el *valor absoluto* de x como $|x| = x$ si $x \geq 0$, y $|x| = -x$ si $x \leq 0$.

TEOREMA 2.19 (División euclidiana en $\mathbb{Z}$). *Dados* $m, n \in \mathbb{Z}$ *con* $n \neq 0$, *existen* $q, r \in \mathbb{Z}$ *tales que* $m = qn + r$ *y* $|r| < |n|$.

DEMOSTRACIÓN. En la demostración del Teorema 2.17 hemos probado, de hecho, el enunciado para $n > 0$. Para $n < 0$, podemos aplicar lo demostrado allí a $-n$. Así, existen $q, r \in \mathbb{Z}$ tales que $m = q(-n) + r$, con $|r| < -n = |n|$. Obviamente, $m = (-q)n + r$, que es una división euclidiana como la deseada. □

DEFINICIÓN 2.20. Los números q y r que aparecen en el Teorema 2.19 se llaman, respectivamente, *cociente* y *resto* de la división de m entre n. Usaremos la notación $\mathrm{quot}(m, n) = q$ y $r = \mathrm{rem}(m, n)$.

OBSERVACIÓN 2.21. A diferencia de lo que ocurría con la división con resto en $\mathbb{N}$, los valores q y r no son ahora únicos, como muestran las dos divisiones $3 = 1 \times 2 + 1$ y $3 = 2 \times 2 - 1$.

EJERCICIO 38. Demostrar que, dados $m, n \in \mathbb{Z}$ con $n \neq 0$, existen, en general, dos restos (y no más) de dividir m entre n en $\mathbb{Z}$. ¿En qué caso son estos dos restos iguales?

2.2. Aritmética Entera

En esta sección vamos a estudiar la aritmética entera elemental.

Divisibilidad e identidad de Bezout. Comencemos fijando alguna nomenclatura.

DEFINICIÓN 2.22. Dados $a, b \in \mathbb{Z}$, diremos que a es un *divisor* de b (o que a *divide* a b) si $b = qa$ para algún $q \in \mathbb{Z}$. Usaremos entonces la notación $a|b$. Equivalentemente, diremos que b es un *múltiplo* de a.

OBSERVACIÓN 2.23. Sean $a, b \in \mathbb{Z}$. Observemos que $a|b$, para $a \neq 0$ si, y sólo si, el resto de dividir b entre a es 0. También es fácil ver que a divide a b si, y sólo si, $|a|$ divide a $|b|$. Es por eso que no se pierde generalidad si enunciamos los resultados que involucran divisibilidad para $\mathbb{N}$ en lugar de para $\mathbb{Z}$.

LEMA 2.24. *Sean* $n, m \in \mathbb{N}$. *Entonces* n *divide a* m *si, y sólo si,* $m\mathbb{Z} \subseteq n\mathbb{Z}$. *Como consecuencia,* $n = m$ *si, y sólo si,* $n\mathbb{Z} = m\mathbb{Z}$.

DEMOSTRACIÓN. Supongamos que $n|m$. Entonces $m = qn$ para algún $q \in \mathbb{N}$. Si $a \in m\mathbb{Z}$, tenemos que $a = km$ para cierto $k \in \mathbb{Z}$, luego $a = km = kqn \in n\mathbb{Z}$. Recíprocamente, si $m\mathbb{Z} \subseteq n\mathbb{Z}$, entonces $m \in n\mathbb{Z}$, luego $m = kn$, para cierto $k \in \mathbb{Z}$. Obviamente, $k \in \mathbb{N}$, con lo que $n|m$. □

PROPOSICIÓN 2.25. *Dados* $a, b \in \mathbb{N}$, *existe* $d \in \mathbb{N}$ *con la siguiente propiedad:* $d|a$, $d|b$ *y, para cualquier* $d' \in \mathbb{N}$ *tal que* $d'|a$ *y* $d'|b$, *se sigue que* $d'|d$. *El número* d *es único con esta propiedad, se llama* máximo común divisor de a *y* b, *y será denotado por* $\mathrm{mcd}(a, b)$.

DEMOSTRACIÓN. Consideremos

$$I = a\mathbb{Z} + b\mathbb{Z} = \{ka + lb \mid k, l \in \mathbb{Z}\}.$$

Comprobemos que I es un subgrupo de $\mathbb{Z}$: si $k, k', l, l' \in \mathbb{Z}$, entonces, por el Ejercicio 37,

$$ka + lb - (k'a + l'b) = (k - k')a + (l - l')b \in I.$$

Por el Teorema 2.17, existe $d \in \mathbb{N}$ tal que $I = d\mathbb{Z}$. Bien, como $a\mathbb{Z} \subseteq d\mathbb{Z}$, deducimos del Lema 2.24 que $d|a$. Análogamente, $d|b$.

Ahora, supongamos que $d'|a$ y $d'|b$. Por el Lema 2.24, tenemos que $a\mathbb{Z} \subseteq d'\mathbb{Z}$ y $b\mathbb{Z} \subseteq d'\mathbb{Z}$. Esto implica claramente que $a\mathbb{Z} + b\mathbb{Z} \subseteq d'\mathbb{Z}$. Por tanto, $d\mathbb{Z} \subseteq d'\mathbb{Z}$ y el Lema 2.24 nos da que $d'|d$. La unicidad de d viene de que si $\overline{d}$ es otro número natural con las mismas propiedades, entonces $d|\overline{d}$ y $\overline{d}|d$, de donde $d = \overline{d}$. □

OBSERVACIÓN 2.26. Si a o b es no nulo, entonces $\mathrm{mcd}(a, b)$ es el máximo, con respecto de la relación de orden "ser divisor de", del conjunto de los divisores comunes de a y b. Es claro que, con nuestra definición, $\mathrm{mcd}(0, 0) = 0$, lo que supone una excepción a la interpretación anterior, puesto todo número natural n verifica que $0 = n \cdot 0$ y, por tanto, n divide[2] a 0.

He aquí una consecuencia de la demostración de la Proposición 2.25.

TEOREMA 2.27 (Identidad de Bezout). *Dados* $a, b \in \mathbb{N}$, *y* $d = \mathrm{mcd}(a, b)$, *existen* $u, v \in \mathbb{Z}$ *tales que* $d = ua + vb$.

DEMOSTRACIÓN. Hemos visto en la demostración de la Proposición 2.25 que $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Por tanto, $d = ua + vb$, para ciertos $u, v \in \mathbb{Z}$. □

Análogamente, podemos demostrar que existe el mínimo común múltiplo de cada par de naturales.

[2]Aquí hay colisión con cierta nomenclatura en anillos. No diríamos que "n es un divisor de cero", porque este nombre se reserva a ciertos elementos en un anillo. Concretamente, si A es un anillo, un *divisor de cero* es un elemento $a \in A$, $a \neq 0$, tal que existe un elemento $b \in A$, $b \neq 0$ verificando que $ab = 0$. Observemos que, con esta definición, $\mathbb{Z}$ carece de divisores de cero.

PROPOSICIÓN 2.28. *Dados* $a, b \in \mathbb{N}$, *existe* $m \in \mathbb{N}$ *con la siguiente propiedad:* $a|m$ *y* $b|m$ *y, para cualquier* $m' \in \mathbb{N}$ *tal que* $a|m'$ *y* $b|m'$, *se sigue que* $m|m'$. *El número* m *es único con esta propiedad, se llama* mínimo común múltiplo de a *y* b, *y será denotado por* $\mathrm{mcm}(a, b)$.

DEMOSTRACIÓN. Observemos que $I = a\mathbb{Z} \cap b\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$. Por el Teorema 2.17, existe $m \in \mathbb{N}$ tal que $I = m\mathbb{Z}$. Ahora, la demostración sigue una línea argumental similar a la de la Proposición 2.25, y se deja su completación como ejercicio. □

OBSERVACIÓN 2.29. Observemos que $\mathrm{mcm}(a, b)$ es el mínimo, con repecto de la relación "ser divisor de", del conjunto de los múltiplos comunes de a y b. Observemos que $\mathrm{mcm}(a, 0) = 0 = \mathrm{mcm}(0, a)$ para cualquier $a \in \mathbb{N}$.

EJERCICIO 39. Completar la demostración de la Proposición 2.28.

Algoritmo de Euclides Extendido. Vamos ahora a exponer un algoritmo fundamental en la aritmética entera.

TEOREMA 2.30. *Dados* $a, b \in \mathbb{N}$, *con* $b \neq 0$, *definimos una sucesión de números naturales* $\{r_i\}_{i \geq 0}$ *como sigue:* $r_0 = a$, $r_1 = b$, *y el término siguiente a cada* r_i *para* $i \geq 1$ *como*

$$r_{i+1} = \begin{cases} \mathrm{rem}(r_{i-1}, r_i) & \textit{si } r_i \neq 0, \\ 0 & \textit{si } r_i = 0. \end{cases}$$

Entonces

(1) Existe $h \geq 1$ *tal que* $r_h \neq 0$ *y* $r_{h+1} = 0$.
(2) $r_h = \mathrm{mcd}(a, b)$.
(3) Existen números enteros $u_0, u_1, \ldots, u_h, u_{h+1}, v_0, v_1, \ldots, v_h, v_{h+1}$ *tales que* $r_i = u_i a + v_i b$ *para todo* $i = 0, 1, \ldots, h, h+1$.

DEMOSTRACIÓN. (1). Observemos que, siempre que $r_i \neq 0$, se tiene que $r_{i+1} < r_i$. Deducimos[3] que existe $h \geq 1$ tal que $r_h \neq 0$ pero $r_{h+1} = 0$.

(2). Para $i \leq h$, tenemos que $r_i \neq 0$, luego podemos hacer uso de la división con resto en $\mathbb{N}$

$$r_{i-1} = q_{i+1} r_i + r_{i+1},$$

donde q_{i+1} es el cociente. De aquí, los divisores comunes de r_{i-1} y r_i son los mismos que los divisores comunes de r_i y r_{i+1}. Así que

$$r_h = \mathrm{mcd}(0, r_h) = \mathrm{mcd}(r_{h+1}, r_h) = \\ \mathrm{mcd}(r_h, r_{h-1}) = \cdots = \mathrm{mcd}(r_1, r_0) = \mathrm{mcd}(b, a).$$

(3) Vamos a definir los elementos $u_i, v_i \in \mathbb{Z}$, $i = 0, 1, \ldots, h, h+1$. Tomamos

$$u_0 = 1, v_0 = 0, u_1 = 0, v_1 = 1,$$

Una vez calculados $u_i, v_i, u_{i-1}, v_{i-1}$, para $1 \leq i \leq h$, definimos

$$u_{i+1} = u_{i-1} - q_{i+1} u_i, \qquad v_{i+1} = v_{i-1} - q_{i+1} v_i.$$

Así,

$$u_{i+1} a + v_{i+1} b = (u_{i-1} - q_{i+1} u_i) a + (v_{i-1} - q_{i+1} v_i) b = \\ u_{i-1} a + v_{i-1} b - q_{i+1}(u_i a + v_i b) = r_{i-1} - q_{i+1} r_i = r_{i+1}.$$

□

[3] Ponemos $r = \min\{r_i \mid i \geq 1\}$. Afirmamos que $r = 0$. En efecto, si $r = r_i$ para cierto $i \geq 1$ y $r = r_i \neq 0$, entonces $r_{i+1} < r_i$, por lo que r no sería mínimo, lo que es una contradicción.

De la demostración del Teorema 2.30, deducimos el Algoritmo 1, que se llama *Algoritmo de Euclides Extendido*.

Algoritmo 1 `Algoritmo de Euclides Extendido`

Input: $a, b \in \mathbb{N}$ con $b \neq 0$.
Output: $\{u_i, v_i, r_i\}_{i=0,\dots,h,h+1}$ tales que $r_i = u_i a + v_i b$ para $i = 0, 1, \dots, h, h+1$,
$r_{h+1} = 0$,
$r_h = \mathrm{mcd}(a, b)$,
Initialitation:
$r_0 \leftarrow a$, $r_1 \leftarrow b$.
$u_0 \leftarrow 1$, $u_1 \leftarrow 0$.
$v_0 \leftarrow 0$, $v_1 \leftarrow 1$.
$q \leftarrow 0$, $r \leftarrow 0$.
$i \leftarrow 1$.
while $r_i \neq 0$ **do**
  $q \leftarrow \mathrm{quot}(r_{i-1}, r_i)$
  $r \leftarrow \mathrm{rem}(r_{i-1}, r_i)$
  $r_{i+1} \leftarrow r$
  $u_{i+1} \leftarrow u_{i-1} - q u_i$
  $v_{i+1} \leftarrow v_{i-1} - q v_i$
  $i \leftarrow i + 1$
return $\{u_i, v_i, r_i\}_{i=0,\dots,h,h+1}$

TEOREMA 2.31. *El Algoritmo 1 es correcto.*

DEMOSTRACIÓN. La demostración de la corrección de un algoritmo consiste en mostrar que el mismo hace lo que dice que hace, es decir, que dada una entrada como la especificada, la salida satisface lo declarado. En el caso del Algoritmo 1, su corrección se sigue de la demostración del Teorema 2.30. □

OBSERVACIÓN 2.32. Como demostraremos en un contexto más general, $\mathrm{mcm}(a, b) = a|u_{h+1}| = b|v_{h+1}|$.

EJEMPLO 2.33. La aplicación del Algoritmo 1 al par de números $a = 2018, b = 1918$ proporciona los resultados recogidos en la siguiente tabla

i	q_i	r_i	u_i	v_i
0		2018	1	0
1		1918	0	1
2	1	100	1	−1
3	19	18	−19	20
4	5	10	96	−101
5	1	8	−115	121
6	1	2	211	−222
7	4	0	−959	1009

Por tanto, $\mathrm{mcd}(2018, 1918) = 2$ y $2 = 211 \times 2018 - 222 \times 1918$. Además, según la Observación 2.32, $\mathrm{mcm}(2018, 1918) = 1935262$.

Observemos que, de acuerdo con las demostraciones de las proposiciones 2.25 y 2.28, tenemos que

$$2018\mathbb{Z} + 1918\mathbb{Z} = 2\mathbb{Z}$$

y

$$2018\mathbb{Z} \cap 1918\mathbb{Z} = 1935262\mathbb{Z}.$$

Ecuaciones diofánticas. Comenzaremos con un resultado que será útil.

LEMA 2.34. *Sean* $a, b, n, m \in \mathbb{N}$ *tales que* $na = mb$. *Si* $\mathrm{mcd}(a, b) = 1$, *entonces* n *es un múltiplo de* b *y* m *es un múltiplo de* a.

DEMOSTRACIÓN. Por la identidad de Bezout, $1 = ua + vb$ para ciertos $u, v \in \mathbb{Z}$. Multiplicando por n, obtenemos

$$n = nua + nvb = umb + nvb = (um + nv)b.$$

Así que n es un múltiplo de b. Análogamente, m es un múltiplo de a. □

EJERCICIO 40. Deducir el Teorema de Euclides (Teorema 1.72) del Lema 2.34.

Sean $a, b, c \in \mathbb{Z}$ y consideremos la ecuación siguiente en las incógnitas x, y:

$$ax + by = c \tag{2.3}$$

Vamos a suponer que $a, b \neq 0$. Y asumiremos, por comodidad, que $a, b, c \in \mathbb{N}$ (ver Observación 2.36.) Diremos que (2.3) tiene solución entera si existen $x, y \in \mathbb{Z}$ satisfaciéndola.

Discutamos primero cuándo (2.3) tiene solución, y después cómo calcular ésta. Escribamos $d = \mathrm{mcd}(a, b)$. Observemos que (2.3) tiene solución entera si, y sólo si, $c \in a\mathbb{Z} + b\mathbb{Z}$. Como $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, tenemos que (2.3) tiene solución si, y sólo si, $c \in d\mathbb{Z}$. Por tanto, (2.3) tiene solución entera si, y sólo si, c es un múltiplo de $d = \mathrm{mcd}(a, b)$.

Ahora, veamos cómo se obtienen todas las soluciones enteras de (2.3), en caso de que las haya. Calculamos, mediante el Algoritmo 1, $u, v \in \mathbb{Z}$ tales que $d = au + bv$. Como estamos en el supuesto de que (2.3) tiene solución, $c = c'd$, para cierto $c' \in \mathbb{N}$. Así que $x_0 = c'u$, $y_0 = c'v$ es una solución, lo que se ve multiplicando $d = au + bv$ por c'.

Una vez calculada una solución particular x_0, y_0, supongamos $x, y \in \mathbb{Z}$ cualquier otra solución. Entonces $a(x - x_0) + b(y - y_0) = 0$. Por otra parte, existen $a', b' \in \mathbb{N}$ tales que $a = a'd$ y $b = b'd$.

Tenemos, por un lado, que

$$a'(x - x_0) = b'(y_0 - y), \tag{2.4}$$

y, por otro,

$$1 = a'u + b'v.$$

Por tanto, $\mathrm{mcd}(a', b') = 1$. Por el Lema 2.34, $|x - x_0|$ es un múltiplo de b' e $|y - y_0|$ es un múltiplo de a'. Esto es, existen $k, l \in \mathbb{Z}$ tales que

$$x - x_0 = kb' \text{ e } y - y_0 = la'.$$

Sustituyendo en (2.4), obtenemos que $a'b'k = -a'b'l$, de donde $k = -l$. Por tanto, $x = x_0 + kb'$, $y = y_0 - ka'$. De aquí, deducimos que la solución general de (2.3) es

$$x = x_0 + kb', \quad y = y_0 - ka', \qquad k \in \mathbb{Z}.$$

EJEMPLO 2.35. Resolvamos la ecuación diofántica

$$2018x + 1918y = 100$$

Usaremos los datos calculados en el Ejemplo 2.33. Como $\mathrm{mcd}(2018, 1918) = 2$, que es un divisor de 100, la ecuación tiene soluciones enteras. Siguiendo la notación de la discusión general anterior, tenemos $d = 2$, $c' = 50$, $a' = 1009$, $b' = 959$, $u = 211$, $v = -222$. Por tanto, una solución particular es

$$x_0 = 50 \times 211, \quad y_0 = 50 \times (-222),$$

en tanto que la solución general es

$$x = 10550 + 959k, \quad y = -11100 - 1009k \qquad (k \in \mathbb{Z}).$$

Si nos hubiéramos dado cuenta de que $x_1 = 1, y_1 = -1$ es también una solución particular, podríamos haber expresado la solución general de la siguiente forma

$$x = 1 + 959k, \quad y = -1 - 1009k, \qquad (k \in \mathbb{Z}),$$

que es más sencilla.

Insistamos que cada solución particular dará una forma distinta a la solución general, pero las infinitas soluciones obtenidas al variar el parámetro entero k son las mismas.

OBSERVACIÓN 2.36. Aunque el procedimiento discutido supone $a, b, c \in \mathbb{N}$, en realidad esto no es una restricción.

Así, por ejemplo, si $a < 0$, basta con observar que la la ecuación

$$ax + by = c$$

es equivalente a

$$(-a)(-x) + by = c.$$

Cambios de signos adecuados dan cuenta también de los demás casos posibles para resolver con $a, b, c \in \mathbb{Z}$. Por cierto, que la misma idea muestra que el cálculo del máximo común divisor de dos enteros, y de los coeficientes de Bezout, se reduce fácilmente al caso de números positivos. Con todo, daremos más adelante estos algoritmos en contextos más generales, de los que $\mathbb{Z}$ será un ejemplo.

2.3. Ideales. Anillos cocientes. Ecuaciones en congruencias

Vamos a ver que ciertas relaciones de equivalencia en un anillo dado permiten dotar al conjunto cociente de estructura de anillo de una manera natural. Comenzaremos por hacerlo para grupos conmutativos con notación aditiva, ya que esta parte de la construcción es común con otros ámbitos importantes, como por ejemplo los espacios vectoriales cocientes.

Cociente de grupos conmutativos. Dado un subgrupo I de un grupo conmutativo $(A, +, 0)$, y $a \in A$, definimos

$$a + I = \{a + x \mid x \in I\}.$$

Vamos a ver que estos subconjuntos de A son las clases de equivalencia para una cierta relación de equivalencia.

LEMA 2.37. *Sea I un subgrupo de un grupo conmutativo $(A, +, 0)$. La relación R en A definida, para $a, b \in I$, por aRb si, y sólo si, $a - b \in I$ es de equivalencia. La clase de equivalencia de $a \in A$ viene descrita por $[a]_R = a + I$.*

DEMOSTRACIÓN. Sea $a \in A$. Puesto que $a - a = 0 \in I$, tenemos que aRa, y R es reflexiva.

Si $a, b \in A$ son tales que aRb, entonces $a - b \in I$. De aquí, $b - a = -(a - b) \in I$, luego bRa.

Finalmente, tomemos $a, b, c \in A$ tales que aRb y bRc. De aquí, $a - c = (a - b) + (b - c) \in I$, ya que $a - b, b - c \in I$. Por tanto, R es transitiva y concluimos que es de equivalencia.

Describamos seguidamente las clases de equivalencia. Tomemos $a \in A$ y $b \in [a]_R$. Esto significa que bRa, por lo que $b - a \in I$. Escribiendo $x = b - a$, obtenemos que $b = a + x \in a + I$. Tenemos, pues, que $[a]_R \subseteq a + I$. Para probar la inclusión recíproca, tomemos $a + x \in a + I$ con $x \in I$. Entonces $a + x - a = x \in I$, de donde $(a + x)Ra$ y $a + x \in [a]_R$. □

PROPOSICIÓN 2.38. *Dado un subgrupo* I *de un grupo conmutativo* $(A, +, 0)$*, denotemos por* A/I *el conjunto cociente de* A *bajo la relación de equivalencia descrita en el Lema 2.37. Entonces* A/I *es un grupo conmutativo con la suma definida por*

$$(a + I) + (b + I) = (a + b) + I, \qquad a + I, b + I \in A/I. \tag{2.5}$$

Dicho grupo se llama grupo cociente de A módulo (o por) I.

DEMOSTRACIÓN. Como de costumbre, hemos de comprobar primero que la suma dada en (2.5) está bien definida. Así, tomados $a + I = a' + I$, $b + I = b' + I$, tenemos que

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

ya que $a - a', b - b' \in I$. Por tanto, $(a + b) + I = (a' + b') + I$.

Ahora es fácil demostrar que la suma definida en (2.5) es asociativa y conmutativa, que el elemento neutro es I, y que si $a + I \in A/I$, entonces su opuesto es $-a + I$. En definitiva, A/I es un grupo conmutativo. □

EJERCICIO 41. Completar la demostración de la Proposición 2.38.

EJEMPLO 2.39. Tomemos $n \in \mathbb{N}$ y el subgrupo $n\mathbb{Z}$ de $(\mathbb{Z}, +, 0)$ y consideremos el grupo cociente $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Vamos a ver que, para $n \neq 0$, el grupo $\mathbb{Z}_n$ tiene n elementos. Dado $a + n\mathbb{Z} \in \mathbb{Z}_n$, tomamos $k \in \mathbb{N}$ tal que $a + kn \geq 0$. Mediante división euclidiana obtenemos $q, r \in \mathbb{N}$ tales que $a + kn = qn + r$, con $r < n$. De esta forma,

$$a + n\mathbb{Z} = (a + kn) + n\mathbb{Z} = (qn + r) + n\mathbb{Z} = r + n\mathbb{Z}.$$

Así que

$$\mathbb{Z}_n = \{r + n\mathbb{Z} \mid 0 \leq r < n\}.$$

De hecho, estos elementos son distintos: si $r + n\mathbb{Z} = s + n\mathbb{Z}$ para $0 \leq r, s < n$, entonces $r - s = qn$, para cierto $q \in \mathbb{Z}$. Así $n > |r - s| = |qn| = |q|n$, lo cual sólo es posible si $q = 0$, es decir, si $r = s$. Así que $\mathbb{Z}_n$ tiene, exactamente, n elementos.

EJERCICIO 42. Si A es un grupo conmutativo finito, e I un subgrupo de A, demostrar que $\mathrm{card}(A) = \mathrm{card}(I)\mathrm{card}(A/I)$, donde $\mathrm{card}(X)$ denota el cardinal (número de elementos) de un conjunto finito X.

Ideales y anillos cocientes. Recordemos que $\mathbb{Z}$ tiene una estructura más rica que la de grupo conmutativo. De hecho, es un anillo conmutativo. Una cuestión natural, cuya respuesta es afirmativa, es la de si los grupos $\mathbb{Z}_n$ tienen también estructura de anillo conmutativo. La construcción general es la siguiente.

DEFINICIÓN 2.40. Sea A un anillo. Un subgrupo I de $(A, +, 0)$ será llamado un *ideal* si verifica que $ax \in I$ y $xa \in I$ para todo $a \in A$ y todo $x \in I$.

PROPOSICIÓN 2.41. *Sea* I *un ideal de un anillo* A. *Entonces el grupo aditivo* A/I *tiene estructura de anillo, con la multiplicación dada por*

$$(a+I)(b+I) = ab+I, \qquad (a+I, b+I \in A/I). \tag{2.6}$$

Este anillo se llama anillo cociente de A módulo I.

DEMOSTRACIÓN. Como de costumbre, hemos de comprobar que la multiplicación dada por (2.6) está bien definida. Así, tomemos $a+I = a'+I$ y $b+I = b'+I$. Tenemos que

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

puesto que $b-b', a-a' \in I$ e I es un ideal. Por tanto, $ab+I = a'b'+I$. La unidad para esta multiplicación es $1+I$, donde $1 \in A$ es el elemento neutro para la multiplicación de A. La comprobación de que esta multiplicación en A/I es asociativa, junto con la propiedad distributiva, se deducen fácilmente de las correspondientes propiedades en A, y se dejan como ejercicio. $\square$

EJERCICIO 43. Terminar la demostración de la Proposición 2.41.

EJEMPLO 2.42. Comprobemos que cada subgrupo $n\mathbb{Z}$ del grupo aditivo $\mathbb{Z}$ es, de hecho, un ideal de $\mathbb{Z}$ con su estructura usual de anillo. Esto es fácil: si $k \in \mathbb{Z}$ y $qn \in n\mathbb{Z}$, con $k, q \in \mathbb{Z}$, entonces $kqn \in n\mathbb{Z}$. De acuerdo con la Proposición 2.41, el grupo $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ es un anillo conmutativo con la multiplicación

$$(a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+n\mathbb{Z}.$$

Para $z \in \mathbb{Z}$, se suele usar la notación simplificada $\overline{z} = z+n\mathbb{Z}$, siempre que el contexto lo permita.

Vamos a introducir la notación de congruencias. Para un ideal I de un anillo A, y elementos $a, b \in A$, usaremos la notación $a \equiv b \pmod{I}$ cuando a y b estén relacionados módulo I, esto es,

$$a \equiv b \pmod{I} \Leftrightarrow a+I = b+I \Leftrightarrow a-b \in I. \tag{2.7}$$

En el caso de $A = \mathbb{Z}$ e $I = n\mathbb{Z}$, abreviaremos escribiendo $a \equiv b \pmod{n}$ en lugar de $a \equiv b \pmod{n\mathbb{Z}}$.

EJEMPLO 2.43. Consideremos la *ecuación en congruencias o modular*

$$ax \equiv b \pmod{n}, \tag{2.8}$$

donde $a, b \in \mathbb{Z}$ son los coeficientes, $n \in \mathbb{N}$, $n \neq 0$ es el *módulo*, y x es una incógnita. Resolver esta ecuación es calcular todos los $x \in \mathbb{Z}$ que la satisfacen.

Observemos que x es una solución de (2.8) si y sólo si existe $k \in \mathbb{Z}$ tal que $ax-b = kn$. Equivalentemente, $ax-kn = b$. Así que (2.8) se reduce a una ecuación diofántica (ver Observación 2.36). Por tanto, tiene solución si, y sólo si, $mcd(a,n)|b$, y su solución se puede extraer resolviendo la ecuación diofántica. También podemos usar una procedimiento que describimos seguidamente.

Observemos que, en caso de existir solución de (2.8), tomamos $a', b' \in \mathbb{Z}$ y $n' \in \mathbb{N}$ tales que $a = a'd$, $b = b'd$, $n = n'd$, para $d = mcd(a,n)$. Así, $ax-kn = b$ es equivalente a $a'x-b' = kn'$, esto es, (2.8) es equivalente a

$$a'x \equiv b' \pmod{n'}. \tag{2.9}$$

La ventaja ahora es que $\mathrm{mcd}(a', n') = 1$. Si calculamos $u, v \in \mathbb{Z}$ tal que $1 = a'u + n'v$, entonces (2.9) es equivalente a

$$x \equiv ub' \pmod{n'}, \tag{2.10}$$

ya que, operando en $\mathbb{Z}_{n'}$, tenemos que (2.9) significa que $\overline{a'}\overline{x} = \overline{b'}$ y $\overline{1} = \overline{a'}\,\overline{u} + \overline{n'}\,\overline{v} = \overline{a'}\,\overline{u}$. Por tanto, multiplicando (2.9) por $\overline{u}$, tenemos que $\overline{x} = \overline{u}\overline{b'}$ en $\mathbb{Z}_{n'}$. Esto es equivalente a (2.10). Por tanto, la solución general de (2.8), cuando existe, es

$$x = ub' + kn', \qquad k \in \mathbb{Z}.$$

EJEMPLO 2.44. Vamos a resolver el sistema de congruencias

$$\begin{cases} 3x \equiv 1 \pmod 5 \\ 6x \equiv 3 \pmod 9 \end{cases}$$

Procederemos obteniendo la solución general de la primera congruencia, para sustituirla en la segunda, y resolver ésta.

Observemos primero que el inverso de 3 módulo 5 es 2, ya que $2 \times 3 = 6$. Por tanto, multiplicando la primera congruencia por 2, obtenemos la congruencia equivalente

$$x \equiv 2 \pmod 5,$$

cuya solución general es

$$x = 2 + 5k, \qquad k \in \mathbb{Z}. \tag{2.11}$$

Observemos que, puesto que $\mathrm{mcd}(6, 9) = 3$, la segunda congruencia puede reducirse a

$$2x \equiv 1 \pmod 3.$$

Sustituyendo el valor de x dado en (2.11), obtenemos

$$4 + 10k \equiv 1 \pmod 3.$$

Reduciendo los coeficientes módulo 3, tenemos que

$$1 + k \equiv 1 \pmod 3,$$

equivalentemente,

$$k \equiv 0 \pmod 3.$$

De modo que

$$k = 3m, \qquad m \in \mathbb{Z}.$$

Sustituyendo este valor en (2.11), obtenemos

$$x = 2 + 15m, \qquad m \in \mathbb{Z}, \tag{2.12}$$

que es la solución general del sistema. De hecho, hemos deducido que cualquier solución es de la forma descrita en (2.12), y es fácil comprobar, sustituyendo, que todo número entero de la forma descrita en (2.12) es, realmente, solución del sistema.

Teorema Chino del Resto y sistemas de ecuaciones en congruencias. Vamos a dar un criterio de existencia de solución de sistemas de ecuaciones en congruencias (2.8). Antes, vamos a estudiar algunas operaciones con ideales de un anillo cualquiera, que ayudarán en esta tarea, y que son básicas para otros muchos propósitos que involucran anillos.

LEMA 2.45. *Sea A un anillo, e I, J ideales de A. Entonces $I \cap J$ es un ideal de A. Además, si definimos*

$$I + J = \{x + y \mid x \in I, y \in J\}$$

obtenemos un ideal de A.

DEMOSTRACIÓN. Es un ejercicio fácil. $\square$

EJERCICIO 44. Sea A un anillo y consideremos el conjunto $\mathcal{I}(A)$ de todos los ideales de A. Demostrar que $(\mathcal{I}(A), \cap, A)$ e $(\mathcal{I}(A), +, \{0\})$ son monoides conmutativos.

DEFINICIÓN 2.46. Dos ideales I, J de un anillo A se dicen *coprimos* si $I + J = A$. Equivalentemente, existen $x \in I, y \in J$ tales que $x + y = 1$.

LEMA 2.47. *Sean* I, J, K *ideales de un anillo* A. *Se verifica que* $I + J = I + K = A$ *si, y sólo si,* $I + J \cap K = A$. *Más en general, si* $I_1, \dots, I_t$ *son ideales de* A*, con* $t \geq 2$*, se tiene que* $I_1 + I_j = A$ *para todo* $j = 2, \dots, t$ *si, y sólo si,* $I_1 + \bigcap_{j=2}^t I_j = A$.

DEMOSTRACIÓN. Supongamos que $I + J = I + K = A$. Entonces existen $x, x' \in I, y \in J, z \in K$ tales que $1 = x + y$ y $1 = x' + z$. Así,

$$1 = x + y = x + y(x' + z) = x + yx' + yz \in I + J \cap K.$$

Por tanto, $I + J \cap K = A$.

Recíprocamente, supongamos que $A = I + J \cap K$. Entonces $I + J \supseteq I + J \cap K = A$, por lo que $I + J = A$. Análogamente, $I + K = A$.

Vayamos con la segunda afirmación. Comencemos demostrando por inducción sobre t que si $I_1 + I_j = A$ para todo $j = 2, \dots, t$, entonces $I_1 + \bigcap_{j=2}^t I_j = A$. Dicha implicación es trivial para $t = 2$. Partiendo de $I_1 + I_j = A$ para todo $j = 2, \dots, t+1$, pongamos $I = I_1, J = \bigcap_{j=2}^t I_j, K = I_{t+1}$. Tenemos entonces, por hipótesis de inducción, que $I + J = A$. Como $I + K = A$, deducimos de lo demostrado que $I + J \cap K = A$. Pero $J \cap K = \bigcap_{j=2}^{t+1} I_j$, lo que completa la inducción.

La implicación recíproca es, como antes, muy fácil. $\square$

TEOREMA 2.48 (Teorema Chino del Resto, versión abstracta.). *Sean* $I_1, \dots, I_t$ *ideales de un anillo* A*, con* $t \geq 2$*. Cada sistema de congruencias*

$$\left\{ \begin{array}{l} x \equiv b_1 \pmod{I_1} \\ x \equiv b_2 \pmod{I_2} \\ \dots\dots\dots\dots\dots \\ x \equiv b_t \pmod{I_t} \end{array} \right. \tag{2.13}$$

para cualesquiera $b_1, b_2, \dots, b_t \in A$ *tiene solución si, y sólo si,* $I_i + I_j = A$ *para todo* $i, j = 1, \dots, t$ *con* $i \neq j$.

DEMOSTRACIÓN. Supongamos primero que $I_i + I_j = A$ para cualesquiera $i \neq j$. Por el Lema 2.47, para todo $i = 1, \dots t$, tenemos que $I_i + \bigcap_{j \neq i} I_j = A$. Para cada $i = 1, \dots, t$, tenemos entonces que $1 = a_i + p_i$, donde $a_i \in I_i$ y $p_i \in \bigcap_{j \neq i} I_j$. Para valores cualesquiera $b_1, b_2, \dots, b_t \in A$, pongamos $x = \sum_{i=1}^t b_i p_i \in A$. Así, para cada $j = 1, \dots, t$, tenemos

$$x + I_j = \sum_{i=1}^t b_i p_i + I_j \overset{(*)}{=} b_j p_j + I_j = b_j(1 - a_j) + I_j = b_j - b_j a_j + I_j \overset{(**)}{=} b_j + I_j, \tag{2.14}$$

luego $x \equiv b_j \pmod{I_j}$. En el anterior cálculo, la igualdad $(*)$ viene de que $p_i \in \bigcap_{k \neq i} I_k \subseteq I_j$ para todo $j \neq i$, luego $b_i p_i + I_j = 0 + I_j$ si $i \neq j$. La igualdad $(**)$ ocurre porque $a_j \in I_j$. Como (2.14) dice que $x \equiv b_j \pmod{I_j}$ para $j = 1, \dots, t$, concluimos que (2.13) tiene solución.

Recíprocamente, supongamos que cada sistema de congruencias (2.13) tiene solución en A. Dado $i = 1, \dots, t$, tomamos $b_j = 0$ si $j \neq i$, y $b_i = 1$. Para $x \in A$ una solución del sistema correspondiente, tenemos que $x - 1 \in I_i$, mientras que $x \in \bigcap_{j \neq i} I_j$. Esto es, $1 = 1 - x + x \in I_i + \bigcap_{j \neq i} I_j$. Por el Lema 2.47, $I_j + I_i = A$ para todo $j \neq i$. □

COROLARIO 2.49 (Teorema Chino del Resto). *Supongamos números naturales* $n_1, n_2, \dots, n_t$. *Cada sistema de congruencias*

$$\left\{ \begin{array}{l} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \cdots\cdots\cdots\cdots\cdots \\ x \equiv b_t \pmod{n_t} \end{array} \right. \tag{2.15}$$

para cualesquiera $b_1, b_2, \dots, b_t \in \mathbb{Z}$ *tiene solución si, y sólo si,* $\mathrm{mcd}(n_i, n_j) = 1$ *para todo* $i, j = 1, \dots, t$ *con* $i \neq j$

OBSERVACIÓN 2.50. Es posible que, sin la condición $\mathrm{mcd}(n_i, n_j) = 1$ para $i \neq j$, el sistema (2.15) tenga solución para algunos $b_1, b_2, \cdots, b_t \in \mathbb{Z}$ **concretos**.

EJERCICIO 45. Demostrar que el sistema de congruencias en $\mathbb{Z}$

$$\left\{ \begin{array}{l} x \equiv 1 \pmod 6 \\ x \equiv 2 \pmod 4 \end{array} \right.$$

no tiene solución, en tanto que

$$\left\{ \begin{array}{l} x \equiv 1 \pmod 6 \\ x \equiv 3 \pmod 4 \end{array} \right.$$

sí que las tiene.

EJERCICIO 46. Sean I y J subgrupos de un grupo aditivo A tales que $I \subseteq J$. Demostrar que J/I es un subgrupo de A/I. Si, además, A es un anillo e I, J son ideales de A, entonces J/I es un ideal de A/I.

EJERCICIO 47. Sea I un subgrupo de un grupo aditivo A, y V un subgrupo de A/I. Demostrar que $J = \{a \in A \mid a + I \in V\}$ es un subgrupo de A que contiene a I. Comprobar que $V = J/I$. Deducir que, si A es un anillo e I es un ideal de A, entonces todo ideal de A/I es de la forma J/I, para J un ideal de A que contiene a I.

EJERCICIO 48. Si $n \in \mathbb{N}$, calcular todos los subgrupos del grupo aditivo $\mathbb{Z}_n$. ¿Cuáles de ellos son ideales?

2.4. Subanillos. Homomorfismos. Unidades

Vamos a seguir presentando conceptos fundamentales del Álgebra abstracta.

Subanillos. Comenzaremos con la noción de subanillo de un anillo, que permitirá tener algunos ejemplos nuevos.

DEFINICIÓN 2.51. Un *subanillo* de un anillo A es un subconjunto S de A que es, a la vez, subgrupo aditivo y submonoide multiplicativo de A. Es decir, S es un *subanillo* de A si, para todo $s, s' \in S$, se verifica

1. $s - s' \in S$.
2. $ss' \in S$.
3. $1 \in S$.

Es claro que un subanillo de A es, a su vez, un anillo.

EJEMPLO 2.52. Admitamos el conjunto de los números reales $\mathbb{R}$ con sus operaciones usuales de suma y producto. Con estas operaciones, $\mathbb{R}$ es un anillo conmutativo (de hecho, es un cuerpo, en la terminología que introduciremos más abajo). Tomemos el subconjunto $\mathbb{Z}[\sqrt{2}]$ de $\mathbb{R}$ definido como sigue:

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

Es fácil comprobar que $\mathbb{Z}[\sqrt{2}]$ es un subanillo de $\mathbb{R}$.

En general, para $D \in \mathbb{N}$, que no sea un cuadrado, se tiene el subanillo de $\mathbb{R}$

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}.$$

Merece la pena mencionar que, para definir $\mathbb{Z}[\sqrt{D}]$, no es necesario en realidad admitir antes $\mathbb{R}$, como veremos más adelante.

EJEMPLO 2.53. Ya que hemos aceptado $\mathbb{R}$, podemos aceptar también que sabemos qué es una función polinómica $f : \mathbb{R} \to \mathbb{R}$. Expícitamente, f es polinómica si existen $a_0, a_1, \ldots, a_n \in \mathbb{R}$ tales que

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \tag{2.16}$$

para todo $x \in \mathbb{R}$. Diremos que f tiene grado n is $a_n \neq 0$.

Si denotamos por $\mathbb{R}[x]$ el conjunto de todas las funciones polinómicas, tenemos que, con la suma y producto usual de funciones, $\mathbb{R}[x]$ es un anillo conmutativo.

Observemos que, si A es cualquier subanillo de $\mathbb{R}$, entonces podemos considerar el conjunto $A[x]$ de todas las funciones polinómicas f de la forma (2.16), tales que $a_0, a_1, \ldots, a_n \in A$. Es fácil ver que $A[x]$ es un subanillo de $\mathbb{R}[x]$. En particular, tendremos el anillo $\mathbb{Z}[x]$.

Más adelante, daremos una definición formal de anillo de polinomios con coeficientes generales, pero por el momento, pensemos sólo en anillos de funciones polinómicas como los recién descritos.

Homomorfismos de grupos. Queremos definir qué es un homomorfismo de anillos. Como un anillo combina dos estructuras más elementales (grupo conmutativo y monoide), damos primero la definición de homomorfismo de grupos.

DEFINICIÓN 2.54. Sean $(A, *, e)$ y $(B, \cdot, u)$ grupos. Un *homomorfismo de grupos* de A a B es una aplicación $f : A \to B$ tal que $f(a * a') = f(a) \cdot f(a')$ para todo $a, a' \in A$. Un homomorfismo de grupos biyectivo se llama isomorfismo de grupos.

EJERCICIO 49. Demostrar que si $f : A \to B$ es un isomorfismo de grupos, entonces $f^{-1} : B \to A$ es un isomorfismo de grupos.

EJERCICIO 50. Sean $(A, *, e)$ y $(B, \cdot, u)$ grupos, y $f : A \to B$ es un homomorfismo de grupos. Demostrar que $f(e) = u$ y que $f(\overline{a}) = \overline{f(a)}$ para todo $a \in A$.

EJEMPLO 2.55. Si $(A, +, 0)$ es un grupo aditivo e I es un subgrupo, entonces la proyección canónica $\pi : A \to A/I$, que recordemos está dada por $\pi(a) = a + I$ para todo $a \in A$, es un homomorfismo de grupos.

Bien, vamos a ver que un homomorfismo entre grupos conmutativos entraña, en particular, un grupo cociente.

TEOREMA 2.56. *Sea* $f : A \to B$ *un homomorfismo de grupos, donde* A *y* B *son grupos aditivos. Entonces* $\mathrm{Im}(f)$ *es un subgrupo de* B *y*

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0\}$$

es un subgrupo de A*. Además, existe un isomorfismo de grupos*

$$\widetilde{f} : A/\mathrm{Ker}(f) \to \mathrm{Im}(f) \tag{2.17}$$

que verifica

$$\widetilde{f}(a + \mathrm{Ker}(f)) = f(a), \qquad \textit{para todo } a \in A. \tag{2.18}$$

DEMOSTRACIÓN. Veamos primero que $\mathrm{Im}(f)$ es un subgrupo de B. Tomemos dos elementos de $\mathrm{Im}(f)$, que son de la forma $f(a), f(a')$ para $a, a' \in A$. Usando el Ejercicio 50, tenemos que

$$f(a) - f(a') = f(a) + f(-a') = f(a - a') \in \mathrm{Im}(f).$$

Veamos que $\mathrm{Ker}(f)$ es un subgrupo de A: dados $a, a' \in \mathrm{Ker}(f)$, entonces $f(a - a') = f(a) - f(a') = 0 - 0 = 0$, donde hemos usado el Ejercicio 50. Dos elementos $a, a' \in A$ están relacionados por la relación de equivalencia definida por el subgrupo $\mathrm{Ker}(f)$ si, y sólo si, $a - a' \in \mathrm{Ker}(f)$. Esto es, $0 = f(a) - f(a')$ o, equivalentemente, $f(a) = f(a')$. Por tanto, dicha relación es $\sim_f$, la relación definida por f en tanto que aplicación. En virtud de la Proposición 1.56 existe una biyección $\widetilde{f} : A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ que verifica (2.18). Por último,

$$\begin{aligned}\widetilde{f}((a + \mathrm{Ker}(f)) + (a' + \mathrm{Kerf}(f))) &= \widetilde{f}(a + a' + \mathrm{Ker}(f)) \\ &= f(a + a') = f(a) + f(a') = \widetilde{f}(a + \mathrm{Ker}(f)) + \widetilde{f}(a' + \mathrm{Ker}(f)),\end{aligned}$$

lo que muestra que $\widetilde{f}$ es un homomorfismo de grupos y, al ser biyectivo, un isomorfismo. □

EJEMPLO 2.57. Si I es cualquier subgrupo de $(A, +, 0)$, y $\pi : A \to A/I$ es la proyección canónica, entonces $\mathrm{Ker}(\pi) = I$. En este caso, $\widetilde{\pi} = \mathrm{id}_{A/I}$.

EJEMPLO 2.58. Es fácil comprobar que un homomorfismo de grupos aditivos $f : A \to B$ es inyectivo si, y sólo si, $\mathrm{Ker}(f) = \{0\}$. En este caso, el Teorema 2.56 dice que $A/\{0\}$ es isomorfo a $\mathrm{Im}(f)$. También sabemos que A es isomorfo a $\mathrm{Im}(f)$.

Observemos que, si consideramos el isomorfismo identidad id_A, tenemos que $\mathrm{Ker}(\mathrm{id}_A) = \{0\}$, luego $A/\{0\}$ es isomorfo a A, mediante la aplicación $\widetilde{\mathrm{id}_A} : A/\{0\} \to A$ definida por $\widetilde{\mathrm{id}_A}(\{a\}) = a$ para todo $\{a\} \in A/\{0\}$.

EJERCICIO 51. Sean $n, m \in \mathbb{N}$ con n divisor de m, y sea $d \in \mathbb{N}$ tal que $m = dn$. Demostrar que la aplicación $f : \mathbb{Z}_n \to \mathbb{Z}_m$ dada por

$$f(x + n\mathbb{Z}) = dx + m\mathbb{Z},$$

para $x + n\mathbb{Z} \in \mathbb{Z}_n$ está bien definida, y es un homomorfismo inyectivo de grupos.

Homomorfismos de anillos. Vayamos con los homomorfismos de anillos.

DEFINICIÓN 2.59. Sean A y B anillos. Una aplicación $f : A \to B$ se dice un *homomorfismo de anillos* si es homomorfismo de grupos, para los grupos aditivos $(A, +, 0)$ y $(B, +, 0)$, y homomorfismo de monoides[4], para los

[4]Aunque no lo hayamos definido explícitamente, un homomorfismo de monoides es aquella aplicación que preserva productos y elementos neutros.

monoides multiplicativos $(A, \cdot, 1)$ y $(B, \cdot, 1)$. En otras palabras, para cualesquiera $a, a' \in A$, se tiene

1. $f(a + a') = f(a) + f(a')$.
2. $f(aa') = f(a)f(a')$.
3. $f(1) = 1$.

Un homomorfismo de anillos f que sea biyectivo se llama un *isomorfismo de anillos*. Entonces f^{-1} resulta ser también un isomorfismo de anillos.

EJEMPLO 2.60. Si I es un ideal de un anillo A, entonces la proyección canónica $\pi : A \to A/I$ es un homomorfismo de anillos.

EJEMPLO 2.61. Consideremos, en el Ejercicio 51, que $n \neq m \neq 1$. Entonces el homomorfismo de grupos f allí definido no es homomorfismo de anillos ya que, por ejemplo, $f(1 + n\mathbb{Z}) = d + m\mathbb{Z} \neq 1 + m\mathbb{Z}$.

Bien, ya estamos en condiciones de formular la versión para anillos del Teorema 2.56.

TEOREMA 2.62. *Sea* $f : A \to B$ *un homomorfismo de anillos. Entonces* $\mathrm{Ker}(f)$ *es un ideal de* A *y el isomorfismo de grupos* $\widetilde{f} : A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ *dado en el Teorema 2.56 es un isomorfismo de anillos.*

DEMOSTRACIÓN. En vista de lo afirmado en el Teorema 2.56, sólo hemos de comprobar que $\widetilde{f}$ es homomorfismo de monoides multiplicativos. Primero comprobamos que preserva el uno: $\widetilde{f}(1 + \mathrm{Ker}(f)) = f(1) = 1$, por ser f homomorfismo de anillos. En segundo, y último, lugar, vemos que $\widetilde{f}$ es multiplicativa:

$$\widetilde{f}(a + \mathrm{Ker}(f))(b + \mathrm{Kerf}(f)) = \widetilde{f}(ab + \mathrm{Ker}(f)) = f(ab) =$$
$$f(a)f(b) = \widetilde{f}(a + \mathrm{Ker}(f))\widetilde{f}(b + \mathrm{Ker}(f)).$$

□

EJEMPLO 2.63. Consideremos el anillo $\mathbb{Z}[x]$ de funciones polinómicas con coeficientes enteros definido en el Ejemplo 2.53. Dado un número real $r \in \mathbb{R}$, consideremos la aplicación $ev_r : \mathbb{Z}[x] \to \mathbb{R}$ definida por $ev_r(f(x)) = f(r)$ para todo $f(x) \in \mathbb{Z}[x]$. Es fácil comprobar que esta aplicación es un homomorfismo de anillos. Por el Teorema 2.62, $\mathrm{Im}(ev_r)$ es un subanillo de $\mathbb{R}$ y $\mathrm{Ker}(ev_r)$ es un ideal de $\mathbb{Z}[x]$, y tenemos un isomorfismo de anillos $\mathbb{Z}[x]/\mathrm{Ker}(ev_r) \cong \mathrm{Im}(ev_r)$.

La determinación de $\mathrm{Ker}(ev_r)$ puede no ser fácil. Un número r para el cual $\mathrm{Ker}(ev_r) = \{0\}$ se llama *transcendente*. Obsérvese que, para un número transcendente r, el subanillo $\mathrm{Im}(ev_r)$ de $\mathbb{R}$ es isomorfo a $\mathbb{Z}[x]$. Esto parece raro, pero el Teorema 2.62 garantiza que es cierto. Quienes son raros son los números reales.

La transcencencia del número e fue demostrada por Hermite en 1873, en tanto que la transcendencia de π hubo de esperar a Lindemann en 1882. No son demostraciones fáciles. De hecho, hay algunos números “famosos”, para los cuales no se sabe si son transcendentes.

Los números no transcendentes se llaman *algebraicos*. Así, un número algebraico r es el que satisface que $\mathrm{Ker}(ev_r) \neq \{0\}$. Por ejemplo, $\sqrt{2}$ es algebraico. También son algebraicos los números racionales, aunque un número algebraico no tiene por qué ser racional (es el caso de $\sqrt{2}$.).

EJERCICIO 52. Sea A un anillo. Demostrar que existe un único homomorfismo de anillos $\chi : \mathbb{Z} \to A$. El número $n \in \mathbb{Z}$ tal que $\mathrm{Ker}(\chi) = n\mathbb{Z}$

se llama *característica de* A. Deducir que A contiene un único subanillo isomorfo a $\mathbb{Z}_n$ (recordemos que $\mathbb{Z}_0$ es isomorfo con $\mathbb{Z}$.)

EJERCICIO 53. Calcular todos los homomorfismos de anillos de $\mathbb{Z}_n$ a $\mathbb{Z}_m$, para $n, m \in \mathbb{N}$.

Teorema Chino del Resto y unidades. En este curso, vamos a dar varios métodos para construir nuevos anillos a partir de anillos conocidos. ASÍ, tenemos el anillo cociente A/I definido a partir de un ideal I de un anillo conmutativo A. La noción de subanillo también produce nuevos ejemplos. Veamos un tercer método, el producto de anillos.

DEFINICIÓN 2.64. Sean $A_1, A_2, \dots, A_t$ anillos. Consideremos el producto cartesiano

$$A_1 \times A_2 \times \cdots \times A_t = \{(a_1, a_2, \dots, a_t) \mid a_i \in A_i \text{ para } i = 1, \dots, t\}$$

Dotamos a este conjunto de las siguientes operaciones suma y multiplicación, definidas a partir de las de los anillos $A_1, \dots, A_t$:

$$(a_1, a_2, \dots, a_t) + (b_1, b_2, \dots, b_t) = (a_1 + b_1, a_2 + b_2, \dots, a_t + b_t),$$

$$(a_1, a_2, \dots, a_t)(b_1, b_2, \dots, b_t) = (a_1b_1, a_2b_2, \dots, a_tb_t),$$

para $(a_1, a_2, \dots, a_t), (b_1, b_2, \dots, b_t) \in A_1 \times A_2 \times \cdots \times A_t$.

Es fácil comprobar que, con estas operaciones, $A_1 \times A_2 \times \cdots \times A_t$ es un anillo, donde el cero es $(0, 0, \cdots, 0)$ y el uno es $(1, 1, \dots, 1)$. Este anillo se llama *anillo producto* de $A_1, A_2, \dots, A_t$. Es conmutativo si cada uno de los A_i's lo es.

EJEMPLO 2.65. Podemos construir, por ejemplo, $\mathbb{Z}_2 \times \mathbb{Z}_2$ o $\mathbb{Z}_2 \times \mathbb{Z}_3$. Veremos dentro de poco que el segundo de estos anillos es “esencialmente” $\mathbb{Z}_6$. Necesitamos el concepto de isomorfismo de anillos[5] para expresar precisamente qué es “esencialmente”.

TEOREMA 2.66 (Teorema Chino del Resto, versión homomorfismo). *Sean* $I_1, I_2, \dots, I_t$ *ideales de un anillo* A*, con* $t \geq 2$*. Entonces la aplicación*

$$f : A \to A/I_1 \times A/I_2 \times \cdots \times A/I_t$$

definida por $f(a) = (a + I_1, a + I_2, \dots, a + I_t)$ *para* $a \in A$ *es un homomorfismo de anillos cuyo núcleo es* $I = I_1 \cap I_2 \cap \cdots \cap I_t$*. Por tanto, en virtud del Teorema 2.62, induce en el cociente* A/I *un homomorfismo inyectivo de anillos*

$$\widetilde{f} : A/I \to A/I_1 \times A/I_2 \times \cdots \times A/I_t,$$

$$\widetilde{f}(a + I) = (a + I_1, a + I_2, \dots, a + I_t).$$

Además, $\widetilde{f}$ *es un isomorfismo de anillos si, y sólo si,* $I_i + I_j = A$ *para todo* $i \neq j$.

DEMOSTRACIÓN. Que f es un homomorfismo de anillos es una comprobación rutinaria.

Para $a \in A$, tenemos que $a \in \operatorname{Ker}(f)$ si, y sólo si $a + I_i = I_i$ para todo $i = 1, \dots, t$, esto es, $a \in I_i$ para todo $i = 1, \dots, t$. Por tanto, $\operatorname{Ker}(f) = I$.

El Teorema 2.62 da ahora el homomorfismo inyectivo $\widetilde{f}$. Caracterizar cuándo éste es sobreyectivo y, por tanto, un isomorfismo, es consecuencia del Teorema 2.48. □

EJERCICIO 54. Detallar el final de la demostración del Teorema 2.66.

Vamos ahora a introducir el grupo de unidades de un anillo.

[5]Recordemos, homomorfismo biyectivo de anillos

DEFINICIÓN 2.67. Sea A un anillo. Un elemento $a \in A$ se llama una *unidad* de A si existe $u \in A$ tal que $au = 1$ y $ua = 1$. El conjunto de las unidades de A se denotará $U(A)$. Que $U(A)$ es un grupo, con la operación producto, es sencillo de comprobar. Compruébalo.

EJEMPLO 2.68. Volvamos a $\mathbb{Z}_n$. La ecuación modular (2.8) es equivalente a la ecuación en $\mathbb{Z}_n$

$$\overline{a}\,\overline{x} = \overline{b}. \tag{2.19}$$

Si tomamos $\overline{b} = \overline{1}$, tenemos que la ecuación (2.19) tiene solución si, y sólo si, $\mathrm{mcd}(a, n) = 1$. Observemos que, para resolverla, basta con calcular $u, v \in \mathbb{Z}$ tal que $1 = au + nv$, ya que, entonces, $\overline{1} = \overline{a}\,\overline{u} + \overline{n}\,\overline{v} = \overline{a}\,\overline{u}$.

Hemos demostrado, pues, que $U(\mathbb{Z}_n) = \{\overline{u} \mid \mathrm{mcd}(u, n) = 1\}$.

Cuando el grupo de unidades es lo mayor posible, y el anillo es conmutativo y no trivial, tenemos un cuerpo.

DEFINICIÓN 2.69. Un anillo conmutativo no trivial A es un *cuerpo* si $U(A) = A \setminus \{0\}$.

EJEMPLO 2.70. Se sigue del Ejemplo 2.68 que el anillo $\mathbb{Z}_n$ es un cuerpo si, y sólo si, n es un número primo.

EJEMPLO 2.71. El anillo $\mathbb{R}$ es un cuerpo.

EJERCICIO 55. Demostrar que si $A_1, \dots, A_t$ son anillos, entonces

$$U(A_1 \times \cdots \times A_t) = U(A_1) \times \cdots \times U(A_t).$$

Seguidamente, vamos a dar un método para calcular el número de unidades de $\mathbb{Z}_n$, donde aparecerá la celebrada función totiente de Euler.

TEOREMA 2.72. *Para cada número natural n distinto de 0, definimos $\varphi(n)$ como el número de naturales $k \leq n$ tales que $\mathrm{mcd}(k, n) = 1$. Entonces:*

1. *Si $m, n \in \mathbb{N}_+$ verifican que $\mathrm{mcd}(n, m) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*
2. *Si $n \in \mathbb{N}$, $n \neq 0, 1$ y $n = p_1^{e_1} \cdots p_t^{e_t}$ es su descomposición como producto de números primos, donde $p_1, \dots, p_t$ son primos distintos y $e_1, \dots, e_t \in \mathbb{N}_+$, entonces*

$$\varphi(n) = (p_1 - 1) \cdots (p_t - 1) p_1^{e_1 - 1} \cdots p_t^{e_t - 1}. \tag{2.20}$$

3. *Si $n \in \mathbb{N}$, $n \neq 0, 1$, entonces*

$$\varphi(n) = n \prod_{\substack{p \text{ primo} \\ p \mid n}} \left(1 - \frac{1}{p}\right)$$

DEMOSTRACIÓN. 1. Como consecuencia del Teorema 2.66, tenemos un isomorfismo de anillos

$$\frac{\mathbb{Z}}{m\mathbb{Z} \cap n\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Dado que $\mathrm{mcm}(m, n) = mn$, tenemos que $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$. Por tanto, tenemos un isomorfismo de anillos

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n,$$

cuya restricción a $U(\mathbb{Z}_{nm})$ da un isomorfismo de grupos multiplicativos $U(\mathbb{Z}_{mn}) \cong U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$. Según el Ejemplo 2.68, $\varphi(k)$ es el cardinal del grupo $U(\mathbb{Z}_k)$. Por tanto, $\varphi(mn) = \varphi(m)\varphi(n)$.

2. Vamos a razonar por inducción sobre $t \geq 1$. Para $t = 1$, hemos de contar los números $0 < u \leq p_1^{e_1}$ tales que $\mathrm{mcd}(u, p_1^{e_1}) = 1$. Es más fácil

contar aquellos u tales que $\mathrm{mcd}(u, p_1^{e_1}) \neq 1$. De hecho, esta condición es equivalente a decir que p_1 es un divisor de u. Pero los múltiplos u de p_1 con $u \leq p_1^{e_1}$ se obtienen como $p_1 k$, con $0 < k \leq p_1^{e_1 - 1}$. Así,

$$\varphi(p_1^{e_1}) = p_1^{e_1} - p_1^{e_1-1} = (p_1 - 1)p_1^{e_1-1}.$$

La inducción se completa fácilmente usando el apartado 1.

3. Esta igualdad se obtiene de (2.20). □

Vamos a concluir con un teorema de Euler que tiene importancia tanto teórica como práctica.[6] Antes de enunciarlo, demostremos un lema que necesitaremos.

LEMA 2.73. *Sea G un grupo conmutativo, para el que usamos notación multiplicativa, con elemento neutro e. Si G es finito y tiene m elementos, entonces $g^m = e$ para todo $g \in G$.*

DEMOSTRACIÓN. La aplicación $f : \mathbb{Z} \to G$, definida por $f(i) = g^i$ para $i \in \mathbb{Z}$, es un homomorfismo de grupos. Sabemos que $\mathrm{Ker}(f)$ es un subgrupo de $\mathbb{Z}$, por lo que, de acuerdo con el Teorema 2.17, existe $n \in \mathbb{N}$ tal que $\mathrm{Ker}(f) = n\mathbb{Z}$. Por el Teorema 2.56, $\mathrm{Im}(f) \cong \mathbb{Z}_n$. Como G es finito, deducimos que $n > 0$. Por el Ejercicio 42, n es un divisor de m, por lo que $m \in \mathrm{Ker}(f)$. Por tanto,

$$e = f(m) = g^m.$$

□

TEOREMA 2.74. *Sea $n \in \mathbb{N}$, $n \neq 0, 1$. Entonces, para todo $a \in \mathbb{Z}$ tal que $\mathrm{mcd}(a, n) = 1$, tenemos que*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{2.21}$$

DEMOSTRACIÓN. Sabemos que $\varphi(n)$ es el cardinal del grupo $U(\mathbb{Z}_n)$. Como $\overline{a} \in U(\mathbb{Z}_n)$, deducimos del Lema 2.73 que $\overline{a}^{\varphi(n)} = \overline{1}$ en $\mathbb{Z}_n$. Esta igualdad es equivalente a (2.21). □

EJEMPLO 2.75. Vamos a calcular los dos últimos dígitos de 13^{41}. Evidentemente, esto es calcular el resto de dividir 13^{41} entre 100. Usaremos la aritmética de $\mathbb{Z}_{100}$. Observemos que $\varphi(100) = \varphi(2^2 5^2) = 40$. Por tanto,

$$13^{41} \equiv 13 \pmod{100},$$

lo que indica que las dos últimas cifras pedidas son 13.

EJERCICIO 56. Sean I, J subgrupos de un grupo aditivo A tales que $I \subseteq J$. Dar un isomorfismo de grupos

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

Comprobar que, si A es un anillo, e I y J son ideales de A, entonces el anterior isomorfismo es de anillos.

EJERCICIO 57. Sea I un ideal de un anillo A. Demostrar que todo ideal de A/I es de la forma J/I para J un ideal de A tal que $I \subseteq J$.

EJERCICIO 58. Sea n un número natural con $n \geq 2$. Calcular todos los subanillos de $\mathbb{Z}_n$. Calcular todos los ideales de $\mathbb{Z}_n$.

EJERCICIO 59. Calcular todos los subanillos de $\mathbb{Z}_2 \times \mathbb{Z}_4$.

[6] Este resultado se utiliza para el diseño del sistema criptográfico RSA, de uso muy extendido.

Capítulo 3

Anillos de Polinomios. Dominios Euclídeos.

3.1. Noción de Anillo de Polinomios

Vamos a introducir una construcción fundamental, la de anillo de polinomios. Los ingredientes para construir estos anillos son un anillo de coeficientes y una indeterminada. Para evitar concebir esta última de manera esotérica, haremos una construcción formal de la misma. Es decir, vamos a dar consistencia matemática a la expresión "suma formal"que se suele usar para hablar de polinomios.

Es conveniente primero discutir de qué manera un anillo se puede considerar "dentro" de otro. Una respuesta obvia es que eso es la noción de subanillo. Sin embargo, este punto de vista es demasiado rígido en la práctica. Veamos un ejemplo de esto.

EJEMPLO 3.1. Consideremos el anillo $\mathbb{R}[x]$ de las funciones polinómicas. Sea $\iota : \mathbb{R} \to \mathbb{R}[x]$ la aplicación que asigna a cada número real $r \in \mathbb{R}$ la función constante $\iota(r) : \mathbb{R} \to \mathbb{R}$, definida por $\iota(r)(x) = r$ para todo $r \in \mathbb{R}$. Es fácil ver que ι es un homomorfismo inyectivo de anillos y, por tanto, la aplicación correstricción de ι da un isomorfismo de anillos $\mathbb{R} \cong \mathrm{Im}(\iota)$.

Observemos que $\mathrm{Im}(\iota)$ es el subanillo de $\mathbb{R}[x]$ formado por las funciones constantes. Bien, una simplificación usual sustituir $\mathbb{R}$ por su imagen isomorfa $\mathrm{Im}(\iota)$ y, por tanto, considerar $\mathbb{R}$ como un subanillo de $\mathbb{R}[x]$. Explícitamente, esto significa considerar cada número real r como la función constantemente r, sin hacer explícito el homomorfismo inyectivo ι.

En general, si tenemos anillos A y B y un homomorfismo inyectivo de anillos $\iota : A \to B$, el anillo A es isomorfo al subanillo $\mathrm{Im}(\iota)$ de B. Siempre que ι esté claro por el contexto, no hay problema en identificar A con $\mathrm{Im}(\iota)$. En la práctica, esto significa que si $a \in A$ y $b \in B$, escribiremos, por ejemplo, ab para representar $\iota(a)b$, o $a + b$ para $\iota(a) + b$. Diremos que B contiene la copia isomorfa $\mathrm{Im}(\iota)$ de A.

TEOREMA 3.2. *Sea A un anillo conmutativo. Existe un anillo conmutativo P que contiene una copia isomorfa de A y un elemento $X \in P$ tal que cualquier elemento no nulo $f \in P$ se representa de manera única como*

$$f = f_0 + f_1X + \cdots + f_nX^n, \tag{3.1}$$

para $f_0, f_1, \ldots, f_n \in A$ y $f_n \neq 0$.

DEMOSTRACIÓN. Vamos a construir primero un anillo S del que P será un subanillo. Tomemos

$$S = Map(\mathbb{N}, A) = \{f \mid \mathbb{N} \xrightarrow{f} A\},$$

el conjunto de todas las aplicaciones de $\mathbb{N}$ a A. Si $f \in S$, escribimos $f(n) = f_n$ para cada $n \in \mathbb{N}$, podemos escribir f como la sucesión $(f_n)_{n\geq 0}$ o, más gráficamente,

$$f = (f_0, f_1, \ldots, f_n, \ldots).$$

Comencemos dotando a S de una suma que lo convierta en grupo aditivo. Definimos, para $f = (f_n)_{n\geq 0}, g = (g_n)_{n\geq 0} \in S$, su suma $f + g = s$, donde $s = (s_n)_{n\geq 0}$ está definida por

$$s_n = f_n + g_n,$$

para $n \in \mathbb{N}$. Es fácil ver que, con esta suma, S es un grupo aditivo. El "cero" es la sucesión constantemente 0, esto es

$$0 = (0, 0, \dots, 0, \dots)$$

El producto es un poco más elaborado. Así, $fg = p$, donde $p = (p_n)_{n\geq 0}$ viene definida por

$$p_n = \sum_{i+j=n} f_i g_j. \tag{3.2}$$

para cada $n \in \mathbb{N}$. Esta multiplicación tiene elemento neutro, que es la sucesión todos cuyos términos son 0 salvo el primero (el que ocupa el lugar 0-ésimo), que es 1. Esto es

$$1 = (1, 0, 0, \dots, 0, \dots)$$

Esta multiplicación es asociativa. En efecto, si

$$f = (f_n)_{n\geq 0}, g = (g_n)_{n\geq 0}, h = (h_n)_{n\geq 0} \in S,$$

entonces el término n–ésimo del producto $(fg)h$ es

$$\sum_{i+j=n} \left(\sum_{u+v=i} f_u g_v \right) h_j = \sum_{u+v+j=n} f_u g_v h_j, \tag{3.3}$$

donde hemos usado que el producto de A es asociativo y distributivo con respecto de la suma de A. Análogamente, el término n–ésimo de $f(gh)$ es

$$\sum_{i+j=n} f_i \left(\sum_{u+v=j} g_u h_v \right) = \sum_{i+u+v=n} f_i g_u h_v. \tag{3.4}$$

Como los miembros de la derecha de (3.3) y (3.4) son iguales, tenemos la multiplicación es asociativa.

Es fácil comprobar, usando que A es conmutativo, que esta multiplicación es también conmutativa.

Queda también testar la propiedad distributiva, lo que se deja como ejercicio rutinario. Tenemos así que S es un anillo conmutativo.

Ahora definimos $\iota : A \to S$ mediante la regla

$$\iota(a) = (a, 0, 0, \dots, 0 \dots), \qquad a \in A.$$

Dadas las operaciones suma y producto definidas en S, y quién es su "uno", es muy fácil comprobar que ι es un homomorfismo inyectivo de anillos. Por tanto, $\mathrm{Im}(\iota)$ es una copia isomorfa de A dentro de S. Usando esta identificación y denotando

$$X = (0, 1, 0, \dots, 0, \dots)$$

es claro que

$$aX = (0, a, 0, \dots, 0, \dots),$$

para cada $a \in A$.

Observemos cuál es el efecto de multiplicar $f \in S$ por X. Llamemos, provisionalmente, $p = Xf$, y analicemos sus términos. Por ejemplo, $p_0 = X_0 f_0 = 0$, ya que $X_0 = 0$. Para $n > 0$, tenemos que

$$p_n = \sum_{i+j=n} X_i f_j = X_1 f_{n-1} = f_{n-1}.$$

Es decir,

$$X(f_0, f_1, \dots) = (0, f_0, f_1, \dots).$$

Deducimos de aquí que, para cada $i \geq 1$, X^i es la sucesión todos cuyos términos son nulos, excepto el i–ésimo, que es 1.

Tomemos ahora el subconjunto P de S de aquellas sucesiones con sólo una cantidad de términos no nulos. Es decir, cada $f \in P$ es de la forma

$$f = (f_0, f_1, \dots, f_m, 0, 0, \dots),$$

esto es, f se puede escribir en la forma

$$f = f_0 + f_1 X + \cdots + f_m X^m,$$

para ciertos $f_0, f_1, \dots, f_m \in A$.

De la definición de la suma en S, deducimos fácilmente que P es un subgrupo aditivo de S. También es cierto que un producto de dos elementos de P se queda en P, ya que, según la Definición 3.2, si $f, g \in P$, entonces existen $n, m \in \mathbb{N}$ tales que $f_i = 0$ para todo $i > n$, y $g_j = 0$ para todo $j > m$, entonces el producto $p = fg$ verifica que $p_k = 0$ para todo $k > n + m$. Por último, es claro que $1 \in P$.

Obviamente, la copia isomorfa de A en S descrita antes, está, de hecho, contenida en P. Por último, cada elemento no nulo $f \in P$ se escribe en la forma

$$f = f_0 + f_1 X + \cdots + f_n X^n$$

con $f_n \neq 0$. Esta forma es única, ya que dice que f es la sucesión

$$f = (f_0, f_1, \dots, f_n, 0, 0 \dots),$$

y dos sucesiones son iguales si, y sólo si, son iguales término a término. $\square$

DEFINICIÓN 3.3. El anillo P definido en el Teorema 3.2 se llama *anillo de polinomios en la indeterminada* X *con coeficientes en* A. Seguidamente, vamos a ver que X se comporta ciertamente como una indeterminada. Usamos la notación $P = A[X]$.

EJERCICIO 60. Completar la demostración de la Proposición 3.2 comprobando los detalles no explicitados.

OBSERVACIÓN 3.4. El anillo S construido en la demostración del Teorema 3.2 se llama *anillo de series formales en* X *con coeficientes en* A, y se usa la notación $S = A[[X]]$. Cada elemento $f = (f_n)_{n \geq 0}$ se representa normalmente por $\sum_{n=0}^{\infty} f_n X^n$. Pero esto no debe de preocuparnos durante este curso.

TEOREMA 3.5 (Propiedad universal del anillo de polinomios). *Sean* A *y* B *anillos conmutativos. Para cada homomorfismo de anillos* $\phi : A \to B$ *y cada elemento* $b \in B$, *existe un único homomorfismo de anillos* $\widehat{\phi} : A[X] \to B$ *tal que* $\widehat{\phi}_{|A} = \phi$ *y* $\widehat{\phi}(X) = b$.

DEMOSTRACIÓN. Veamos primero que, de existir, $\widehat{\phi}$ ha de ser único. Para ello, tomamos $f = f_0 + f_1X + \cdots + f_nX^n \in A[X]$ y le aplicamos $\widehat{\phi}$, que se supone homomorfismo de anillos, por lo que

$$\begin{aligned}(3.5)\quad \widehat{\phi}(f) = \widehat{\phi}(f_0) + \widehat{\phi}(f_1)\widehat{\phi}(X) + \cdots + \widehat{\phi}(f_n)\widehat{\phi}(X)^n \\ = \phi(f_0) + \phi(f_1)b + \cdots + \phi(f_n)b^n.\end{aligned}$$

De modo que, de existir $\widehat{\phi}$ en las condiciones requeridas, ha de estar definido por (3.5), lo que prueba su unicidad.

Definamos ahora $\widehat{\phi} : A[X] \to B$. Declaramos que $\widehat{\phi}(0) = 0$ y, para $0 \neq f \in A[X]$, usando la representación única de f dada en (3.1), definimos

$$\widehat{\phi}(f) = \phi(f_0) + \phi(f_1)b + \cdots + \phi(f_n)b^n.$$

Para comprobar que $\widehat{\phi}$, así definido, es un homomorfismo de anillos, es cómodo representar cada $f \in A[X]$, de manera compacta, como $f = \sum_i f_iX^i$. En esta notación se sobreentiende que $f_i \in A$ es nulo salvo una cantidad finita de subíndices $i \in \mathbb{N}$. Así, la suma indicada es finita y

$$\widehat{\phi}(f) = \sum_i \phi(f_i)b^i.$$

Bien, dados $f, g \in A[X]$, tenemos

$$\begin{array}{rcl}\widehat{\phi}(f+g) & = & \widehat{\phi}(\sum_i f_iX^i + \sum_i g_iX^i) \\ & = & \widehat{\phi}(\sum_i (f_i + g_i)X^i) \\ & = & \sum_i \phi(f_i + g_i)b^i \\ & = & \sum_i \phi(f_i)b^i + \sum_i \phi(g_i)b^i \\ & = & \widehat{\phi}(f) + \widehat{\phi}(g),\end{array}$$

y

$$\begin{array}{rcl}\widehat{\phi}(fg) & = & \widehat{\phi}((\sum_i f_iX^i)(\sum_i g_iX^i)) \\ & = & \widehat{\phi}(\sum_k(\sum_{i+j=k} f_ig_j)X^k) \\ & = & \sum_k \phi(\sum_{i+j=k} f_ig_j)b^k \\ & = & \sum_k(\sum_{i+j=k} \phi(f_i)\phi(g_j))b^k \\ & = & \left(\sum_i \phi(f_i)b^i\right)\left(\sum_i \phi(g_i)b^i\right) \\ & = & \widehat{\phi}(f)\widehat{\phi}(g).\end{array}$$

Como, claramente, $\widehat{\phi}(1) = \phi(1) = 1$, tenemos que $\widehat{\phi}$ es ciertamente un homomorfismo de anillos. Además, $\widehat{\phi}(a) = \phi(a)$ para todo $a \in A$, y $\widehat{\phi}(X) = b$. □

Una consecuencia importante del anterior teorema es la noción de evaluación, que sugiere que X se comporta como lo que esperamos de una indeterminada.

COROLARIO 3.6. *Si A es un subanillo de B y $b \in B$, entonces tenemos el homomorfismo de anillos $ev_b : A[X] \to B$ dado por*

$$ev_b(f) = \sum_i f_ib^i, \qquad (f = \sum_i f_iX^i \in A[X]).$$

Este es el llamado homomorfismo evaluación en b. *Se usa la notación $f(b) = ev_b(f)$.*

EJEMPLO 3.7. El anillo de polinomios $\mathbb{R}[X]$ y el de funciones polinómicas $\mathbb{R}[x]$ son isomorfos. Explícitamente, si denotamos por x a la función

polinómica identidad en $\mathbb{R}$, entonces tenemos el homomorfismo evaluación $ev_x : \mathbb{R}[X] \to \mathbb{R}[x]$. Se trata de un homomorfismo sobreyectivo, ya que si
$$p(x) = a_n x^n + \cdots + a_0$$
es una función polinómica, entonces
$$ev_x(a_n X^n + \cdots + a_0) = p(x).$$
También es inyectivo, puesto que su núcleo es cero. En efecto, si $f = f_0 + f_1 X + \cdots + f_n X^n \in Ker(ev_x)$, entonces la función polinómica $f(x) = ev_x(f) = f_0 + f_1 x + \cdots + f_n x^n$ ha de ser nula. Pero esto implica que[1] $f_0 = \cdots = f_n = 0$.

3.2. División de polinomios

Comencemos definiendo algunos parámetros asociados a un polinomio.

Sea A una anillo conmutativo, y tomemos un polinomio no nulo $f \in A[X]$,
$$f = f_0 + f_1 X + \cdots + f_n X^n,$$
con $f_i \in A$ para $i = 0, 1, \ldots, n$ y $f_n \neq 0$. Cada $f_i X^i$ se recibe el nombre de *monomio* de f.

Llamamos *grado* de f al número natural $\deg(f) = n$. El *coeficiente líder o director* de f se define como $\mathrm{lc}(f) = f_n$, en tanto que el *monomio líder o director* de f es $\mathrm{lm}(f) = f_n X^n$.

Para trabajar con agilidad con polinomios, introducimos el símbolo $-\infty$, y decimos que $\deg(0) = -\infty$. Convenimos que $-\infty < n$ para todo $n \in \mathbb{N}$, y también que
$$-\infty + n = -\infty = n + (-\infty) = -\infty + (-\infty).$$
Con esta convención, tenemos que, si $0 \neq f \in A[X]$, entonces
$$f = \mathrm{lc}(f) X^{\deg(f)} + f_\downarrow,$$
para $f_\downarrow \in A[X]$ tal que $\deg(f_\downarrow) < \deg(f)$.

El siguiente lema recoge las propiedades básicas del grado.

LEMA 3.8. *Sean* $f, g \in A[X]$ *no nulos. Entonces*

1. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.
2. $\deg(f+g) < \max\{\deg(f), \deg(g)\}$ *si, y sólo si,*
$$\deg(f) = \deg(g) \text{ y } \mathrm{lc}(g) + \mathrm{lc}(f) = 0.$$
3. $\deg(fg) \leq \deg(f) + \deg(g)$.
4. $\deg(fg) < \deg(f) + \deg(g)$ *si, y sólo si,* $\mathrm{lc}(f)\mathrm{lc}(g) = 0$.

DEMOSTRACIÓN. Escribamos $f = f_n X^n + f_\downarrow$ y $g = g_m X^m + g_\downarrow$, con $n = \deg(f)$ y $m = \deg(g)$.

1 y 2. Podemos suponer, sin pérdida de generalidad, que $n \leq m$. Tenemos que
$$f + g = f_n X^n + f_\downarrow + g_m X^m + g_\downarrow.$$
Si $n < m$, entonces en los polinomios $f_\downarrow, g_m X^m, g_\downarrow$ sólo aparecen monomios de grado menor que n. Así, $\deg(f) = n = \max\{n, m\}$. Si $n = m$, entonces
$$f + g = (f_n + g_n) X^n + f_\downarrow + g_\downarrow.$$
Así que, si $f_n + g_n \neq 0$, entonces $\deg(f+g) = n = \max\{n, m\}$. En caso de ser $f_n + g_n = 0$, vemos que $\deg(f+g) = \deg(f_\downarrow + g_\downarrow) < n$.

[1]Podemos demostrar por inducción sobre n que si $f(x)$ se anula en infinitos valores, entonces $f_0 = \cdots = f_n = 0$.

3 y 4. Tenemos que

$$fg = (f_n X^n + f_\downarrow)(g_m X^m + g_\downarrow) = f_n g_m X^{n+m} + f_n X^n g_\downarrow + g_m X^m f_\downarrow + f_\downarrow g_\downarrow. \tag{3.6}$$

Razonamos por inducción sobre $\deg(f) + \deg(g) = n + m$.

Si $n+m = 0$, entonces $n = m = 0$ y, por tanto, $f, g \in A$. Por tanto, $fg \in A$ y $\deg(fg) = 0 = \deg(f) + \deg(g)$ si $fg \neq 0$, y $\deg(fg) = -\infty < 0$ si $fg = 0$.

Supongamos ahora que $n + m > 0$. Por hipótesis de inducción,

$$\deg(f_n X^n g_\downarrow) \leq n + \deg(g_\downarrow) < n + m.$$

Análogamente, $\deg(g_m X^m f_\downarrow) < n+m$ y $\deg(f_\downarrow g_\downarrow) < n+m$. Así que, si $f_n g_m \neq 0$, deducimos que de (3.6) que $\deg(fg) = n + m = \deg(f) + \deg(g)$. En tanto que si $f_n g_n = 0$, deducimos que

$$\begin{aligned}\deg(fg) &= \deg(f_n X^n g_\downarrow + g_m X^m f_\downarrow + f_\downarrow g_\downarrow)\\ &\leq \text{máx}\{\deg(f_n X^n g_\downarrow), \deg(g_m X^m f_\downarrow), \deg(f_\downarrow g_\downarrow)\} < n + m\end{aligned}$$

Lo que completa la inducción. □

Esta función grado permite dar un algoritmo de división con resto para polinomios. Antes de dar éste, vamos a demostrar un lema que usaremos un par de veces.

LEMA 3.9. *Sean* $f, g \in A[X]$ *con* $\deg(f) \geq \deg(g) \geq 0$, *y pongamos* $m = \deg(f) - \deg(g)$. *Entonces*

$$\deg\left(\mathrm{lc}(g)f - \mathrm{lc}(f)X^m g\right) < \deg(f).$$

DEMOSTRACIÓN. Tenemos

$$\begin{aligned}&\mathrm{lc}(g)f - \mathrm{lc}(f)X^m g\\ &\quad= \mathrm{lc}(g)(\mathrm{lc}(f)X^{\deg(g)} + f_\downarrow) - \mathrm{lc}(f)(X^m \mathrm{lc}(g)X^{\deg(g)} + X^m g_\downarrow)\\ &\quad= \mathrm{lc}(g)\mathrm{lc}(f)X^{\deg(f)} + \mathrm{lc}(g)f_\downarrow - \mathrm{lc}(f)\mathrm{lc}(g)X^{m+\deg(g)} - \mathrm{lc}(f)X^m g_\downarrow\\ &\quad= \mathrm{lc}(g)f_\downarrow - \mathrm{lc}(f)X^m g_\downarrow.\end{aligned}$$

Por otra parte,

$$\begin{aligned}&\deg(\mathrm{lc}(g)f_\downarrow - \mathrm{lc}(f)X^m g_\downarrow)\\ &\quad\leq \text{máx}\{\deg(\mathrm{lc}(g)f_\downarrow), \deg(\mathrm{lc}(f)X^m g_\downarrow)\}\\ &\quad\leq \text{máx}\{\deg(f_\downarrow), m + \deg(g_\downarrow)\} < \deg(f).\end{aligned}$$

□

TEOREMA 3.10 (Pseudo-división o División libre de fracciones). *Sean* $f, g \in A[X]$ *con* $g \neq 0$. *Entonces existen* $q, r \in A[X]$ *y* $\ell \in \mathbb{N}$ *tales que*

1. $\mathrm{lc}(g)^\ell f = qg + r$,
2. $\deg(r) < \deg(g)$.

DEMOSTRACIÓN. Observemos primero que si $\deg(f) < \deg(g)$, tenemos la división trivial $f = 0g + f$ (obviamente, entendemos que $\mathrm{lc}(g)^0 = 1$). Por tanto, podemos suponer que $f \neq 0$ y razonar por inducción sobre $\deg(f)$.

Si $\deg(f) = 0$ y $\deg(g) > 0$, tenemos, como antes, una división trivial.

Si $\deg(f) = 0 = \deg(g)$, entonces $f, g \in A$, y tenemos que $\mathrm{lc}(g)f = fg + 0$ da una división tomando $r = 0$ y $q = f$.

Bien, supongamos ahora que $\deg(f) > 0$. Si $\deg(f) < \deg(g)$, volvemos a tener una división trivial.

Discutamos, pues, el caso $\deg(f) \geq \deg(g)$. Escribimos

$$f = \mathrm{lc}(f)X^{\deg(f)} + f_\downarrow, g = \mathrm{lc}(g)X^{\deg(g)} + g_\downarrow.$$

Pongamos $m = \deg(f) - \deg(g)$. Por el Lema 3.9, $\deg(\mathrm{lc}(g)f - \mathrm{lc}(f)X^m g) < \deg(f)$. Por hipótesis de inducción, existen $\ell \in \mathbb{N}$, $q_1, r \in A[X]$ con $\deg(r) < \deg(g)$ tales que

$$\mathrm{lc}(g)^\ell(\mathrm{lc}(g)f - \mathrm{lc}(f)X^m g) = q_1 g + r.$$

Por tanto,

$$\mathrm{lc}(g)^{\ell+1} f = \mathrm{lc}(g)^\ell \mathrm{lc}(f)X^m g + q_1 g + r = qg + r,$$

tomando $q = \mathrm{lc}(g)^\ell \mathrm{lc}(f)X^m + q_1$. Esto completa la inducción y demuestra el teorema. □

DEFINICIÓN 3.11. La igualdad

$$\mathrm{lc}(g)^\ell f = qg + r$$

con la condición

$$\deg(r) < \deg(g)$$

se llama *división libre de fracciones* o *pseudo-división* en $A[X]$ de f entre g. El polinomio q se llama *pseudo-cociente* en tanto que r se llama *pseudo-resto.*

Reorganizando las ideas de la demostración del Teorema 3.10 obtenemos el Algoritmo 2.

Algoritmo 2 `Pseudo-División` o `División libre de fracciones`

Input: $f, g \in A[X]$ con $g \neq 0$, donde A es cualquier anillo conmutativo.
Output: $\ell \geq 0$, $q, r \in A[X]$, tales que $\mathrm{lc}(g)^\ell f = qg + r$, con $\deg r < \deg g$.

Initialitation:
$q \leftarrow 0$
$r \leftarrow f$
$\ell \leftarrow 0$
while $\deg g \leq \deg r$ **do**
  $q \leftarrow \mathrm{lc}(g)q + \mathrm{lc}(r)X^{\deg r - \deg g}$
  $r \leftarrow \mathrm{lc}(g)r - \mathrm{lc}(r)X^{\deg r - \deg g} g$
  $\ell \leftarrow \ell + 1$
return ℓ, q, r

TEOREMA 3.12. *El Algoritmo 2 calcula correctamente una división libre de fracciones de f entre g.*

DEMOSTRACIÓN. Llamemos $r_\ell, q_\ell \in A[X]$ al estado de r y q antes de pasar el filtro de entrada al bucle "while", para un $\ell \geq 0$ dado. Afirmamos que dichos valores verifican que $\mathrm{lc}(g)^\ell f = q_\ell g + r_\ell$, igualdad que llamaremos "división parcial".

Para $\ell = 0$, la identidad $\mathrm{lc}(g)^0 f = q_0 g + r_0$ es obvia, por los valores iniciales asignados en el algoritmo (entendemos que $\mathrm{lc}(g)^0 = 1$).

Razonemos ahora que si $\ell \geq 0$ y r_ℓ, q_ℓ verifican la división parcial y pasan el filtro, entonces los valores que salen del bucle "while" , $r_{\ell+1}, q_{\ell+1}$, siguen verificando una división parcial. En efecto, si $\deg(r_\ell) \geq \deg(g)$, tenemos

$$\begin{aligned} q_{\ell+1} g + r_{\ell+1} &= (\mathrm{lc}(g)q_\ell + \mathrm{lc}(r_\ell)X^{\deg r_\ell - \deg g})g + \mathrm{lc}(g)r_\ell - \mathrm{lc}(r_\ell)X^{\deg r_\ell - \deg g} g \\ &= \mathrm{lc}(g)q_\ell g + \mathrm{lc}(g)r_\ell \\ &= \mathrm{lc}(g)(q_\ell g + r_\ell) \\ &= \mathrm{lc}(g)^{\ell+1} f. \end{aligned}$$

Si el par r_ℓ, q_ℓ no pasa el filtro del bucle, es porque $\deg(r_\ell) < \deg(g)$, y salimos con la división realizada.

Razonemos ahora que no podemos entrar en un bucle infinito. Si r_ℓ, q_ℓ han pasado el filtro, entonces, por el Lema 3.9,

$$\deg r_{\ell+1} = \deg(\mathrm{lc}(g)r_\ell - \mathrm{lc}(r_\ell)X^{\deg r_\ell - \deg g} g) < \deg r_\ell.$$

Por tanto, la condición que abre el bucle "while" no puede repetirse indefinidamente, lo que significa que el algoritmo termina en un número finito de pasos. □

OBSERVACIÓN 3.13. La prueba del Teorema 3.12 demuestra también el Teorema 3.10.

EJEMPLO 3.14. El siguiente cuadro contiene los cálculos de la división libre de fracciones en $\mathbb{Z}[X]$ de $f = 3X^3 + 5X + 1$ entre $g = 2X + 1$ mediante el Algoritmo 2.

	$f = 3X^3 + 5X + 1$	$g = 2X + 1$	
ℓ	r_ℓ	q_ℓ	$\mathrm{lc}(r_\ell)X^{\deg(r_\ell)-\deg(g)}$
0	$3X^3 + 5X + 1$	0	$3X^2$
1	$6X^3 + 10X + 2$ $-6X^3 - 3X^2$ $-3X^2 + 10X + 2$	0 $3X^2$ $3X^2$	 $-3X$
2	$-6X^2 + 20X + 4$ $6X^2 + 3X$ $23X + 4$	$6X^2$ $-3X$ $6X^2 - 3X$	 23
3	$46X + 8$ $-46X - 23$ -15	$12X^2 - 6X$ 23 $12X^2 - 6X + 23$	

En gris aparecen cálculos intermedios para obtener los sucesivos restos. Por lo demás, la mecánica es similar a la de la división usual con resto de polinomios que sabéis del colegio. La línea para $\ell = 0$ da información redundante, y puede prescindirse de ella, si se quiere y se tiene claro qué ha de aparecer en la línea $\ell = 1$.

El resultado es la división, puesto que $\ell = 3$, es

$$8f = (12X^2 - 6X + 23)g - 15.$$

Si se quiere obtener la división "tradicional" en $\mathbb{Q}[X]$, ésta se obtiene multiplicando por $1/8$, con lo que obtenemos

$$f = \left(\frac{3}{2}X^2 - \frac{3}{4}X + \frac{23}{8}\right) g - \frac{15}{8}.$$

Esta idea puede exportarse al caso general, siempre que $\mathrm{lc}(g)$ sea una unidad en el anillo de coeficientes A. Ése es el contenido del Corolario 3.16.

EJEMPLO 3.15. Hagamos, como curiosidad, la división libre de fracciones de $\overline{3}X^2 + X + \overline{1}$ entre $\overline{2}X + \overline{1}$ en $\mathbb{Z}_4[X]$.

	$f = \overline{3}X^3 + X + \overline{1}$	$g = \overline{2}X + 1$
ℓ	r	q
0	$\overline{3}X^3 + X + \overline{1}$	$\overline{0}$
1	$\overline{2}X^3 + \overline{2}X + \overline{2}$ $\overline{2}X^3 + X^2$ $X^2 + \overline{2}X + \overline{2}$	$\overline{3}X^2$
2	$\overline{2}X^2$ $\overline{2}X^2 + \overline{3}X$ $\overline{3}X$	$\overline{2}X^2 + X$
3	$\overline{2}X$ $\overline{2}X + \overline{1}$ $\overline{1}$	$\overline{2}X + \overline{3}$

La división da la igualdad

$$\overline{0} = (\overline{2}X + \overline{3})(\overline{2}X + \overline{1}) + \overline{1},$$

que, por supuesto, es correcta.

Obsérvese que, el mismo resultado, podría haberse obtenido tomando la pseudo-división dada en el Ejemplo 3.14 y reduciendo los coeficientes módulo 4. ¿Por qué?

COROLARIO 3.16 (División euclídea de polinomios). *Sean* $f, g \in A[X]$ *y supongamos que* $\mathrm{lc}(g) \in U(A)$*. Entonces existen* $q, r \in A[X]$ *tales que*

1. $f = qg + r$,
2. $\deg(r) < \deg(g)$.

DEMOSTRACIÓN. Se deduce inmediatamente del Teorema 3.10, ya que $\mathrm{lc}(g)^\ell \in U(A)$ para todo $\ell \geq 0$ y podemos, por tanto, multiplicar por $\mathrm{lc}(g)^{-\ell}$ la división libre de fracciones para obtener la división establecida en el enunciado. □

DEFINICIÓN 3.17. La igualdad

$$f = qg + r$$

con la condición

$$\deg(r) < \deg(g)$$

se llama *división con resto* o *división euclídea* de f entre g. El polinomio q se llama *cociente*, mientras que r se llama *resto*.

Es posible también modificar el bucle "while" del Algoritmo 2 para calcular directamente la división euclídea sin pasar previemante la división libre de fracciones. Mientras que el Corolario 3.16 se deduce del enunciado del Teorema 3.10, de la demostración del Teorema 3.12, convenientemente adaptada, se deduce la corrección del Algoritmo 3.

EJEMPLO 3.18. El siguiente cuadro contiene los cálculos de la división euclídea en $\mathbb{Q}[X]$ de $f = 3X^3 + 5X + 1$ entre $g = 2X + 1$ mediante el Algoritmo

Algoritmo 3 División Euclídea de Polinomios

Input: $f, g \in A[X]$ con $\mathrm{lc}(g) \in U(A)$, donde A es cualquier anillo conmutativo.
Output: $q, r \in A[X]$, tales que $f = qg + r$, con $\deg r < \deg g$.
Initialitation:
$q \leftarrow 0$
$r \leftarrow f$
while $\deg g \leq \deg r$ **do**
$q \leftarrow q + \mathrm{lc}(g)^{-1}\mathrm{lc}(r)X^{\deg r - \deg g}$
$r \leftarrow r - \mathrm{lc}(g)^{-1}\mathrm{lc}(r)X^{\deg r - \deg g}g$
return q, r

3.

	$f = 3X^3 + 5X + 1$	$g = 2X + 1$
ℓ	r	q
0	$3X^3 + 5X + 1$	0
1	$-3X^3 - \frac{3}{2}X^2$ $-\frac{3}{2}X^2 + 5X + 1$	$\frac{3}{2}X^2$
2	$\frac{3}{2}X^2 + \frac{3}{4}X$ $\frac{23}{4}X + 1$	$\frac{3}{2}X^2 - \frac{3}{4}X$
3	$-\frac{23}{4}X - \frac{23}{8}$ $\frac{-15}{8}$	$\frac{3}{2}X^2 - \frac{3}{4}X + \frac{23}{8}$

El resultado de la división es

$$f = \left(\frac{3}{2}X^2 - \frac{3}{4}X + \frac{23}{8}\right) g - \frac{15}{8}.$$

Observemos que, en cada paso, hemos de calcular los coeficientes en $\mathbb{Q}$, lo que, en general, cuesta más que en $\mathbb{Z}$.

EJEMPLO 3.19. Consideremos el homomorfismo evaluación

$$ev_{\sqrt{2}} : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{2}],$$

que es claramente sobreyectivo. Además, $X^2 - 2 \in \mathrm{Ker}(ev_{\sqrt{2}})$. Supongamos ahora $f \in \mathrm{Ker}(ev_{\sqrt{2}})$. Entonces $f(\sqrt{2}) = 0$. Por la división con resto, existen $q, r \in \mathbb{Z}[X]$ tales que $f = q \cdot (X^2 - 2) + r$, con $\deg(r) < 2$. Se tiene, así, que $0 = f(\sqrt{2}) = r(\sqrt{2})$. Veamos que esto implica que $r = 0$. De lo contrario, r sería de grado 1, por lo que $r = aX + b$, para ciertos $a, b \in \mathbb{Z}$, con $a \neq 0$. Así que $a\sqrt{2} + b = 0$, y $\sqrt{2}$ sería un número racional, cosa que sabemos no es cierta. Por tanto, $r = 0$ y $f = q \cdot (X^2 - 2)$. Hemos demostrado, pues, que

$$\mathrm{Ker}(ev_{\sqrt{2}}) = \{p(X)(X^2 - 2) : p(X) \in \mathbb{Z}[X]\}.$$

3.3. Dominios de ideales principales y divisibilidad

En esta sección, estudiaremos una noción central en el ámbito del Álgebra, como es la de dominio de ideales principales.

Divisibilidad en un dominio de integridad. Dominios de ideales principales. Un tipo de anillo conmutativo fundamental está constituido por los dominios de integridad.

DEFINICIÓN 3.20. Por un *dominio de integridad* entenderemos un anillo conmutativo no trivial A tal que si $ab = 0$ para $a, b \in A$, entonces $a = 0$ o $b = 0$.

EJEMPLO 3.21. El anillo $\mathbb{Z}$ es un dominio de integridad.

EJEMPLO 3.22. Todo cuerpo es un dominio de integridad. Así lo son, $\mathbb{R}$ y $\mathbb{Z}_p$ para p primo. Cada subanillo de un dominio de integridad es claramente un dominio de integridad. Por tanto $\mathbb{Z}[\sqrt{D}]$ es un dominio de integridad.

EJERCICIO 61. Demostrar que un anillo conmutativo finito A es un dominio de integridad si, y sólo si, A es un cuerpo.

PROPOSICIÓN 3.23. *Un anillo conmutativo A es un dominio de integridad si, y sólo si, el anillo de polinomios $A[X]$ es un dominio de integridad.*

DEMOSTRACIÓN. Si A es un dominio de integridad y $f, g \in A[X]$ son no nulos, entonces, por el Lema 3.8, $\deg(fg) = \deg(f) + \deg(g) \geq 0$, ya que $\mathrm{lc}(f)\mathrm{lc}(g) \neq 0$. Por tanto, $fg \neq 0$, y $A[X]$ es un dominio de integridad. Recíprocamente, como A es un subanillo de $A[X]$, el primero ha de ser un dominio de integridad si lo es el segundo. □

Recordemos que, como consecuencia del Teorema 2.17, cualquier ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ para cierto $n \in \mathbb{N}$. Este tipo de ideales son importantes, y reciben el nombre de principales.

DEFINICIÓN 3.24. Sea A un anillo conmutativo. Un ideal I se dice *principal* si existe $a \in I$ tal que $I = \{ba \mid b \in A\}$. Se suele usar la notación $I = \langle a \rangle$ o, también, $I = Aa$. El elemento a se llama *generador* de I.

Los ideales de la forma $J = Aa_1 + \cdots + Aa_n$ para ciertos $a_1, \ldots, a_n$, se llaman *finitamente generados*, y los elementos $a_1, \ldots, a_n$ *generadores* de J. Usamos la notación $J = \langle a_1, \ldots, a_n \rangle$. Explícitamente,

$$\langle a_1, \ldots, a_n \rangle = \{b_1 a_1 + \cdots + b_n a_n \mid b_1, \ldots, b_n \in A\}.$$

DEFINICIÓN 3.25. Un dominio de integridad se llama *dominio de ideales principales* si todo ideal suyo es principal.

EJEMPLO 3.26. El anillo $\mathbb{Z}$ es un dominio de ideales principales.

El siguiente es un resultado fundamental.

TEOREMA 3.27. *Si K es un cuerpo, entonces el anillo de polinomios $K[X]$ es un dominio de ideales principales.*

DEMOSTRACIÓN. Que $K[X]$ es un dominio de integridad es una consecuencia de la Proposición 3.23.

Sea I cualquier ideal de $K[X]$. Si $I = \{0\}$, entonces, obviamente, $I = \langle 0 \rangle$, y es principal. Supongamos que $I \neq \langle 0 \rangle$. Tomemos $g \in I$ tal que

$$\deg(g) = \min\{\deg(f) \mid f \in I, f \neq 0\}.$$

Como $g \in I$, tenemos que $\langle g \rangle \subseteq I$. Para demostrar la inclusión recíproca, sea $f \in I$. Por la División Euclídea, existen $q, r \in K[X]$ tales que $f = qg + r$ y $\deg(r) < \deg(g)$. Ahora bien, $r = f - qg \in I$. Como g es de grado mínimo entre los polinomios no nulos de I, deducimos que $r = 0$. Por tanto, $f = qg \in \langle g \rangle$. □

DEFINICIÓN 3.28. Sean $a, b \in A$, donde A es un anillo conmutativo. Diremos que a *divide* a b (o que a *es un divisor* de b) si existe $c \in A$ tal que $b = ca$. También se dice que b *es un múltiplo* de a. Para señalar esta situación, usaremos la notación $a|b$.

EJERCICIO 62. Demostrar que, para $a, b \in A$ con A anillo conmutativo, se tiene que $a|b$ si, y sólo si, $\langle b \rangle \subseteq \langle a \rangle$. Como consecuencia, $(A, |\ )$ resulta ser un conjunto pre-ordenado.

EJEMPLO 3.29. Sea A un anillo conmutativo y $\alpha \in A$. Tomemos $f \in A[X]$ un polinomio no nulo. Por la división euclídea, podemos encontrar $q, r \in A[X]$ tales que $f = (X - \alpha)q + r$, con $\deg(r) < 1$. Evaluando esta igualdad en α, tenemos que $f(\alpha) = r$. Así, si $f(\alpha) = 0$, entonces $(X - \alpha)|f$.

Recíprocamente, si $X - \alpha$ es un divisor de f, entonces existe $c \in A[X]$ tal que $f = (X - \alpha)c$. Evaluando en α, obtenemos $f(\alpha) = 0$.

Decimos que α es una *raíz* de f si $f(\alpha) = 0$ o, equivalentemente, según hemos visto, si $(X - \alpha)|f$.

PROPOSICIÓN 3.30. *Dados $a, b \in A$, donde A es un dominio de integridad, las siguientes condiciones son equivalentes.*

(I) $a|b$ *y* $b|a$;
(II) Existe $u \in U(A)$ *tal que* $a = ub$;
(III) $\langle a \rangle = \langle b \rangle$.

DEMOSTRACIÓN. De acuerdo con el Ejercicio 62, $a|b$ si, y sólo si, $\langle b \rangle \subseteq \langle a \rangle$. Esto da la equivalencia (I) $\Leftrightarrow$ (III)

(I) $\Rightarrow$ (II). Por hipótesis, existen $c, d \in A$ tales que $b = ca$ y $a = db$. Entonces $a = cda$. Por tanto, $a(1 - cd) = 0$. Como A es un dominio de integridad, tenemos que, o bien $a = 0$, o bien $1 - cd = 0$. En el primer caso, $b = 0$ y $a = 0 = 1 \cdot 0 = 1b$. Tomando $u = 1$, tenemos (II). En el segundo, $1 = cd$ y, por tanto, $c, d \in U(A)$. Tomando $u = d$, tenemos (II).

(II) $\Rightarrow$ (I). Como $a = ub$, tenemos que $b|a$. Pero $b = u^{-1}a$, por lo que $a|b$. □

DEFINICIÓN 3.31. Dos elementos $a, b \in A$, donde A es un DI, se dicen *asociados* si satisfacen cualesquiera de las condiciones equivalentes de la Proposición 3.30. Usaremos, en este contexto, la notación $a \sim b$. La condición (III) de la Proposición 3.30 muestra que $\sim$ es una relación de equivalencia en A.

EJERCICIO 63. Para un dominio de integridad A, consideremos la relación de equivalencia $\sim$ "ser asociados". Denotemos, para $a \in A$, por $[a]$ su clase de equivalencia en el conjunto cociente $A/\!\sim$. Razonar que $[0] = \{0\}$ y que $[1] = U(A)$. Deducir que A es un cuerpo si, y sólo si, $A/\!\sim\, = \{[0], [1]\}$.

EJERCICIO 64. Sea A un DI y $A/\!\sim$ el conjunto cociente bajo la relación "ser asociados" $\sim$. Demostrar que la operación en $A/\!\sim$ dada por $[a][b] = [ab]$ para $[a], [b] \in A/\!\sim$ está bien definida y que, con esta operación, $A/\!\sim$ es un monoide conmutativo. Deducir que

$$\widetilde{A} = \{[a] \in A/\!\sim\ \mid a \neq 0\}$$

es un submonoide de $A/\!\sim$.

EJERCICIO 65. Demostrar que, si A es un DI, entonces $U(A[X]) = U(A)$.

DEFINICIÓN 3.32. Sean $a_1, \dots, a_n \in A$, donde A es un dominio de integridad. Diremos que $d \in A$ es un *divisor común* de $a_1, \dots, a_n$ si $d|a_1, \dots, d|a_n$.

Un divisor común d de $a_1, \dots, a_n$ se llama *máximo común divisor* de $a_1, \dots, a_n$ si se tiene que cualquier otro divisor común d' de $a_1, \dots, a_n$, ha de verificar que $d'|d$.

LEMA 3.33. *Sean* $a_1, \ldots, a_n \in A$*, donde* A *es un DI,* $d \in A$*. Entonces* d *es un máximo común divisor de* $a_1, \ldots, a_n$ *si, y sólo si,* $\langle d \rangle$ *es mínimo, para la inclusión, entre todos los ideales principales de* A *que contienen a* $\langle a_1, \ldots, a_n \rangle$*.*

Como consecuencia, si d *es un máximo común divisor de* $a_1, \ldots, a_n$*, entonces el conjunto de todos los máximos comunes divisores de* $a_1, \ldots, a_n$ *es la clase de equivalencia* $[d] \in A/\!\sim$*, es decir, el conjunto de los elementos asociados a* d*. Por* $\mathrm{mcd}(a_1, \ldots, a_n)$ *se denotará cualquiera de estos elementos.*

DEMOSTRACIÓN. Observemos que, si $a \in A$, entonces a es un común divisor de $a_1, \ldots, a_n$ si, y sólo si, $\langle a_1, \ldots, a_n \rangle \subseteq \langle a \rangle$.

Supongamos que d es un mcd de $a_1, \ldots, a_n$, y d' es tal que $\langle a_1, \ldots, a_n \rangle \subseteq \langle d' \rangle$. Como d' es un divisor común de $a_1, \ldots, a_n$, deducimos que $d'|d$. Por tanto, $\langle d \rangle \subseteq \langle d' \rangle$, y $\langle d \rangle$ resulta ser mínimo entre los ideales principales de A que contienen a $\langle a_1, \ldots, a_n \rangle$. El razonamiento para demostrar el recíproco es igual de sencillo.

Ahora, dado un mcd d de $a_1, \ldots, a_n$, entonces $d' \in A$ es mcd de $a_1, \ldots, a_n$ si, y sólo si, $\langle d \rangle = \langle d' \rangle$. De acuerdo con la Proposición 3.30, esto es equivalente a decir que d y d' son asociados. □

PROPOSICIÓN 3.34. *Si* $a_1, \ldots, a_n \in A$*, para* A *un dominio de ideales principales, entonces existe un máximo común divisor de* $a_1, \ldots, a_n$*. De hecho,* $d = \mathrm{mcd}(a_1, \ldots, a_n)$ *precisamente para aquellos* $d \in A$ *tales que* $\langle a_1, \ldots, a_n \rangle = \langle d \rangle$*.*

DEMOSTRACIÓN. Como A es un DIP, $\langle a_1, \ldots, a_n \rangle = \langle d \rangle$ para algún $d \in A$. Se sigue del Lemma 3.33 que $d = \mathrm{mcd}(a_1, \ldots, a_n)$. □

El siguiente corolario se sigue inmediatamente.

COROLARIO 3.35 (Identidad de Bezout). *Sean* $a, b \in A$*, donde* A *es un DIP, y* $d = \mathrm{mcd}(a, b)$*. Existen* $u, v \in A$ *tales que* $d = ua + vb$*.*

EJERCICIO 66. Supongamos $a, b, c \in A$, donde A es un DI, tales que los máximos comunes divisores involucrados en la igualdad

$$\mathrm{mcd}(\mathrm{mcd}(a, b), c) = \mathrm{mcd}(a, \mathrm{mcd}(b, c))$$

existen. Demostrar que la citada igualdad es correcta.

Vayamos con el mínimo común múltiplo. Primero, lo definiremos en un dominio de integridad cualquiera, y luego veremos que siempre existe cuando manejamos elementos de un DIP.

DEFINICIÓN 3.36. Sean $a_1, \ldots, a_n \in A$, donde A es un dominio de integridad. Diremos que $m \in A$ es un múltiplo común de $a_1, \ldots, a_n$ si $a_1|m, \ldots, a_n|m$. Un *mínimo común múltiplo* de $a_1, \ldots, a_n$ es un múltiplo común m de $a_1, \ldots, a_n$ y tal que si m' es cualquier otro múltiplo común de $a_1, \ldots, a_n$, entonces $m|m'$.

LEMA 3.37. *Sean* $a_1, \ldots, a_n \in A$*, donde* A *es un DI. Un elemento* m *de* A *es un mínimo común múltiplo de* $a_1, \ldots, a_n$ *si, y sólo si,* $\langle m \rangle$ *es máximo, para la inclusión, entre todos los ideales principales de* A *contenidos en* $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle$*.*

Como consecuencia, si m *es un mínimo común múltiplo de* $a_1, \ldots, a_n$*, entonces el conjunto de todos los mínimos comunes múltiplos de* $a_1, \ldots, a_n$ *es la clase de equivalencia* $[m] \in A/\!\sim$*, es decir, el conjunto de los elementos asociados a* m*. Por* $\mathrm{mcm}(a_1, \ldots, a_n)$ *se denotará cualquiera de estos elementos.*

DEMOSTRACIÓN. Observemos que, si $a \in A$, entonces a es un común múltiplo de $a_1, \dots, a_n$ si, y sólo si, $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle \supseteq \langle a \rangle$. Supongamos que m es un mcm de $a_1, \dots, a_n$, y m' es tal que $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle \supseteq \langle m' \rangle$. Como m' es un múltiplo común de $a_1, \dots, a_n$, deducimos que $m | m'$. Por tanto, $\langle m' \rangle \subseteq \langle m \rangle$, y $\langle m \rangle$ es, por tanto, máximo entre los ideales principales de A contenidos en $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle$. El razonamiento para demostrar el recíproco es igual de sencillo.

Ahora, dado un mcm m de $a_1, \dots, a_n$, entonces $m' \in A$ es mcm de $a_1, \dots, a_n$ si, y sólo si, $\langle m \rangle = \langle m' \rangle$. De acuerdo con la Proposición 3.30, esto es equivalente a decir que m y m' son asociados. □

PROPOSICIÓN 3.38. *Si* $a_1, \dots, a_n \in A$ *para* A *es un dominio de ideales principales, entonces existe un mínimo común múltiplo de* $a_1, \dots, a_n$. *De hecho,* $m = \mathrm{mcm}(a_1, \dots, a_n)$ *precisamente para aquellos* $m \in A$ *tales que* $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle = \langle m \rangle$.

DEMOSTRACIÓN. Como A es un DIP, $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle = \langle m \rangle$ para algún $m \in A$. Se sigue del Lema 3.33 que $m = \mathrm{mcm}(a_1, \dots, a_n)$. □

EJERCICIO 67. Supongamos $a, b, c \in A$, donde A es un DI, tales que los mínimos comunes múltiplos involucrados en la igualdad

$$\mathrm{mcm}(\mathrm{mcm}(a, b), c) = \mathrm{mcm}(a, \mathrm{mcm}(b, c))$$

existen. Demostrar que la citada igualdad es correcta.

Elementos irreducibles y primos. Una de las cualidades más interesantes de un DIP es que, a partir de él, pueden construirse muchos cuerpos. En particular, podemos aplicar esta idea a $K[X]$, donde K es un cuerpo dado. Veamos primero una definición importante.

DEFINICIÓN 3.39. Un elemento a de un DI A se dirá *irreducible* si $a \neq 0$, $a \notin U(A)$ y para cualquier factorización $a = bc$, con $b, c \in A$, se tiene que, o bien $b \in U(A)$, o bien $c \in U(A)$.

EJEMPLO 3.40. Los elementos irreducibles de $\mathbb{Z}$ son los números naturales primos y sus opuestos.

EJEMPLO 3.41. Si K es un cuerpo, entonces todo polinomio $f \in K[X]$ de grado 1 (éstos se llaman *lineales*) es irreducible. En efecto, si $\deg(f) = 1$ y $f = gh$ para $g, h \in K[X]$, entonces $1 = \deg(g) + \deg(h)$. Por tanto, o bien $\deg(g) = 0$, o bien $\deg(h) = 0$. Esta disyunción se traduce en que o bien $g \in K \setminus \{0\}$ o bien $h \in K \setminus \{0\}$. Como $U(K[X]) = U(K) = K \setminus \{0\}$, concluimos que f es irreducible.

Para la identificación de los polinomios irreducibles en $K[X]$ de grados 2 y 3, ver Ejercicio 72.

EJEMPLO 3.42. Vamos a demostrar que $X^2 + 1$ es irreducible en $\mathbb{R}[X]$. La única manera de no serlo, es poder factorizarlo como $X^2 + 1 = gh$, para g y h polinomios lineales. Supongamos que $g = aX + b$, con $a, b \in \mathbb{R}$ y $a \neq 0$. Entonces $\alpha = -b/a \in \mathbb{R}$ es una raíz de g y, por tanto, de $X^2 + 1$. Así que $\alpha^2 + 1 = 0$, lo que es imposible, porque $\alpha^2 \geq 0$.

Observemos que el polinomio $(X^2 + 1)^2 \in \mathbb{R}[X]$ no tiene raíces en $\mathbb{R}$ a pesar de ser reducible.

DEFINICIÓN 3.43. Un elemento p de un DI A se llama *primo* si $p \neq 0$, $p \notin U(A)$ y siempre que $p | ab$ para $a, b \in A$, entonces $p | a$ o $p | b$.

EJERCICIO 68. Demostrar que si p es un elemento no nulo de un dominio de integridad A, entonces p es primo si, y sólo si, $A/\langle p\rangle$ es un dominio de integridad.

LEMA 3.44. *Todo elemento primo de un DI es irreducible.*

DEMOSTRACIÓN. Supongamos que p es un elemento primo de un dominio de integridad A, y consideremos una factorización $p = bc$ con $b, c \in A$. Entonces $p|b$ o $p|c$. En el primer caso, la Proposición 3.30 asegura que $b = up$, para cierto $u \in U(A)$. Por tanto, $p = upc$, luego, cancelando p, obtenemos $1 = uc$ y $c \in U(A)$. Si $p|c$, obtenemos, con igual argumento, que $b \in U(A)$. Así que p es irreducible. □

TEOREMA 3.45. *Sea $0 \neq p \in A$, donde A es un DIP. Las siguientes afirmaciones son equivalentes.*

(I) $A/\langle p\rangle$ *es un cuerpo.*
(II) $A/\langle p\rangle$ *es un dominio de integridad.*
(III) p *es primo.*
(IV) p *es irreducible.*

DEMOSTRACIÓN. Primero, observemos que todas las afirmaciones entrañan que $p \notin U(A)$ (recordemos que tanto DI como cuerpos son no triviales, por definición).

(I) ⇒ (II). Evidente.

(II) ⇒ (III). Ejercicio 68.

(III) ⇒ (IV). Lema 3.44.

(IV) ⇒ (I). Si p es irreducible y tomamos $b + \langle p\rangle \in A/\langle p\rangle$ distinto de cero, entonces $b \notin \langle p\rangle$. Tomemos $d = \mathrm{mcd}(p, b)$, que existe por ser A un DIP. Como p es irreducible, deducimos que, o bien d es asociado a p, o bien $d \in U(A)$. En el primer caso, $p|b$, lo que implica que $b \in \langle p\rangle$. Así que hemos de admitir que $d \in U(A)$. Por tanto, $1 = \mathrm{mcd}(p, b)$ (recordemos que esta notación significa "1 es un mcd de p y b"). Por Bezout[2], existen $u, v \in A$ tales que $1 = pu + bv$. Luego, en $A/\langle p\rangle$, $b + \langle p\rangle$ tiene como inverso multiplicativo a $v + \langle p\rangle$. Esto demuestra que $A/\langle p\rangle$ es un cuerpo. □

Números complejos. El Teorema 3.45 permite obtener muchos nuevos sistemas numéricos, como es el caso del cuerpo de los números complejos que vamos a construir a partir del de los números reales.

EJEMPLO 3.46. Estamos en condiciones de afirmar, en vista del Ejemplo 3.42 y del Teorema 3.45, que $C = \mathbb{R}[X]/\langle X^2 + 1\rangle$ es un cuerpo.

Observemos que, si $f + \langle X^2 + 1\rangle$ es cualquier elemento de tal cuerpo, entonces, por división euclídea, $f = (X^2+1)q+r$, con $r = aX+b$ para ciertos $a, b \in \mathbb{R}$. Así, cualquier elemento de C se expresa en la forma

$$a + bX + \langle X^2 + 1\rangle = a + \langle X^2 + 1\rangle + (b + \langle X^2 + 1\rangle)(X + \langle X^2 + 1\rangle). \tag{3.7}$$

Ahora, la aplicación $\iota : \mathbb{R} \to C$ que lleva $r \in \mathbb{R}$ en $\iota(r) = r + \langle X^2 + 1\rangle$ es un homomorfismo inyectivo de anillos. Así que podemos identificar $\mathbb{R}$ como un subanillo de C, con lo que el miembro de la derecha de 3.7 deviene, bien entendida esta identificación,

$$a + b(X + \langle X^2 + 1\rangle).$$

Si escribimos $i = X + \langle X^2 + 1\rangle$, tenemos que cada elemento de C se escribe en la forma $a + bi$, para $a, b \in \mathbb{R}$. Además,

$$i^2 = (X + \langle X^2 + 1\rangle)^2 = X^2 + \langle X^2 + 1\rangle = -1 + \langle X^2 + 1\rangle = -1,$$

[2] Y aquí es donde se usa definitivamente que A es un DIP.

Quienes conozcan el cuerpo de los números complejos, lo habrán reconocido en C. Usaremos, por tanto, la notación $\mathbb{C} = C$, para este cuerpo.

Hemos visto que, con las simplificaciones notacionales hechas, cada elemento de $\mathbb{C}$ se expresa como $a+bi$, para $a, b \in \mathbb{R}$ y que $i^2 = -1$. Usando las propiedades asociativas, conmutativas y distributiva de las operaciones de $\mathbb{C}$, tenemos que

$$(a+bi)(c+di) = ac - bd + (ad+bc)i;$$

la multiplicación de números complejos.

Convenzámonos de que la expresión $a+bi$, con $a, b \in \mathbb{R}$, de cada número complejo, es única. Si $a+bi = a'+b'i$ entonces $a - a' + (b-b')i = 0$. Esto lleva a que $a - a' + (b-b')X \in \langle X^2+1 \rangle$. Mirando grados, esto es sólo posible si $a - a' + (b-b')X = 0$ en $\mathbb{R}[X]$. O sea, $a = a'$, y $b = b'$.

El cuerpo $\mathbb{C}$ es fundamental en la Ciencia, así que demos algunas propiedades básicas del mismo. Dado un número complejo $z = a + bi$, con $a, b \in \mathbb{R}$, a se llama *parte real* de z y b se llama *parte imaginaria*. El número $\bar{z} = a - bi$ se llama *conjugado* de z.

Una propiedad reseñable es que la aplicación $\overline{(-)} : \mathbb{C} \to \mathbb{C}$ que lleva cada z en su conjugado $\bar{z}$ es un isomorfismo de anillos[3], que deja fijos los números reales. Es un ejercicio fácil comprobar esto. Obviamente, $\overline{(-)}$ es su propio inverso para la composición. Además,

$$z\bar{z} = a^2 + b^2,$$

es claramente un número real no negativo. Definimos el *módulo* de z como $|z| = \sqrt{z\bar{z}}$. Este módulo mide la longitud del vector de componentes (a, b) del plano real. Vemos que $z = 0$ si, y sólo si, $|z| = 0$. De la ecuación $z\bar{z} = |z|^2$ extraemos, para $z \neq 0$, la fórmula

$$z^{-1} = \frac{\bar{z}}{|z|^2},$$

con la que se suele calcular el inverso multiplicativo de un número complejo.

Ejercicios.

EJERCICIO 69. Sean $a, b, x, y \in A$, con A un DIP, tales que $xa = yb$. Demostrar que, si $\mathrm{mcd}(x, y) = 1$, entonces $\mathrm{mcm}(a, b) = ax$. (Sugerencia: usar la identidad de Bezout).

EJERCICIO 70. Demostrar que $\mathbb{R}[X]/\langle X^2 - 1 \rangle$ es un anillo isomorfo al anillo producto $\mathbb{R} \times \mathbb{R}$.

EJERCICIO 71. Sea A un anillo conmutativo no trivial e I un ideal de A, $I \neq A$. Decimos que I es *maximal* si para cualquier J ideal de A tal que $I \subsetneq J$, entonces $J = A$. Demostrar que I es un ideal maximal si, y sólo si, A/I es un cuerpo.

EJERCICIO 72. Sea K un cuerpo. Dado un polinomio $f \in K[X]$ cuyo grado es 2 o 3, demostrar que f es irreducible si, y sólo si, f tiene una raíz en K.

EJERCICIO 73. Construir cuerpos con 4 y 8 elementos.

EJERCICIO 74. Sea $m \in A$, con $m \neq 0$, donde A es un DIP. Sea $a \in A$. Demostrar que $a + \langle m \rangle \in U(A/\langle m \rangle)$ si, y sólo si, $\mathrm{mcd}(a, m) = 1$.

[3]se suele decir que es un automorfismo de cuerpos

3.4. Dominios Euclídeos

Un dominio euclídeo es un dominio de integridad que disfruta de una división con resto análoga a la de números enteros o polinomios. Seguidamente, damos la definición técnica. Recordemos que, para un anillo A, escribimos $A^* = A \setminus \{0\}$.

DEFINICIÓN 3.47. Sea A un dominio de integridad. Una *función euclídea* en A es una aplicación $\phi : A^* \to \mathbb{N}$ que satisface las siguientes condiciones:

1. Si $a, b \in A^*$ y $a|b$ entonces $\phi(a) \leq \phi(b)$.
2. Dados $a, b \in A$ con $b \neq 0$, existen $q, r \in A$ tales que $a = qb + r$, donde $r = 0$ o bien $\phi(r) < \phi(b)$.

La segunda condición establece que, en A, existe una división con resto.

Si A viene dotado de una función euclídea, diremos que A es un *dominio euclídeo* (abreviatura *DE*).

EJEMPLO 3.48. El anillo $\mathbb{Z}$ de los números enteros en un dominio euclídeo con la función euclídea valor absoluto.

EJEMPLO 3.49. Si K es un cuerpo, entonces la aplicación que asigna a cada polinomio no nulo de $K[X]$ su grado es una función euclídea. Por tanto, $K[X]$ es un dominio euclídeo.

EJEMPLO 3.50. Cualquier cuerpo K es un dominio euclídeo con la función euclídea constantemente 0 sobre los elementos de K^*. Este ejemplo no es demasiado interesante, claro.

En esta sección, nos disponemos a dar algunos ejemplos más de dominios euclídeos. Pero, antes, veamos qué ventajas da el disponer de una función euclídea.

OBSERVACIÓN 3.51. Sean $a, b \in A$ con $b \neq 0$, para A un DE con función euclídea ϕ. Si $a = qb + r$ es una división con resto en A, entonces $b|a$ si, y sólo si, $r = 0$. En efecto, si $r = 0$, obviamente $b|a$. Recíprocamente, supongamos que $b|a$, y sea $c \in A$ tal que $a = cq$. Entonces $0 = (q - c)b + r$. Si $r \neq 0$, entonces $\phi(r) = \phi((c - q)b) \geq \phi(b)$, lo que es una contradicción. Por tanto, $r = 0$.

TEOREMA 3.52. *Todo dominio euclídeo es un dominio de ideales principales.*

DEMOSTRACIÓN. Sea A un DE con función euclídea ϕ, e I un ideal no nulo de A. Pongamos $n = \min\{\phi(a) \mid 0 \neq a \in I\}$. Si tomamos $0 \neq g \in I$ con $n = \phi(g)$, es fácil ver, mediante la realización de una división con resto, de manera similar a la demostración del Teorema 3.27, que $I = \langle g \rangle$. □

Por tanto, en un DE, hay máximo común divisor y mínimo común múltiplo de cualquier conjunto finito de elementos. Además, se tiene la identidad de Bezout. La novedad ahora es que, si la división con resto es realizable en la práctica, entonces los coeficientes de la indentidad de Bezout se pueden calcular mediante la versión general del Algoritmo Extendido de Euclides (Algoritmo 4).

Para a, b elementos del dominio euclídeo A con función euclídea Φ, con $b \neq 0$, los elementos $q, r \in A$ tales que $a = qb + r$ con $r = 0$ o $\phi(r) < \phi(b)$ se llaman, respectivamente, *cociente* y *resto* de la división. Escribiremos $r = \mathrm{rem}(a, b)$ y $q = \mathrm{quot}(a, b)$, bien entendido que dichos elementos no son, en general, únicos.

Algoritmo 4 `Algoritmo Extendido de Euclides para un DE`

Input: $a, b \in A$ con $b \neq 0$, donde A es un dominio euclídeo.
Output: $\{u_i, v_i, r_i\}_{i=0,\dots,h,h+1}$ tales que $r_i = au_i + bv_i$ para $i = 0, 1, \dots, h, h+1$,
$r_{h+1} = 0$,
$r_h = \mathrm{mcd}(a, b)$,
$u_{h+1} a = \mathrm{mcm}(a, b)$.
Initialitation:
$r_0 \leftarrow a$, $r_1 \leftarrow b$.
$u_0 \leftarrow 1$, $u_1 \leftarrow 0$.
$v_0 \leftarrow 0$, $v_1 \leftarrow 1$.
$q \leftarrow 0$, $r \leftarrow 0$.
$i \leftarrow 1$.
while $r_i \neq 0$ **do**
  $q \leftarrow \mathrm{quot}(r_{i-1}, r_i)$
  $r \leftarrow \mathrm{rem}(r_{i-1}, r_i)$
  $r_{i+1} \leftarrow r$
  $u_{i+1} \leftarrow u_{i-1} - u_i q$
  $v_{i+1} \leftarrow v_{i-1} - v_i q$
  $i \leftarrow i + 1$
return $\{u_i, v_i, r_i\}_{i=0,\dots,h,h+1}$

TEOREMA 3.53. *El Algoritmo 4 es correcto.*

DEMOSTRACIÓN. Observemos que, siempre que $r_i \neq 0$, se tiene que, o bien $r_{i+1} = 0$ o bien $\phi(r_{i+1}) < \phi(r_i)$. Así que existe $h \geq 1$ tal que $r_h \neq 0$ pero $r_{h+1} = 0$.

Para $i \leq h$, tenemos que $r_i \neq 0$, luego podemos hacer uso de la división con resto en A

$$r_{i-1} = q_{i+1} r_i + r_{i+1},$$

donde q_{i+1} es el cociente. De aquí, los divisores comunes de r_{i-1} y r_i son los mismos que los divisores comunes de r_i y r_{i+1}. Así que

$$r_h = \mathrm{mcd}(0, r_h) = \mathrm{mcd}(r_{h+1}, r_h) = \\ \mathrm{mcd}(r_h, r_{h-1}) = \cdots = \mathrm{mcd}(r_1, r_0) = \mathrm{mcd}(b, a).$$

Vamos a definir los elementos $u_i, v_i \in A$, $i = 0, 1, \dots, h, h+1$. Tomamos

$$u_0 = 1, v_0 = 0, u_1 = 0, v_1 = 1,$$

Una vez dados $u_i, v_i, u_{i-1}, v_{i-1}$, para $1 \leq i \leq h$, definimos

$$u_{i+1} = u_{i-1} - q_{i+1} u_i, \qquad v_{i+1} = v_{i-1} - q_{i+1} v_i.$$

Así,

$$u_{i+1} a + v_{i+1} b = (u_{i-1} - q_{i+1} u_i) a + (v_{i-1} - q_{i+1} v_i) b = \\ u_{i-1} a + v_{i-1} b - q_{i+1}(u_i a + v_i b) = r_{i-1} - q_{i+1} r_i = r_{i+1}.$$

Veamos, por último, que $u_{h+1} a = \mathrm{mcm}(a, b)$. Observemos primero que

$$0 = r_{h+1} = u_{h+1} a + v_{h+1} b,$$

luego $u_{h+1} a = -v_{h+1} b$, así que $u_{h+1} a$ es múltiplo común de a y b.

Con objeto de razonar que $u_{h+1} a = \mathrm{mcm}(a, b)$, demostremos que

$$-u_{i+1} v_i + u_i v_{i+1} = (-1)^i$$

para todo $0 \leq i \leq h$. Dicha igualdad es clara para $i = 0$. Si $1 \leq i \leq h$, supuesta la igualdad demostrada parar $i-1$, tenemos

$$-u_{i+1}v_i+u_iv_{i+1} = -(u_{i-1}-q_iu_i)v_i+u_i(v_{i-1}-q_iv_i) = -u_{i-1}v_i+u_iv_{i-1} = (-1)^i.$$

En particular, $u_{h+1}v_h - u_hv_{h+1} = (-1)^h$. De aquí, $\mathrm{mcd}(u_{h+1}, v_{h+1}) = 1$.

Por el Ejercicio 69, $\mathrm{mcm}(a, b) = au_{h+1}$. □

3.4.1. Nuevos ejemplos de DE. Seguidamente, vamos a ver algunos ejemplos adicionales de dominios euclídeos, que proceden del ámbito de la Teoría de Números.

Tomemos $D \in \mathbb{Z}$ que no es un cuadrado. Esto último significa que $D \neq a^2$ para todo $a \in \mathbb{Z}$.

Definimos

$$\mathbb{Q}(\sqrt{D}) = \{x + y\sqrt{D} \mid x, y \in \mathbb{Q}\},$$

que es un subanillo[4] de $\mathbb{C}$. Notemos que, si $D < 0$, $\sqrt{D} = i\sqrt{-D}$, donde ésta última es la raíz cuadrada positiva real de $-D > 0$. Por ejemplo, $\sqrt{-2} = i\sqrt{2}$. También consideraremos

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\},$$

que es un subanillo[5] de $\mathbb{Q}(\sqrt{D})$. Para algunos valores de D, se trata de un dominio euclídeo. Queremos conocer algunos de ellos.

LEMA 3.54. *Si* $x + y\sqrt{D} = 0$ *para* $x, y \in \mathbb{Q}$, *entonces* $x = y = 0$.

DEMOSTRACIÓN. Si $x = 0$, entonces $y\sqrt{D} = 0$, lo que implica, puesto que $\sqrt{D} \neq 0$, que $y = 0$. La estrategia es, así, demostrar que si $x \neq 0$, entonces llegamos a una contradicción. Tendremos entonces que $\sqrt{D} = yx^{-1} \in \mathbb{Q}$, por lo que D es el cuadrado de un número racional. Esto no es posible por el Ejercicio 27.

□

Definimos la *norma* de $x + y\sqrt{D}$ como

$$N(x + y\sqrt{D}) = x^2 - y^2D \in \mathbb{Q}.$$

Observemos que, si escribimos $z = x+y\sqrt{D}$, y denotamos por $\overline{z} = x-y\sqrt{D}$, entonces podemos reescribir la norma de z como

$$N(z) = z\overline{z}.$$

Observemos que, para $D < 0$, $\overline{z}$ es el conjugado, en tanto que número complejo, de z. Pero, para $D > 0$, esto no es así. Esperemos que esta comodidad en la notación no os lleve a confusión...

EJERCICIO 75. Demostrar que la aplicación $\alpha : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}(\sqrt{D})$ definida por $\alpha(z) = \overline{z}$ para todo $z \in \mathbb{Q}(\sqrt{D})$ es un automorfismo de anillos. Deducir que $N(zw) = N(z)N(w)$ para todo $z, w \in \mathbb{Q}(\sqrt{D})$.

LEMA 3.55. *Sea* $z \in \mathbb{Q}(\sqrt{D})$. *Entonces* $z = 0$ *si, y sólo si,* $N(z) = 0$.

DEMOSTRACIÓN. Pongamos $z = x + y\sqrt{D}$. Si $z = 0$, entonces, por el Lema 3.54, $x = y = 0$ y, por tanto, $N(z) = 0$. Recíprocamente, si $N(z) = 0$, entonces $z\overline{z} = 0$. Esto implica que, o bien $z = 0$, o bien $\overline{z} = 0$. En el segundo caso, $x - y\sqrt{D} = 0$, lo que implica, de nuevo por el Lema 3.54, que $x = y = 0$. □

[4]Comprobar. Algo más adelante, veremos que, de hecho, se trata de un subcuerpo.

[5]Comprobar.

Como consecuencia del Lema 3.55, si $z \in \mathbb{Q}(\sqrt{D})$ es no nulo, su inverso en $\mathbb{C}$ se calcula por la fórmula

$$z^{-1} = \frac{\bar{z}}{N(z)}. \tag{3.8}$$

De manera que, si $z \in \mathbb{Q}(\sqrt{D})$ es no nulo, entonces $z^{-1} \in \mathbb{Q}(\sqrt{D})$, y este anillo es un cuerpo. El subanillo $\mathbb{Z}[\sqrt{D}]$ es un dominio de integridad, pero no un cuerpo, como resultará evidente tras ver la siguiente proposición.

PROPOSICIÓN 3.56. *Definamos, para* $z \in \mathbb{Z}[\sqrt{D}]$, $\phi(z) = |N(z)|$, *donde* $|\ |$ *denota el valor absoluto. Se tiene que* $U(\mathbb{Z}[\sqrt{D}]) = \{z \in \mathbb{Z}[\sqrt{D}] \mid \phi(z) = 1\}$.

DEMOSTRACIÓN. Si $\phi(z) = 1$, entonces $N(z) = 1$ o $N(z) = -1$. De la ecuación (3.8), deducimos que $z^{-1} \in \mathbb{Z}[\sqrt{D}]$, luego z es una unidad. Recíprocamente, supongamos que $z \in \mathbb{Z}[\sqrt{D}]$, y sea $u \in \mathbb{Z}[\sqrt{D}]$ tal que $1 = zu$. Así, $1 = \phi(1) = \phi(z)\phi(u)$. Como $\phi(z), \phi(u) \in \mathbb{N}$, deducimos que $\phi(z) = 1$. □

TEOREMA 3.57. *La función* $\phi : \mathbb{Z}[\sqrt{D}]^* \to \mathbb{N}$ *es una función euclídea para* $D = -2, -1, 2, 3$.

DEMOSTRACIÓN. Primero, observemos que, si $z', w' \in \mathbb{Z}[\sqrt{D}]^*$ y $z'|w'$, entonces $w' = vz'$ para algún $v \in \mathbb{Z}[\sqrt{D}]$. Así, $\phi(w') = \phi(v)\phi(z') \geq \phi(z')$, puesto que $\phi(v) \geq 1$.

Vayamos ahora con la división con resto. Tomemos ahora $w, z \in \mathbb{Z}[\sqrt{D}]$ cualesquiera con $z \neq 0$. Una consecuencia de (3.8) es que $wz^{-1} = x + y\sqrt{D}$ para ciertos $x, y \in \mathbb{Q}$. Sean $a, b \in \mathbb{Z}$ tales que $|x - a| \leq 1/2$ e $|y - b| \leq 1/2$, y definamos

$$q = a + b\sqrt{D} \quad \text{y} \quad r = w - qz.$$

Obviamente, $q, r \in \mathbb{Z}[\sqrt{D}]$. Ahora,

$$\begin{aligned} |N(rz^{-1})| &= |N((w - qz)z^{-1})| = |N(wz^{-1} - q)| \\ &= |N(x - a + (y - b)\sqrt{D})| = |(a - x)^2 - (b - y)^2 D|. \end{aligned}$$

Distingamos casos. Si $D = -2, -1$, entonces

$$|N(rz^{-1})| = (a - x)^2 - (b - y)^2 D \leq \frac{1}{4} - \frac{1}{4}D < 1.$$

Si $D = 2$, tenemos que

$$|N(rz^{-1})| = |(a - x)^2 - 2(b - y)^2| \leq |a - x|^2 + 2|b - y|^2 \leq \frac{1}{4} + \frac{2}{4} < 1.$$

Si $D = 3$, entonces

$$|N(rz^{-1})| = |(a-x)^2 - 3(b-y)^2| = \begin{cases} (a - x)^2 - 3(b - y)^2 & \text{si } (a - x)^2 \geq 3(b - y)^2 \\ 3(b - y)^2 - (a - x)^2 & \text{si } 3(b - y)^2 \geq (a - x)^2. \end{cases}$$

Como el primer valor es menor o igual que $1/4$, y el segundo menor o igual que $3/4$, tenemos que ambos valores son estrictamente menores que 1, claro.

En definitiva, $|N(rz^{-1})| < 1$ para los valores $D = -2, -1, 2, 3$. Pero

$$|N(rz^{-1})| = |N(r)N(z^{-1})| = |N(r)||N(z)|^{-1} = \phi(r)\phi(z)^{-1}.$$

Por tanto, $\phi(r) < \phi(z)$. □

EJEMPLO 3.58. Tomemos $D = -1$. Usamos la notación tradicional es $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. Este es el anillo de los *enteros de Gauss*. En $\mathbb{Z}[i]$, vamos a dividir $w = 3$ entre $z = 1 + i$. Tenemos

$$\frac{3}{1+i} = \frac{3(1-i)}{(1+i)(1-i)} = \frac{-3i+3}{2} = \frac{3}{2} - \frac{3}{2}i.$$

Tomamos $q = 1 - i$, con lo que $r = w - qz = 3 - (1-i)(1+i) = 1$.

3.5. Ecuaciones en congruencias en un DE

Hemos visto que, en un dominio euclídeo, disponemos de una división y un algoritmo extendido de Euclides. Esto abre la posibilidad de usar procedimientos formalmente idénticos a los usados en $\mathbb{Z}$ para la resolución de ecuaciones y sistemas de ecuaciones en congruencias, así como ecuaciones "diofánticas". Vamos, para no aburrirnos, a hacer una exposición algo diferente que entonces.

PROPOSICIÓN 3.59. *Sean* $a, b, c \in A$*, donde* A *es un DIP. La ecuación*

$$ax + by = c \tag{3.9}$$

en las incógnitas x, y *tiene solución en* A *si, y sólo si,* $\operatorname{mcd}(a, b)$ *divide a* c.

DEMOSTRACIÓN. Observemos que (3.9) tiene solución en A si, y sólo si, $c \in \langle a \rangle + \langle b \rangle$. Como $\langle a \rangle + \langle c \rangle = \langle d \rangle$ para $d = \operatorname{mcd}(a, c)$, obtenemos que (3.9) tiene solución si, y sólo si, $c \in \langle d \rangle$. □

Consideremos ahora la ecuación en congruencias en un DIP A:

$$ax \equiv b \pmod{m}, \tag{3.10}$$

donde $a, b, m \in A$, con $m \neq 0$. Aquí, $a \equiv b \pmod{m}$ es una abreviatura de la notación general $a \equiv b \pmod{\langle m \rangle}$ introducida en (2.7).

PROPOSICIÓN 3.60. *La congruencia* (3.10) *tiene solución en* A *si, sólo si, la ecuación* $ax + my = b$ *tiene solución en* A*. Como consecuencia, una condición necesaria y suficiente para que* (3.10) *tenga solución es que* $\operatorname{mcd}(a, m)$ *es un divisor de* b.

DEMOSTRACIÓN. Resolver la ecuación (3.10) es calcular todos los $x \in A$ que la satisfacen. Observemos que x es una solución de (3.10) si y sólo si existe $k \in A$ tal que $ax - b = km$. Equivalentemente, $ax - km = b$. El criterio para la existencia de solución se sigue ahora de la Proposición 3.59. □

Supongamos ahora que A es un DE, lo que permite usar el Algoritmo 4 para calcular la solución general de (3.10). Efectivamente, podemos calcular $d = \operatorname{mcd}(a, m)$, y $u, v \in A$ tales que $d = au + mv$. En caso de existir solución de (3.10), calculamos $a', b' \in A$ y $m' \in \mathbb{N}$ tales que $a = a'd$, $b = b'd$, $m = m'd$. Así, $ax - km = b$ es equivalente a $a'x - b' = km'$, esto es, (2.8) es equivalente a

$$a'x \equiv b' \pmod{m'}. \tag{3.11}$$

La ventaja ahora es que $1 = a'u + m'v$, y, en $A/\langle m' \rangle$, tenemos que

$$(u + \langle m' \rangle)(a' + \langle m' \rangle) = 1 + \langle m' \rangle.$$

Como (3.11) es equivalente a la ecuación

$$(a' + \langle m' \rangle)(x + \langle m' \rangle) = b' + \langle m' \rangle,$$

podemos despejar

$$x + \langle m' \rangle = (u + \langle m' \rangle)(b' + \langle m' \rangle).$$

Esto es,

$$x = ub' + km'$$

para $k \in A$.

EJEMPLO 3.61. Consideremos el polinomio $X^2 + 1 \in \mathbb{Z}_3[X]$. Estamos, por abuso de notación, considerando que $\mathbb{Z}_3 = \{0, 1, 2\}$ entendiendo cada clase de equivalencia módulo 3 dada por su representante natural más pequeño.

Bien, el polinomio $X^2 + 1$ es irreducible, ya que tiene grado dos y no tiene raíces en $\mathbb{Z}_3$. Por tanto, $\mathbb{Z}_3[X]/\langle X^2+1\rangle$ es un cuerpo. Observemos que, en virtud de la división con resto en $\mathbb{Z}_3[X]$, cada elemento de dicho cuerpo se escribe de manera única como

$$a + bX + \langle X^2 + 1\rangle, \qquad (a, b \in \mathbb{Z}_3).$$

Por tanto, $\mathbb{Z}_3[X]/\langle X^2 + 1\rangle$ es un cuerpo con 9 elementos. Por otra parte, la aplicación $\mathbb{Z}_3 \to \mathbb{Z}_3[X]/\langle X^2 + 1\rangle$ que lleva $b \in \mathbb{Z}_3$ en $b + \langle X^2 + 1\rangle$ es un homomorfismo inyectivo de anillos. Podemos, pues, considerar que nuestro cuerpo de 9 elementos contiene una copia de $\mathbb{Z}_3$. De esta forma, si ponemos

$$\alpha = X + \langle X^2 + 1\rangle,$$

tenemos que

$$\frac{\mathbb{Z}_3[X]}{\langle X^2 + 1\rangle} = \{a\alpha + b : a, b \in \mathbb{Z}_3\}.$$

Observemos que, con la identificación hecha,

$$\alpha^2 = X^2 + \langle X^2 + 1\rangle = -1 + \langle X^2 + 1\rangle = 2 + \langle X^2 + 1\rangle = 2.$$

Tenemos, pues, que $\alpha^2 = 2$, y esta identidad sirve para operar en el cuerpo de 9 elementos construido. Así, por ejemplo, obtenemos que $2\alpha^2 = 1$, por lo que $\alpha^{-1} = 2\alpha$.

EJERCICIO 76. Resolver en $\mathbb{Z}[i]$ el sistema de congruencias

$$\begin{cases} x \equiv i \pmod{3} \\ x \equiv 2 \pmod{2+i} \\ x \equiv 1+i \pmod{3+2i} \\ x \equiv 3+2i \pmod{4+i} \end{cases}$$

EJERCICIO 77. Sean $\alpha_1, \dots, \alpha_n \in A$ raíces de un polinomio no nulo $f \in A[X]$, y supongamos que A es un DI. Demostrar que, si todas estas raíces son distintas, entonces f tiene grado al menos n.

EJERCICIO 78. Sean $x_0, x_1, \dots, x_n \in K$, con K un cuerpo. Supongamos que, para $0 \le i < j \le n$, $x_i \neq x_j$, y sean $y_0, y_1, \dots, y_n \in K$ cualesquiera. Demostrar que el sistema de congruencias en $K[X]$

$$\begin{cases} f(X) \equiv y_0 \pmod{X - x_0} \\ f(X) \equiv y_1 \pmod{X - x_1} \\ \vdots \\ f(X) \equiv y_n \pmod{X - x_n} \end{cases}$$

tiene una única solución de grado menor o igual que n. Dicha solución se llama *polinomio interpolador* de los datos $y_0, y_1 \dots, y_n$ en los nodos $x_0, x_1, \dots, x_n$. Como aplicación, dar la ecuación de la parábola que pasa por los puntos $(-1, 9), (2, 7), (3, 1/2) \in \mathbb{R}^2$

Capítulo 4

Factorización única

Recordemos que el Teorema Fundamental de la Aritmética afirma que cada número natural mayor que 1 se descompone de manera única como producto de números primos. En este capítulo, vamos a ver que esta propiedad se puede extender a cierto tipo de dominios de integridad que incluyen, en particular, a los dominios de ideales principales.

Comencemos, no obstante, viendo que hay dominios de integridad "sencillos" que no son dominios de ideales principales.

EJEMPLO 4.1. Vamos a demostrar que $\mathbb{Z}[\sqrt{-5}]$ no es un DIP exhibiendo un par de elementos suyos para los que no existe mínimo común múltiplo.

Dos elementos sin mínimo común múltiplo. Tomemos

$$\alpha = 2, \beta = 1 + \sqrt{-5},$$

y supongamos que existe $m = \mathrm{mcm}(\alpha, \beta)$. Escribamos $m = a + b\sqrt{-5}$, para $a, b \in \mathbb{Z}$. Como $m|\alpha\beta = 2 + 2\sqrt{-5}$, tomando normas, tenemos que

$$a^2 + 5b^2 = N(m)|N(\alpha\beta) = 24.$$

Por otro lado,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \tag{4.1}$$

por lo que 6 es un múltiplo común de α y β. Así que $m|6$. Tomando normas de nuevo, $a^2 + 5b^2$ divide a 36. Por tanto, $a^2 + 5b^2$ divide al máximo común divisor de 24 y 36 en $\mathbb{N}$, esto es, a 12.

Pero m ha de ser un múltiplo de α y de β, lo que implica que su norma $a^2 + 5b^2$ ha de ser un múltiplo común de 4 y 6. Toda esta información implica que $a^2+5b^2 = 12$. Reduciendo módulo 5, obtenemos $a^2 \equiv 2 \pmod 5$. Pero esta congruencia no tiene solución. Así que suponer la existencia de $\mathrm{mcm}(\alpha, \beta)$ lleva a una contradicción y descarta dicha existencia. Así, pues, $\mathbb{Z}[\sqrt{-5}]$ no es un DIP.

Un irreducible que no es primo. Vamos a demostrar que 2 es un irreducible de $\mathbb{Z}[\sqrt{-5}]$ que no es primo, lo que valdría, en virtud del Teorema 3.45, como argumento alternativo para afirmar que $\mathbb{Z}[\sqrt{-5}]$ no es un DIP. Si $2 = wz$ para $w, z \in \mathbb{Z}[\sqrt{-5}]$, de nuevo tomando normas, tendríamos $4 = N(z)N(w)$. Si ninguno de estos factores fuera 1, ambos serían igual a 2, pero es fácil ver que en $\mathbb{Z}[\sqrt{-5}]$ no hay números de norma 2. Así que, o bien z, o bien w tiene norma 1 y el que esté en tal caso ha de ser una unidad gracias a la Proposición 3.56.

Para demostrar que el irreducible 2 no es primo, miremos (4.1) para ver que 2 es un divisor del producto $(1 + \sqrt{-5})(1 - \sqrt{-5})$. No obstante, 2 no puede ser un divisor, siempre en $\mathbb{Z}[\sqrt{-5}]$, de ninguno de esos factores. Por ejemplo, si 2 dividiera a $1 + \sqrt{-5}$, tomando normas tendríamos que 4 divide, como número natural, a 6, cosa que no ocurre. Otro tanto se puede razonar para el factor $1 - \sqrt{-5}$.

Un anillo con cuatro elementos y dos caras. Analicemos el aspecto del anillo cociente $\mathbb{Z}[\sqrt{-5}]/\langle 2\rangle$. Reduciendo módulo 2 los coeficientes enteros a y b para un elemento $a+b\sqrt{-5}+\langle 2\rangle$, tenemos que

$$\mathbb{Z}[\sqrt{-5}]/\langle 2\rangle = \{0+\langle 2\rangle,\ 1+\langle 2\rangle,\ \sqrt{-5}+\langle 2\rangle,\ 1+\sqrt{-5}+\langle 2\rangle\}.$$

Esos cuatro elementos son distintos, lo que se comprueba sin gran dificultad usando, de nuevo, que la norma de 2 es 4.

Vamos a mostrar, por último, que el anillo de cuatro elementos anterior es isomorfo a un cociente de un anillo de polinomios. El único homomorfismo de anillos $\chi : \mathbb{Z} \to \mathbb{Z}[\sqrt{-5}]/\langle 2\rangle$ verifica que $2 \in \ker\chi$. Puesto que 2 es primo en $\mathbb{Z}$, esto implica que $2\mathbb{Z} = \ker\chi$. Por el Teorema del isomorfismo, obtenemos un homomorfismo inyectivo de anillos

$$\varphi = \overline{\chi} : \mathbb{Z}_2 \to \mathbb{Z}[\sqrt{-5}]/\langle 2\rangle$$

cuya imagen es $\{0+\langle 2\rangle, 1+\langle 2\rangle\}$. Ahora, la propiedad universal del anillo de polinomios $\mathbb{Z}_2[X]$ nos proporciona un homomorfismo de anillos

$$\widetilde{\varphi} : \mathbb{Z}_2[X] \to \mathbb{Z}[\sqrt{-5}]/\langle 2\rangle$$

que, sobre los elementos de $\mathbb{Z}_2$, actúa como φ y lleva X en $1+\sqrt{-5}+\langle 2\rangle$. Por tanto,

$$\widetilde{\varphi}(X^2) = (1+\sqrt{-5})^2 + \langle 2\rangle = 1 + 2\sqrt{-5} - 5 + \langle 2\rangle = 0 + \langle 2\rangle.$$

De aquí, $X^2 \in \ker\widetilde{\varphi}$. Ahora bien, $\mathbb{Z}_2[X]$ es un DIP, por lo que $\ker\widetilde{\varphi}$ es un ideal principal de $\mathbb{Z}_2[X]$. De hecho, vimos en la demostración del Teorema 3.27 que un generador se se obtiene como cualquier polinomio no nulo de grado mínimo que pertenezca a $\ker\widetilde{\varphi}$. Así que, si vemos que $\ker\widetilde{\varphi}$ no contiene polinomios no nulos de grado menor que 2, colegiremos que $\ker\widetilde{\varphi} = \langle X^2\rangle$.

Si $\overline{a}X + \overline{b} \in \ker\widetilde{\varphi}$, para $\overline{a}, \overline{b} \in \mathbb{Z}_2$, entonces $a + b\sqrt{-5} + \langle 2\rangle = \langle 2\rangle$. Pero esto sólo es posible[1] si $a = b = 0$, de donde $\overline{a} = \overline{b} = \overline{0}$.

Como, además, $\widetilde{\varphi}$ es claramente sobreyectivo, el Teorema de isomorfía nos da un isomorfismo de anillos

$$\frac{\mathbb{Z}_2[X]}{\langle X^2\rangle} \cong \frac{\mathbb{Z}[\sqrt{-5}]}{\langle 2\rangle}.$$

Unas observaciones finales sobre $\mathbb{Z}[\sqrt{-5}]/\langle 2\rangle$. No es un cuerpo, ya que tiene un elemento no nulo cuyo cuadrado es 0. Esto también demuestra que no es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Y no es isomorfo a $\mathbb{Z}_4$, ya que éste tiene característica 4 mientras que la característica de aquél es 2.

La existencia de mínimo común múltiplo está relacionada en las propiedades de factorización de un dominio de integridad. Veamos una proposición que nos será útil.

PROPOSICIÓN 4.2. *Sea* A *un DI, y* $a, b \in A$ *tales que* $ab \neq 0$. *Si existe* $\mathrm{mcm}(a,b)$, *y tomamos* $d \in A$ *tal que* $ab = d \cdot \mathrm{mcm}(a,b)$, *entonces* $d = \mathrm{mcd}(a,b)$.

DEMOSTRACIÓN. Bien, escribamos $m = \mathrm{mcm}(a,b)$, y tomemos $d \in A$ como en el enunciado. Puesto que $a|m$ y $b|m$, existen $a', b' \in A$ tales que $m = aa'$ y $m = bb'$. Por tanto, $ab = dm = daa'$ y $ab = dbb'$. Se sigue inmediatamente que $b = da'$ y $a = db'$. Por tanto, d es un divisor común de a y b.

[1] Obviamente, tomamos $a, b \in \{0, 1\}$.

Supongamos ahora $e \in A$ otro divisor común de a y b. Existirán, pues, $a'', b'' \in A$ tales que $a = ea''$ y $b = eb''$. Pongamos $m' = ea''b''$. Es claro que m' es un múltiplo común de a y b. Por tanto, $m|m'$. Así que existe $m'' \in A$ tal que $m' = mm''$. Por tanto,

$$dm = ab = m'e = mm''e,$$

de donde $d = m''e$ y $e|d$. Concluimos que $d = mcd(a, b)$. □

4.1. Dominios de Factorización Única

¿Qué vamos a entender como una factorización buena? La idea es que sea similar a aquélla de la que disfrutan los números enteros. Seguiremos denotando por $\sim$ a la relación de equivalencia "ser asociados".

DEFINICIÓN 4.3. Sea $a \in A$, donde A es un DI. Supongamos que $a \neq 0$ y $a \notin U(A)$. Diremos que a *admite factorización única* si

1. Existen irreducibles no asociados entre sí $p_1, \dots, p_r \in A$, y naturales $e_1, \dots, e_r \geq 1$ tales que $a \sim p_1^{e_1} \cdots p_r^{e_r}$.
2. Si $q_1, \dots, q_s \in A$ son irreducibles no asociados entre sí tales que $a \sim q_1^{f_1} \cdots q_s^{f_s}$ para ciertos naturales $f_1, \dots, f_s \geq 1$, entonces $r = s$ y, tras eventual reordenación, $f_i = e_i$ y $q_i \sim p_i$ para todo $i = 1, \dots, r$.

Si se da la primera condición, diremos que a *admite factorización completa*, y que $p_1^{e_1} \cdots p_r^{e_r}$ es una factorización completa de a.

EJEMPLO 4.4. Todo elemento irreducible admite factorización única. En efecto, sea $p \in A$, con A DI, irreducible. Obviamente, sólo hemos de razonar la segunda condición. Si $p = uq_1^{f_1} \dots q_s^{f_s}$ para $u \in U(A)$, y $q_1, \dots, q_s \in A$ irreducibles, entonces, como $f_1 \geq 1$, tenemos que $uq_1^{f_1-1} \cdots q_s^{f_s} \in U(A)$, lo cual es imposible, salvo que $s = 1$ y $f_1 = 1$.

EJERCICIO 79. Si a admite factorización única y b es asociado con a, entonces b admite factorización única.

DEFINICIÓN 4.5. Un dominio de integridad se llama *dominio de factorización única* (DFU), si todo elemento $a \neq 0$ tal que $a \notin U(A)$ admite factorización única. Entenderemos que todo cuerpo es un DFU, si bien de forma trivial.

TEOREMA 4.6. *Sea A un DI tal que todo elemento no nulo y no unidad admite factorización completa. Entonces A es un DFU si, y sólo si, todo elemento irreducible de A es primo.*

DEMOSTRACIÓN. Supongamos que A es un DFU y sea $p \in A$ irreducible. Supongamos que $a, b \in A$ son tales que $p|ab$, con lo que $pc = ab$ para cierto $c \in A$. Podemos suponer que $a, b \notin U(A)$, ya que, de lo contrario, se obtiene fácilmente que $p|a$ o bien $p|b$. De esta manera, $c \notin U(A)$, porque p es irreducible.

Bien, tomemos factorizaciones completas de $a \sim p_1^{e_1} \cdots p_r^{e_r}$, $b \sim y_1^{f_1} \cdots y_s^{f_s}$, $c \sim x_1^{g_1} \cdots x_t^{g_t}$. Tenemos, pues, que $px_1^{g_1} \cdots x_t^{g_t} \sim p_1^{e_1} \cdots p_r^{e_r} y_1^{f_1} \cdots y_s^{f_s}$. Por unicidad, puesto que suponemos que A es un DFU, obtenemos que, o bien $p \sim p_i$ para algún $i \in \{1, \dots, r\}$, o bien $p \sim y_j$ para algún $j \in \{1, \dots, s\}$. En el primer caso, $p|a$, mientras que, en el segundo, $p|b$, con lo que hemos demostrado que p es primo.

Vayamos por el recíproco. Sea $a \in A$, $a \neq 0$, $a \notin U(A)$. A cada factorización completa $a \sim p_1^{e_1} \cdots p_r^{e_r}$ le asociamos su *peso* $\sum_{i=1}^r e_i$. Definimos $\mu(a)$ como el mínimo de los pesos de las factorizaciones completas de a.

Demostraremos la unicidad de las factorizaciones completas de los elementos de A por inducción sobre $\mu(a)$. Así, si $\mu(a) = 1$, entonces a es irreducible, y tenemos la unicidad (ver Ejemplo 4.4).

Supongamos ahora $\mu(a) > 1$ y asumamos, como hipótesis de inducción, que todo elemento b con $\mu(b) < \mu(a)$ tiene unicidad en sus factorizaciones completas. Bien, sean dos factorizaciones $a \sim p_1^{e_1} \cdots p_r^{e_r} \sim q_1^{f_1} \cdots q_s^{f_s}$, donde la primera tiene peso $\mu(a)$. Como $e_1 > 0$, p_1 es un divisor de $q_1^{f_1} \cdots q_s^{f_s}$. Como p_1 es primo, por hipótesis, ha de dividir a alguno de los q_i, que podemos suponer, tras reindexación, $i = 1$. Luego, al ser q_1 irreducible, $p_1 \sim q_1$. Así que $b := p_1^{e_1-1} \cdots p_r^{e_r} \sim q_1^{f_1-1} \cdots q_s^{f_s}$. Como el peso de la primera factorización completa es $\mu(a) - 1$, podemos aplicar la hipótesis de inducción a b y deducir que $r = s$ y, tras eventual reordenación, $p_i \sim q_i$ para todo $i = 1, \dots, r$ y $e_i = f_i$. En realidad, $e_1 - 1 = f_1 - 1$, pero esto implica, obviamente, que $e_1 = f_1$. □

OBSERVACIÓN 4.7. Durante la prueba del Teorema 4.6, hemos demostrado que todas las factorizaciones de un elemento a de un DFU tienen el mismo peso, concretamente, el peso mínimo $\mu(a)$.

TEOREMA 4.8. *Todo DIP es un DFU.*

DEMOSTRACIÓN. Puesto que, en un DIP, cada irreducible es primo (ver Teorema 3.45), sólo hemos de demostrar que cada elemento admite una factorización completa (factorización, para abreviar). Sea A, pues, un DIP, y consideremos

$$X = \{a \in A \mid a \neq 0, a \notin U(A)\}.$$

Es claro que, si A no es un cuerpo, entonces $X \neq \emptyset$. Podemos escribir como unión disjunta $X = B \cup M$, donde

$$B = \{a \in X \mid a \text{ admite factorización}\},$$

$$M = \{a \in X \mid a \text{ no admite factorización}\}.$$

Nuestro objetivo es demostrar que $M = \emptyset$. Veamos que, si $M \neq \emptyset$, entonces M satisface una propiedad que nos llevará posteriormente a una contradicción. La propiedad es la siguiente: si $a \in M$, entonces existe $a' \in M$ tal que $\langle a \rangle \subsetneq \langle a' \rangle$.

En efecto, dado $a \in M$, éste no puede ser irreducible, luego $a = bc$ para $b, c \notin U(A)$. Pero, además, si $b, c \in B$, entonces $a = bc \in B$, ya que disponer de una factorización de b y otra de c da claramente una factorización de su producto. Así que o $b \in M$, o $c \in M$. Tomamos a' el apropiado de entre estos dos elementos. Como $a'|a$, deducimos la inclusión $\langle a \rangle \subseteq \langle a' \rangle$. La inclusión es estricta, puesto que a' no es asociado con a.

Haciendo uso reiterado de esta propiedad de M, podemos definir, a partir de $a_0 \in M$, una sucesión $a_0, a_1, \dots, a_n \cdots$ de elementos de M que da lugar a

$$\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \cdots \langle a_n \rangle \subsetneq \cdots$$

Definamos $I = \bigcup_{n \geq 0} \langle a_n \rangle$. Aunque, en general, la unión de ideales no es un ideal, sí ocurre en este caso especial que I es un ideal de A. Se deja como ejercicio comprobar esto.

Bien, al ser A un DIP, existe $x \in A$ tal que $I = \langle x \rangle$. Así, $x \in \langle a_n \rangle$ para algún $n \geq 0$. Por tanto,

$$I = \langle x \rangle \subseteq \langle a_n \rangle \subseteq I,$$

lo que sólo es posible si $\langle a_n \rangle = \langle a_m \rangle$ para todo $m \geq n$. Contradicción. □

EJEMPLO 4.9. Según vimos en el Ejemplo 4.1, $2 \in \mathbb{Z}[\sqrt{-5}]$ es irreducible pero no primo, por lo que este anillo no es un DFU. Veamos explícitamente la no unicidad de las factorizaciones completas. Tenemos

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

Vamos a demostrar que $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ son irreducibles. Denotemos por z cualquiera de estos números y supongamos $z = wr$, con $w, r \in \mathbb{Z}[\sqrt{-5}]$. Si $w \notin U(\mathbb{Z}[\sqrt{-5}])$, por la Proposición 3.56, $N(w) > 1$. Por tanto, $N(r)$ es un divisor de $4, 9$ o 6 menor estrictamente que esos números naturales. En particular $a^2 + 5b^2 \leq 3$. Así que $b = 0$ y $a^2 = 1$. De donde $r = 1$ o $r = -1$. Esto significa que $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ son irreducibles, y 6 tiene dos factorizaciones en $\mathbb{Z}[\sqrt{-5}]$ distintas.

En un DFU, la divisibilidad puede expresarse a través de las factorizaciones en irreducibles.

LEMA 4.10. *Sean* $p_1, \dots, p_r$ *irreducibles de un DFU* A, *y consideremos* $e_1, \dots, e_r, f_1, \dots, f_r \in \mathbb{N}$. *Sean* $a = p_1^{e_1} \cdots p_r^{e_r}, b = p_1^{f_1} \cdots p_r^{f_r} \in A$ *(entendemos que* $p_i^0 = 1$*). Entonces* a *divide a* b *si, y sólo si,* $e_i \leq f_i$ *para todo* $i = 1, \dots, r$.

DEMOSTRACIÓN. Si $a \mid b$, entonces $b = ax$ para $x \in A$. Además, cada divisor irreducible de x lo es, obviamente, de b, Por tanto, $x \sim p_1^{g_1} \cdots p_r^{g_r}$ para ciertos exponentes $g_1, \dots, g_r \in \mathbb{N}$. Así que $p_1^{f_1} \cdots p_r^{f_r} \sim p_1^{e_1+g_1} \cdots p_r^{e_r+g_r}$. Por la unicidad de las descomposiciones en irreducibles en un DFU, obtenemos que $f_i = e_i + g_i$ para todo $i = 1, \dots, r$. Por tanto, $f_i \geq g_i$ para todo $i = 1, \dots, r$. El recíproco es claro. □

Concluyamos viendo que en un DFU existen mínimos comunes múltiplos y máximos comunes divisores.

PROPOSICIÓN 4.11. *Sea* A *un DFU, y* $a, b \in A$ *no nulos y no unidades. Entonces existen* $\mathrm{mcm}(a, b)$ *y* $\mathrm{mcd}(a, b)$.

DEMOSTRACIÓN. Tomemos los irreducibles $p_1, \dots, p_r \in A$ que aparecen, salvo asociados, en las factorizaciones de a y b. De esta manera, podemos escribir $a \sim p_1^{e_1} \cdots p_r^{e_r}$ y $b \sim p_1^{f_1} \cdots p_r^{f_r}$, para $e_1, \dots, e_r, f_1, \dots, f_r \in \mathbb{N}$. Estamos entendiendo que $p_i^0 = 1$, claro.

Sea, para cada $i = 1, \dots, r$, $g_i = \text{máx}\{e_i, f_i\}$. Afirmamos que $\mathrm{mcm}(a, b) = p_1^{g_1} \cdots p_r^{g_r}$.

Es bastante obvio que $p_1^{g_1} \cdots p_r^{g_r}$ es múltiplo común de a y b. Supongamos ahora m otro múltiplo común de a y b. Claramente, $p_1, \dots, p_r$ están entre los divisores irreducibles que aparecen en la descomposición completa de m. Así, $m = p_1^{h_1} \cdots p_r^{h_r} x$, donde p_i no divide a x para todo $i = 1, \dots, r$. El Lema 4.10 nos da ahora que $h_i \geq g_i$ para cada $i = 1, \dots, r$. Por tanto, m es múltiplo de $p_1^{g_1} \cdots p_r^{g_r}$ y tenemos que

$$\mathrm{mcm}(a, b) = p_1^{g_1} \cdots p_r^{g_r}.$$

la existencia de $\mathrm{mcd}(a, b)$ viene garantizada por la Proposición 4.2. Además, de allí obtenemos también que

$$\mathrm{mcd}(a, b) = p_1^{k_1} \cdots p_r^{k_r},$$

donde $k_i = \text{mín}\{e_i, f_i\}$ para $i = 1, \dots, r$.

□

4.2. Factorización única de polinomios

Nuestro objetivo en esta sección es demostrar que, si A es un DFU, entonces el anillo de polinomios $A[X]$ es un DFU. Vamos a ir construyendo las herramientas para demostrar esto conforme las vayamos necesitando. Estas herramientas son de interés independiente.

LEMA 4.12. *Sea* A *un anillo conmutativo y* $a \in A$*. Denotemos por* Aa *el ideal principal de* A *generado por* a*, mientras que* $\langle a \rangle$ *denotará el ideal principal de* $A[X]$ *generado por* a*. Existe un isomorfismo de anillos*

$$\frac{A[X]}{\langle a \rangle} \cong \frac{A}{Aa}[X].$$

DEMOSTRACIÓN. Consideremos el homomorfismo de anillos

$$\phi : A \to \frac{A}{Aa}[X]$$

definido por $\phi(b) = b + Aa$ para todo $b \in A$ (obviamente, estamos considerando $b + Aa$ como como polinomio constante).

Por la propiedad universal del anillo de polinomios $A[X]$, existe un único homomorfismo de anillos

$$\widetilde{\phi} : A[X] \to \frac{A}{Aa}[X]$$

dado por $\widetilde{\phi}(\sum_i f_i X^i) = \sum_i (f_i + Aa)X^i$, que es claramente sobreyectivo. Observemos que $\sum_i f_i X^i \in \mathrm{Ker}\widetilde{\phi}$ si, y sólo si, $f_i \in Aa$ para todo i. Esto es, $\mathrm{Ker}\widetilde{\phi} = \langle a \rangle$. El lema se sigue ahora del Teorema de Isomorfía para anillos. □

LEMA 4.13. *Sea* A *un DI, y* $p \in A$ *un elemento primo. Entonces* p *es elemento primo en* $A[X]$*.*

DEMOSTRACIÓN. Por el Ejercicio 68, A/Ap es un DI. El Lema 4.12 da que $A[X]/\langle p \rangle \cong (A/Ap)[X]$, luego es un DI. Así, p es primo en $A[X]$. □

Vamos ahora con una noción fundamental en esta sección.

DEFINICIÓN 4.14. Sea $f = f_0 + f_1 X + \cdots + f_n X^n \in A[X]$, con $f_n \neq 0$ y A un DFU. El *contenido* de f se define como

$$c(f) = \mathrm{mcd}(f_0, f_1, \dots, f_n) \in A.$$

El polinomio f se dice *primitivo* si $c(f) = 1$.

OBSERVACIÓN 4.15. Por la propia definición de contenido, se desprende que éste está definido salvo asociados.

EJEMPLO 4.16. Sea $f = 2X^2 + 2 \in \mathbb{Z}[X]$. Entonces $c(f) = 2$. Pero si considero $f \in \mathbb{Q}[X]$, entonces $c(f) = 1$ (porque 2 es asociado con 1 en $\mathbb{Q}$).

LEMA 4.17 (Lema de Gauss). *Sea* A *un DFU, y* $f, g \in A[X]$ *polinomios primitivos. Entonces* fg *es primitivo.*

DEMOSTRACIÓN. Supongamos que fg no es primitivo. Entonces existe un primo[2] $p \in A$ tal que $p | c(fg)$ en A. Puesto que $c(fg)$ divide a fg en $A[X]$, deducimos que p divide a fg. Por el Lema 4.13, p divide a f o bien p divide a g. Supongamos la primera opción. Entonces $f = ph$ para cierto $h \in A[X]$. Escribiendo $f = \sum_i f_i X^i, h = \sum_i h_i X^i$, obtenemos que $f_i = ph_i$ para todo i. Así que $p | c(f)$ y f no es primitivo. □

[2]Como A es DFU, existe un divisor irreducible p que es primo por el Teorema 4.6.

LEMA 4.18. *Si* A *es un DFU,* $a \in A$ *y* $f \in A[X]$ *es primitivo, entonces* $c(af) = a$.

DEMOSTRACIÓN. Pongamos $f = f_0 + f_1 X + \cdots + f_n X^n$, con $f_i \in A$, para $i = 0, \ldots, n$. Como $1 = mcd(f_0, f_1, \ldots, f_n)$, tenemos, en vista de la demostración de la Proposición 4.11, que

$$a = mcd(af_0, af_1, \ldots, af_n) = c(af).$$

□

PROPOSICIÓN 4.19. *Sean* $f, g \in A[X]$ *con* A *un DFU. Entonces* $c(fg) = c(f)c(g)$.

DEMOSTRACIÓN. Escribamos $f = c(f)f^*$, $g = c(g)g^*$, para f^* y g^* primitivos. Entonces $fg = c(f)c(g)f^*g^*$. Por el Lema de Gauss, f^*g^* es primitivo. Por el Lema 4.18, $c(fg) = c(f)c(g)$. □

Necesitamos ahora construir el cuerpo de fracciones de un dominio de integridad. Su definición es una generalización del proceso de creación del cuerpo $\mathbb{Q}$ a partir de $\mathbb{Z}$.

PROPOSICIÓN 4.20. *Sea* A *un dominio de integridad, y* $A^* = A \setminus \{0\}$. *En el conjunto* $A \times A^*$ *definimos la relación* R *dada por* $(a, s)R(b, t)$ *si* $at = bs$.

1. *La relación* R *es de equivalencia. Denotemos por* $Q = (A \times A^*)/R$ *el conjunto cociente y, para cada* $(a, t) \in A \times A^*$, *por* $\frac{a}{s}$ *su clase de equivalencia en* Q.
2. *El conjunto* Q *es un cuerpo con operaciones suma y producto que satisfacen*
$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}, \qquad (\frac{a}{s}, \frac{b}{t} \in Q).$$
3. *La aplicación* $\iota : A \to Q$ *definida por* $\iota(a) = \frac{a}{1}$ *para* $a \in A$ *es un homomorfismo inyectivo de anillos.*

DEMOSTRACIÓN. Ejercicio rutinario pero recomendable para principiantes. Tiene analogías con la construcción de $\mathbb{Z}$ a partir de $\mathbb{N}$ que vimos ya hace tiempo. □

DEFINICIÓN 4.21. El cuerpo Q construido en la Proposición 4.20 se llama *cuerpo de fracciones* de A.

EJEMPLO 4.22. El cuerpo de fracciones de $\mathbb{Z}$ es el cuerpo $\mathbb{Q}$ de los números racionales.

EJEMPLO 4.23. Si K es un cuerpo, entonces el cuerpo de fracciones de $K[X]$ se denota por $K(X)$ y se llama *cuerpo de funciones racionales* con coeficientes en K.

La siguiente proposición revela el papel del cuerpo de fracciones cuando se estudian polinomios irreducibles con coeficientes en un DFU.

PROPOSICIÓN 4.24. *Sea* A *un DFU y* Q *su cuerpo de fracciones. Dado* $f \in A[X]$ *con* $\deg(f) \geq 1$, *tenemos que* f *es irreducible en* $A[X]$ *si, y sólo si,* f *es primitivo en* $A[X]$ *y* f *es irreducible en* $Q[X]$.

DEMOSTRACIÓN. Comencemos observando que si f no es primitivo, entonces f no es irreducible. Esto es claro, ya $f = c(f)f^*$, con $c(f) \notin U(A) = U(A[X])$ y $f^* \in A[X]$ primitivo. Como $\deg(f^*) \geq 1$, deducimos que f no es irreducible.

Bien, supongamos ahora que f es irreducible en $A[X]$. Ya sabemos que es primitivo. Procedamos a demostrar que es irreducible en $Q[X]$.

Supongamos una factorización $f = gh$, con $g, h \in Q[X]$. Tomemos $a, b \in A$ no nulos tales que $ag, bh \in A[X]$. Por la Proposición 4.19,

$$ab = c(abf) = c(agbh) = c(ag)c(bh). \tag{4.2}$$

Si tomamos $g_1, h_1 \in A[X]$ primitivos tales que $ag = c(ag)g_1, bh = c(bh)h_1$, tenemos que

$$abf = c(ag)c(bh)g_1h_1. \tag{4.3}$$

Deducimos de (4.2) y (4.3) que $f = g_1h_1$. Al ser f irreducible en $A[X]$, tenemos que $g_1 \in U(A[X])$ o bien $h_1 \in U(A[X])$. En el primer caso, $g_1 \in U(A)$ y, por tanto, $ag = c(ag)g_1 \in A \subseteq Q^*$. Por tanto, $g \in Q^*$. En el segundo caso, se deduce que $h \in Q^*$. Por tanto, f es irreducible en $Q[X]$.

Recíprocamente, si f es irreducible en $Q[X]$ y primitivo, y suponemos que $f = kq$ para $k, q \in A[X]$, como $c(f) = c(k)c(f)$, tenemos que $c(k), c(f) \in U(A)$. Ahora, puesto que f es irreducible en $Q[X]$, o bien k tiene grado 0, y entonces $k \sim c(k) \in U(A)$, o bien q tiene grado cero y $q \sim c(q) \in U(A)$. Así, f es irreducible en $A[X]$. □

LEMA 4.25. *Sea A un DFU y Q su cuerpo de fracciones. Sean $f, g \in A[X]$ tales que $f|g$ en $Q[X]$. Si f es primitivo en $A[X]$, entonces $f|g$ en $A[X]$.*

DEMOSTRACIÓN. Supongamos que $g = hf$ para $h \in Q[X]$. Tomemos $a \in A$ no nulo tal que $ah \in A[X]$ (por ejemplo, el producto de todos los denominadores de los coeficientes de h). Obviamente, $ag = ahf$, por lo que la Proposición 4.19 implica que $ac(g) = c(ah)$, puesto que f es primitivo. Si ahora escribimos $ah = c(ah)h_1$ para cierto polinomio primitivo $h_1 \in A[X]$, tenemos que

$$ag = ahf = c(ah)h_1f = ac(g)h_1f,$$

de donde $g = c(g)h_1f$. Por tanto, $f|g$ en $A[X]$. □

TEOREMA 4.26. *Si A es un DFU, entonces el anillo de polinomios $A[X]$ es un DFU.*

DEMOSTRACIÓN. En virtud del Teorema 4.6, hemos de demostrar que cada irreducible de $A[X]$ es primo y que cada polinomio no nulo y no unidad en $A[X]$ admite una factorización completa.

Veamos primero que todo elemento irreducible de $A[X]$ es primo. Si $p \in A$ es irreducible en $A[X]$ entonces es irreducible en A. Como A es un DFU, tenemos, en virtud del Teorema 4.6, que p es primo en A. El Lema 4.13 da ahora que p es primo en $A[X]$.

Supongamos ahora $f \in A[X]$ irreducible con $\deg(f) \geq 1$. Por la Proposición 4.24, f es primitivo. Supongamos que $f|gh$ para $g, h \in A[X]$. Obviamente, $f|gh$ en $Q[X]$ y, al ser $Q[X]$ un DIP, tenemos que f es primo en $Q[X]$, por lo que $f|g$ o $f|h$ en $Q[X]$. Por el Lema 4.25, $f|g$ en $A[X]$ o $f|h$ en $A[X]$. Por tanto, f es primo en $A[X]$.

En vista del Teorema 4.6, sólo nos resta demostrar que cada elemento no nulo y no unidad de $A[X]$ es producto de irreducibles. Bien, sea $f \in A[X]$, $f \neq 0$ y $f \notin U(A[X]) = U(A)$. Podemos escribir $f = c(f)f^*$, con $f^* \in A[X]$ primitivo. Puesto que A es un DFU, $c(f)$ se escribe como producto de irreducibles en A, que sabemos lo son en $A[X]$, podemos suponer que f es primitivo de grado positivo. Razonando por inducción sobre $\deg(f)$, supongamos que $\deg(f) = 1$. Como f es primitivo e irreducible en $Q[X]$ (tiene grado 1), deducimos de la Proposición 4.24 que lo es en $A[X]$.

Supongamos que $\deg(f) > 1$. Si f es irreducible, no hay nada que demostrar. Si no, $f = gh$ para $g, h \in A[X]$ no unidades. Como f es primitivo, ni g ni h pueden pertenecer a A. Por tanto, ambos tienen grado menor que $\deg(f)$ y, por hipótesis de inducción, admiten factorizaciones como producto de irreducibles. Por tanto, así lo hace f y hemos terminado la demostración. □

EJEMPLO 4.27. Si partimos de un anillo conmutativo A, podemos construir el anillo de polinomios $A[X]$ en un indeterminada X. Ahora, podemos considerar el anillo $A[X]$ como anillo de coeficientes de un nuevo anillo de polinomios $A[X][Y]$, donde Y denota una nueva indeterminada. ¿Qué aspecto tienen los elementos de $A[X][Y]$? Bien, tomemos $f \in A[X][Y]$. Entonces

$$f = \sum_j f_j Y^j,$$

para $f_j \in A[X]$. Ahora, para cada índice j,

$$f_j = \sum_i f_{ij} X^i,$$

donde $f_{ij} \in A$. De modo que

$$f = \sum_{i,j} f_{ij} X^i Y^j.$$

Vemos que f viene a ser un polinomio en las indeterminadas X, Y con coeficientes en A, y es por eso que el anillo $A[X][Y]$ se suele denotar por $A[X, Y]$. Observemos que, por aplicación iterada del Teorema 4.26, $A[X, Y]$ es un DFU siempre que A lo sea.

4.3. Polinomios irreducibles sobre un DFU

En esta sección, abordamos el problema, en general difícil, de decidir si un polinomio con coeficientes en un DFU es irreducible. Sea[3], pues, A un DFU, y $f \in A[X]$ no nulo. Si $\deg(f) = 0$, entonces $f \in A$ y el problema de decidir si f es irreducible se resuelve en A.

Supongamos ahora que $\deg(f) \geq 1$. La primera idea es escribir $f = c(f)f^*$, donde $f^* \in A[X]$ es primitivo del mismo grado que f. Si f no es primitivo, entonces $c(f)$ no es una unidad, y f no es irreducible. Por tanto, podemos limitarnos al caso de ser f primitivo. Sea Q el cuerpo de fracciones de A. Por la Proposición 4.24, f es irreducible en $A[X]$ si, y sólo si, f es irreducible en $Q[X]$.

Lo más sencillo que puede ocurrir, para que un polinomio primitivo de grado mayor que 1 no sea irreducible, es que tenga una raíz. De hecho, cada raíz en Q de un polinomio proporciona un factor irreducible de grado 1.

EJEMPLO 4.28. Sea $f \in A[X]$ primitivo no constante, donde A es un DFU con cuerpo de fracciones Q. Supongamos que $a/b \in Q$ es una raíz de f, con $a, b \in A$ tales que $\mathrm{mcd}(a, b) = 1$. Entonces $bX - a$ es un divisor irreducible de f en $A[X]$. En efecto, $X - a/b$ divisor de f en $Q[X]$, por lo que $bX - a$ es un divisor de f en $Q[X]$. Ahora, $bX - a$ es primitivo, luego, por el Lema 4.25, $bX - a$ es un divisor de f en $A[X]$.

[3]Mantendremos durante toda esta sección la hipótesis de que A es un DFU.

PROPOSICIÓN 4.29. *Sea* $f = f_0 + f_1X + \cdots + f_nX^n \in A[X]$ *con* $f_n \neq 0$. *Suponemos que* A *es un DFU con cuerpo de fracciones* Q. *Si* $a/b \in Q$ *es una raíz de* f *y* $\mathrm{mcd}(a,b) = 1$, *entonces* $b|f_n$ *y* $a|f_0$.

DEMOSTRACIÓN. Tenemos que

$$0 = f_0 + f_1\frac{a}{b} + \cdots + f_n\left(\frac{a}{b}\right)^n.$$

De aquí,

$$0 = f_0b^n + f_1ab^{n-1} + \cdots + f_na^n.$$

Esta igualdad implica que $b|f_na^n$. Como $\mathrm{mcd}(a,b) = 1$, deducimos que $b|f_n$. Análogamente, $a|f_0$. □

EJEMPLO 4.30. Veamos que $f = X^3 - 1/2X + 2 \in \mathbb{Q}[X]$ es irreducible. Como f tiene grado 3, será irreducible si, y sólo si, no tiene raíces en $\mathbb{Q}$. Ahora, las raíces de f son las mismas que las de $2f = 2X^3 - X + 4$. Si este polinomio tuviese raíces en $\mathbb{Q}$, estarían, en virtud de la Proposición 4.29, en la lista $-1, 1, -2, 2, -4, 4, -1/2, 1/2$. Puede comprobarse que f no se anula en ninguno de estos valores, por lo que f es irreducible en $\mathbb{Q}[X]$. Observemos que $2f$, al ser primitivo, es irreducible en $\mathbb{Z}[X]$.

El siguiente lema contiene la herramienta más general que podemos brindar en este curso para bregar con la factorización de polinomios. Se trata, además, de una idea bastante elemental.

LEMA 4.31. *Supongamos un homomorfismo de anillos conmutativos*

$$\phi : S \to B$$

y consideremos el homomorfismo de anillos

$$\varphi : S[X] \to B[X]$$

definido por

$$\varphi(\sum_i s_iX^i) = \sum_i \phi(s_i)X^i, \qquad (\sum_i s_iX^i \in S[X]).$$

Supongamos que $f = f_0 + f_1X + \cdots + f_nX^n \in S[X]$ *con* $\phi(f_n) \neq 0$, *y que* B *y* S *son dominios de integridad. Si* $f = hg$ *con* $g, h \in S[X]$, *entonces*

$$\deg(g) = \deg(\varphi(g)) \text{ y } \deg(h) = \deg(\varphi(h)).$$

DEMOSTRACIÓN. Es claro que $\deg(\varphi(g)) \leq \deg(g)$ y $\deg(\varphi(h)) \leq \deg(h)$. Ahora,

$$\begin{aligned} n = \deg(f) = \deg(g) + \deg(h) &\geq \deg(\varphi(g)) + \deg(\varphi(h)) \\ &= \deg(\varphi(gh)) = \deg(\varphi(f)) = n. \end{aligned}$$

Esto sólo es posible si las desigualdades anteriores son igualdades. □

El siguiente es un criterio clásico de irreducibilidad.

PROPOSICIÓN 4.32 (Criterio de Eisenstein). *Sea* $f = f_0 + f_1X + \cdots f_nX^n \in A[X]$, *con* $f_n \neq 0$. *Suponemos que* A *es un DFU y que* f *es primitivo. Supongamos que existe* $p \in A$ *primo tal que*

1. p *no divide a* f_n.
2. p *divide a* f_i *para todo* $i = 0, \ldots, f_{n-1}$.
3. p^2 *no divide a* f_0.

Entonces f *es irreducible en* $A[X]$.

DEMOSTRACIÓN. Consideremos el homomorfismo de anillos

$$\varphi : A[X] \to (A/Ap)[X]$$

definido por

$$\varphi(\sum_i a_i X^i) = \sum_i (a_i + Ap)X^i = \sum_i \overline{a_i} X^i,$$

donde estamos usando la notación $\overline{a_i} = a_i + Ap$.

Supongamos $f = hg$, para $g, h \in A[X]$. Entonces $\overline{f_n} X^n = \varphi(f) = \varphi(g)\varphi(h)$ en $(A/Ap)[X]$. Si vemos esta factorización en $K[X]$, donde K es el cuerpo de fracciones de A/Ap, tenemos, ya que $K[X]$ es un DFU, que $\varphi(g) = uX^k$ y $\varphi(h) = vX^{n-k}$ para $u, v \in K$ tales que $\overline{a_n} = uv$ y $k = \deg(g)$ (por el Lema 4.31).

Si $0 < k < n$, entonces $\varphi(g)(0) = 0 = \varphi(h)(0)$. Así, p ha de dividir al término independiente de g y también al de h, luego p^2 ha de dividir a su producto, esto es, a f_0. Por tanto, $k = 0$ o $k = n$. En el primer caso, g es constante y, al ser primitivo, $g \in U(A)$. En el segundo caso, $h \in U(A)$. Por tanto, f es irreducible. □

EJEMPLO 4.33. Sea $a \in \mathbb{Z}$ libre de cuadrados[4], y $n \in \mathbb{N}$, $n \geq 2$. Existe un divisor primo p de a tal que p^2 no divide a a. Podemos así aplicar el criterio de Eisenstein para deducir que $X^n - a$ es irreducible en $\mathbb{Z}[X]$. Por tanto, así lo es en $\mathbb{Q}[X]$. Como consecuencia, si $n \geq 2$, obtenemos que ninguna raíz n–ésima de a es un número racional.

EJEMPLO 4.34. Tomemos $f = Y^3 + X^2Y^2 + XY + X \in \mathbb{Z}[X, Y] = \mathbb{Z}[X][Y]$. Es claro que $X \in \mathbb{Z}[X]$ es irreducible. Aplicamos el Criterio de Eisenstein para $p = X$ y obtenemos que f es irreducible en $\mathbb{Z}[X][Y]$. También los es en $\mathbb{Q}[X, Y]$, usando el mismo argumento. Y, puesto que f es primitivo en $\mathbb{Q}[X][Y]$, también es irreducible en $\mathbb{Q}(X)[Y]$.

El Lema 4.31 no es sólo una herramienta para demostrar el Criterio de Eisenstein, sino que puede usarse para estudiar la irreducibilidad de algunos polinomios, eligiendo adecuadamente el homomorfismo ϕ. El siguiente es un caso sencillo.

PROPOSICIÓN 4.35. *Supongamos que A es un DFU, B un DI y $\phi : A \to B$ un homomorfismo de anillos. Sea*

$$\varphi : A[X] \to B[X]$$

definido por

$$\varphi(\sum_i a_i X^i) = \sum_i \phi(a_i) X^i.$$

Si $f = f_0 + f_1X + \cdots + f_nX^n \in A[X]$ es primitivo con $\phi(f_n) \neq 0$ y $\varphi(f) \in B[X]$ es irreducible, entonces f es irreducible.

DEMOSTRACIÓN. Supongamos una factorización $f = gh$ con $g, h \in A[X]$. Tenemos, pues, una factorización $\varphi(f) = \varphi(g)\varphi(h)$ en $B[X]$. Puesto que $\varphi(f)$ es irreducible, esto implica que $\varphi(g) \in U(B)$ o bien $\varphi(h) \in U(B)$. En el primer caso, $\deg(g) = \deg(\varphi(g)) = 0$, luego $g \in A$. Como f es primitivo, deducimos que $g \in U(A)$. En el segundo caso, deducimos que $h \in U(A)$. Por tanto, f es irreducible. □

[4]Libre de cuadrados significa que en la factorización como producto de primos de a, cada uno de ellos aparece una sóla vez. También se asume que $a \neq 0, 1, -1$.

EJEMPLO 4.36. Dado un número primo $p \in \mathbb{N}$, podemos tomar $\mathbb{Z} \to \mathbb{Z}_p$ la proyección canónica, y el homomorfismo correspondiente

$$\varphi : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$$

dado por

$$\varphi(\sum_i a_i X^i) = \sum_i \overline{a_i} X^i.$$

Aquí, $\overline{a_i}$ denota la clase de a_i módulo p. De hecho, para $f \in \mathbb{Z}[X]$ solemos denotar también $\overline{f} = \varphi(f)$, siempre y cuando se esté seguro de qué significa en cada caso la notación.

Veamos un ejemplo concreto: sea $f = X^4 + 15X^3 + 7 \in \mathbb{Z}[X]$. Reduciendo módulo 2, tenemos que $\overline{f} = X^4 + X^3 + 1 \in \mathbb{Z}_2[X]$. Comprobemos que $\overline{f}$ es irreducible. Como no tiene raíces en $\mathbb{Z}_2$, los únicos factores irreducibles de $\overline{f}$ han de ser de grado 2. Ahora, el único polinomio irreducible cuadrático[5] en $\mathbb{Z}_2[X]$ es $X^2 + X + 1$. Realizando la división euclídea de $\overline{f}$ entre el mismo, obtenemos resto X, luego X^2+X+1 no es un divisor de $\overline{f}$. Así, $\overline{f}$ es irreducible y, por la Proposición 4.35, f es irreducible en $\mathbb{Z}[X]$.

EJEMPLO 4.37. Tomemos ahora $f = X^4 + 10X^3 + 5X^2 - 2X - 3 \in \mathbb{Z}[X]$. Reduciendo módulo 2, obtenemos $\overline{f} = X^4 + X^2 + 1 = (X^2 + X + 1)^2 \in \mathbb{Z}_2[X]$. De aquí, no podemos deducir obviamente que f sea reducible o irreducible. Pero sí podemos obtener cierta información: si $f = gh$ con $g, h \in \mathbb{Z}[X]$ de grado positivo, entonces $\overline{f} = \overline{g}\overline{h}$. Como $\mathbb{Z}_2[X]$ es un DFU y $X^2 + X + 1$ es irreducible ahí, deducimos que $\deg \overline{g} = \deg \overline{h} = 2$ y, así, $\deg g = \deg h = 2$.

Reduzcamos ahora módulo 3, con lo que obtenemos

$$\overline{f} = X(X^3 + X^2 + \overline{2}X + 1) \in \mathbb{Z}_3[X].$$

Ahora, $X^3 + X^2 + \overline{2}X + 1$ no tiene raíces en $\mathbb{Z}_3$, por lo que, como es de grado 3, es irreducible. Aquí también se tiene que, de la igualdad $\overline{f} = \overline{g}\overline{h}$ en $\mathbb{Z}_3[X]$, uno de los polinomios g o h ha de tener grado 3 y el otro grado 1. Esto es una contradicción, que viene de suponer que f no es irreducible. Luego f ha de ser irreducible en $\mathbb{Z}[X]$.

EJEMPLO 4.38. Sea

$$f = Y^5 - Y^4 - 2Y^3 + Y - 1 + (Y - 2Y^3)X + (Y^4 + Y^3 + 1)X^2 + Y^3X^3 \in \mathbb{Q}[X, Y].$$

El homomorfismo evaluación $ev_1 : \mathbb{Q}[Y] \to \mathbb{Q}$ que lleva $a \in \mathbb{Q}[Y]$ en $a(1)$ da lugar al homomorfismo de anillos $\varphi : \mathbb{Q}[Y][X] = \mathbb{Q}[X, Y] \to \mathbb{Q}[X]$ definido por $\varphi(g(X, Y)) = g(X, 1)$, para $g(X, Y) \in \mathbb{Q}[X, Y]$.

Observemos que $f(X, 1) = -2 - X + 3X^2 + X^3 \in \mathbb{Q}[X]$. Por la Proposición 4.35, basta con que demostremos que $f(X, 1)$ es irreducible en $\mathbb{Q}[X]$ para que f lo sea en $\mathbb{Q}[X, Y]$. Ahora, $f(X, 1) \in \mathbb{Z}[X]$ es primitivo, luego sólo hemos de razonar que es irreducible en $\mathbb{Z}[X]$. Reduciendo módulo 3, obtenemos $\overline{f(X, 1)} = \overline{1} + \overline{2}X + X^3 \in \mathbb{Z}_3[X]$. Al ser de grado 3, y como $\mathbb{Z}_3$ es un cuerpo, tenemos que $\overline{f(X, 1)}$ es irreducible si, y sólo si, no tiene raíces en $\mathbb{Z}_3$. Pero[6] $\overline{f(0, 1)} = \overline{1} \neq 0$, $\overline{f(1, 1)} = \overline{1} \neq 0$ y $\overline{f(-1, 1)} = \overline{-1} \neq 0$. Por tanto, $\overline{f(X, 1)}$ es irreducible en $\mathbb{Z}_3[X]$, lo que implica que $f(X, 1)$ lo es en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$, y, de aquí, $f(X, Y)$ es irreducible en $\mathbb{Q}[X, Y]$,

[5] Es fácil listar todos los polinomios cuadráticos en $\mathbb{Z}_2[X]$ y comprobar si tienen raíces.

[6] Aquí puede parecer que cometemos un abuso de lenguaje, pero no es tal, si tenemos en cuenta que evaluar y tomar clases módulo 3 es lo mismo que reducir módulo 3 y luego evaluar...

EJEMPLO 4.39. Una formulación del Teorema Fundamental del Álgebra dice que los polinomios irreducibles en $\mathbb{C}[X]$ son, exactamente, los de grado 1. Desgraciadamente, las herramientas desarrolladas hasta aquí no permiten dar una demostración de este hecho. Observemos que, dado que cada polinomio no constante de $\mathbb{C}[X]$ es producto de polinomios irreducibles, ya que es un DFU, obtenemos que cada polinomio no constante de $\mathbb{C}[X]$ es producto de polinomios de grado 1. En relación con esto, una formulación tradicional del Teorema Fundamental del Álgebra es que cada polinomio no constante en $\mathbb{C}[X]$ tiene, al menos, una raíz en $\mathbb{C}$.

EJEMPLO 4.40. El polinomio $X^2+Y^2-1 \in \mathbb{C}[X,Y]$ es irreducible, en virtud de la aplicación del Criterio de Eisenstein para el primo $p = X-1 \in \mathbb{C}[X]$, viendo, claro, $X^2+Y^2-1 \in \mathbb{C}[X][Y]$.

EJEMPLO 4.41. Planteemos el problema de decidir si $Y^3 - X^2 \in \mathbb{C}[X,Y]$ es un polinomio irreducible. Viéndolo como polinomio en $\mathbb{C}[X][Y]$, se trata de un polinomio primitivo. Así, es irreducible si, y sólo si, lo es en $\mathbb{C}(X)[Y]$. Al ser de grado 3, será irreducible si, y sólo si, no tiene raíces en $\mathbb{C}(X)$. Supongamos una tal raíz $f(X)/g(X)$, con $f(X), g(X) \in \mathbb{C}[X]$.

$$\left(\frac{f(X)}{g(X)}\right)^3 - X^2 = 0.$$

De modo que $f(X)^3 = g(X)^3X^2$. Si ponemos $n = \deg f, m = \deg g$, deducimos que $3n = 3m+2$. Como esta identidad no es posible para $n, m \in \mathbb{N}$, deducimos que $Y^3 - X^2$ es irreducible en $\mathbb{C}[X,Y]$.

4.4. Raíces múltiples y Fórmula de Taylor

Sea A un anillo conmutativo y tomemos un polinomio $f \in A[X]$ de grado $n \geq 1$. Sabemos (ver Ejemplo 3.29) que $\alpha \in A$ es una raíz si, y sólo si $X - \alpha$ es un divisor de f. El siguiente resultado profundiza en esta idea cuando A es un dominio de integridad.

PROPOSICIÓN 4.42. *Sea A un DI y $\alpha_1, \dots, \alpha_k \in A$ distintos. Dado un polinomio $f \in A[X]$ no constante, tenemos que $f(\alpha_i) = 0$ para todo $i = 1, \dots, k$ si, y sólo si,*

$$(X-\alpha_1)\cdots(X-\alpha_k)$$

divide a f.

DEMOSTRACIÓN. Si $(X-\alpha_1)\cdots(X-\alpha_k)$ divide a f, entonces

$$f = (X-\alpha_1)\cdots(X-\alpha_k)g$$

para cierto $g \in A[X]$. Esto, obviamente, implica que $f(\alpha_i) = 0$ para todo $i = 1, \dots, k$.

Recíprocamente, el Ejercicio 3.29 nos da que $f = (X-\alpha_1)g$ para cierto $g \in A[X]$. Ahora, para $i \neq 1$ tenemos que $0 = f(\alpha_1) = (\alpha_i - \alpha_1)g(\alpha_i)$. Como A es un DI, esto implica que $g(\alpha_i) = 0$ para todo $i = 2, \dots, k$. Una sencilla inducción sobre el grado me da que $(X-\alpha_2)\cdots(X-\alpha_k)$ divide a g, de donde deducimos fácilmente que $(X-\alpha_1)\cdots(X-\alpha_k)$ divide a f. □

Seguidamente, queremos averiguar cuándo un polinomio de la forma $X - \alpha$ se puede sacar como factor de otro polinomio más de una vez.

DEFINICIÓN 4.43. Sea A un anillo conmutativo y $f \in A[X]$ un polinomio no constante. Una raíz $\alpha \in A$ de f se dice *múltiple* si $(X-\alpha)^2$ divide a f.

Para tratar con raíces múltiples, es útil disponer de la derivada formal de un polinomio. Concretamente, sea $f = \sum_i f_i X^i \in A[X]$, con A anillo conmutativo. Definimos la *derivada formal* de f como el polinomio

$$f' = \sum_{i \geq 1} i f_i X^{i-1}.$$

Recordemos que if_i denota la suma de f_i consigo mismo i veces.

LEMA 4.44. *Sean* $f, g \in A[X]$*, para* A *anillo conmutativo, y* $a \in A$*. Entonces*

1. $(af)' = af'$.
2. $(f+g)' = f' + g'$.
3. $(fg)' = f'g + fg'$.

DEMOSTRACIÓN. Es una comprobación tediosa pero sin sorpresas. □

PROPOSICIÓN 4.45. *Sea* $f \in A[X]$ *con* A *un anillo conmutativo, y* $\alpha \in A$*. Entonces* α *es una raíz múltiple de* f *si, y sólo si,* α *es una raíz de* f *y de* f'*.*

DEMOSTRACIÓN. Si α es raíz múltiple de f, entonces $f = (X-\alpha)^2 g$ para cierto $g \in A[X]$. Calculando mediante el uso del Lema 4.44, obtenemos que

$$f' = (X-\alpha)\left((X-\alpha)g' + 2g\right)$$

Tenemos, pues, que $f(\alpha) = f'(\alpha) = 0$.

Recíprocamente, puesto que α es supuesta una raíz de f, escribimos $f = (X-\alpha)h$ para cierto $h \in A[X]$. Derivando y despejando h, obtenemos

$$h = f' - (X-\alpha)h'.$$

Como $f'(\alpha) = 0$, obtenemos que $h(\alpha) = 0$, por lo que $h = (X-\alpha)p$, para $p \in A[X]$ adecuado. Luego $f = (X-\alpha)^2 p$. □

Vamos a concluir con una herramienta básica del Cálculo, la Fórmula de Taylor. Lo haremos en un contexto algebraico básico, es decir, para polinomios.

Para $f \in A[X]$, con A anillo conmutativo, podemos definir su sucesión de derivadas de orden superior mediante el siguiente proceso. Escribimos $f^{(0)} = f$ y , supuesta definida $f^{(k)}$ para un cierto $k \geq 0$, definimos $f^{(k+1)} = (f^{(k)})'$. Así, $f^{(1)} = f'$. Se suele usar la notación $f'' = f^{(2)}$, $f''' = f^{(3)}$. Nos referiremos a $f^{(k)}$ como el k–ésimo polinomio derivado de f, o derivada de orden k de f.

Si denotamos $m_i = X^i$ para $i \in \mathbb{N}$, tenemos que $m_i^{(k)} = 0$ si $k > i$, mientras que, para $k \leq i$, tenemos

$$m_i^{(k)} = \frac{i!}{(i-k)!} X^{i-k} = \frac{i!}{(i-k)!} m_{i-k}.$$

Observemos que $\frac{i!}{(i-k)!} \in \mathbb{N}$, por lo que la anterior expresión tiene sentido cualquiera sea el anillo conmutativo A.

PROPOSICIÓN 4.46. *Sea* K *un cuerpo de característica* 0*, y* $f \in K[X]$*. Entonces, si* Y *denota otra indeterminada, se verifica:*

$$f(X+Y) = \sum_i \frac{1}{i!} f^{(i)}(X) Y^i. \tag{4.4}$$

DEMOSTRACIÓN. Una cuestión previa es que, si n es un número entero, lo estamos identificando con su imagen bajo el único homomorfismo de anillos $\mathbb{Z} \to K$. Como la característica de K se supone 0, este homomorfismo es inyectivo y, por tanto, si $n \neq 0$, entonces es también no nulo visto como elemento de K. Al ser K cuerpo, tenemos garantizada la consistencia de la afirmación $1/n \in K$.

Comencemos demostrando (4.4) para cada monomio $m_i(X) = X^i$. Tenemos el siguiente cálculo:

$$m_i(X+Y) = (X+Y)^i = \sum_{k=0}^{i} \frac{i!}{(i-k)!k!} X^{i-k}Y^k = \sum_{k=0}^{i} \frac{1}{k!} m_i^{(k)}(X)Y^k.$$

Para el caso general, observemos que, si $f = \sum_j f_j X^j \in K[X]$, tenemos

$$\begin{aligned} f(X+Y) = \sum_j f_j m_j(X+Y) &= \sum_j f_j \sum_i \frac{1}{i!} m_j^{(i)}(X)Y^i \\ &= \sum_i \frac{1}{i!} (\sum_j f_j m_j^{(i)}(X))Y^i = \sum_i \frac{1}{i!} f^{(i)}(X)Y^i. \end{aligned}$$

□

COROLARIO 4.47 (Fórmula de Taylor). *Sea* $f \in K[X]$ *y* $\alpha \in K$, *con* K *un cuerpo de característica cero. Entonces*

$$f = \sum_i \frac{1}{i!} f^{(i)}(\alpha)(X-\alpha)^i. \tag{4.5}$$

DEMOSTRACIÓN. Pongamos en (4.4) $X = \alpha$. Obtenemos

$$f(\alpha + Y) = \sum_i \frac{1}{i!} f^{(i)}(\alpha)Y^i.$$

Ahora, en esta última fórmula, tomemos $Y = X - \alpha$, y obtenemos

$$f(X) = f(\alpha + (X-\alpha)) = \sum_i \frac{1}{i!} f^{(i)}(\alpha)(X-\alpha)^i.$$

□

Una aplicación de la Fórmula de Taylor es estudiar la multiplicidad de una raíz.

DEFINICIÓN 4.48. Sea K un cuerpo de característica 0, $f \in K[X]$ no constante y $\alpha \in K$. Diremos que α es una raíz de f de mulltiplicidad $k \geq 1$ si $(X-\alpha)^k | f$ pero $(X-\alpha)^{k+1}$ no divide a f.

PROPOSICIÓN 4.49. *Sea* K *un cuerpo de característica* 0 *y* $f \in K[X]$ *no constante. Un elemento* $\alpha \in K$ *es una raíz de* f *de multiplicidad* $k \geq 1$ *si, y sólo si,* $f^{(i)}(\alpha) = 0$ *para todo* $i = 0, \ldots, k-1$ *pero* $f^{(k)}(\alpha) \neq 0$.

DEMOSTRACIÓN. Se deduce fácilmente de (4.5) como ejercicio. □

Capítulo 5

Ejercicios Finales

EJERCICIO 80. Decidir razonadamente si las siguientes afirmaciones son verdaderas o falsas.

1. Sea X un conjunto no vacío. Una relación de equivalencia en X es una partición de $X \times X$.
2. Sea X un conjunto. Existe una aplicación inyectiva $f : X \to \mathcal{P}(X)$ que no es sobreyectiva.
3. Sea X un conjunto finito no vacío. Existe una relación de equivalencia R en X tal que el cardinal de X y el de X/R son iguales.
4. Sea X un conjunto no vacío. Existe una única aplicación $f : X \to \emptyset$.
5. Sea X un conjunto no vacío. Existe una única aplicación $f : X \to \mathcal{P}(\emptyset)$.
6. Sea X un conjunto con dos elementos, e Y un conjunto con tres elementos. Existen, exactamante, 6 aplicaciones inyectivas de X a Y.
7. Sea $n \in \mathbb{N}$ tal que $n \geq 2$. El conjunto
$$X = \{m \in \mathbb{N} \mid m \neq 1 \text{ y } m \text{ divide a } n\},$$
tiene un mínimo que es un número primo.
8. Todo monoide con dos elementos es conmutativo.
9. Sea $X = \{1, 2, 3\}$. En $X \times X$ definimos la relación R siguiente: para
$$(n, m), (n', m') \in X \times X,$$
$(n, m)R(n', m')$ si $n+m' = n'+m$. Esta relación R es de equivalencia.
10. En $X = \{n \in \mathbb{N} \mid n \geq 2\}$ definimos la relación R siguiente: para $n, m \in X$, nRm si n y m tienen un divisor primo común. Esta relación R es de equivalencia.

EJERCICIO 81. Escoger la respuesta correcta. Sea A un anillo conmutativo no trivial tal que, para todo $f, g \in A[X]$, $\deg(fg) = \deg(f) + \deg(g)$. Entonces:

(a) A es un cuerpo.
(b) A es un dominio de factorización única.
(c) A es un dominio de integridad.
(d) Ninguna de las otras afirmaciones es correcta.
(e) La propiedad enunciada es correcta para cualquier anillo conmutativo no trivial A.

EJERCICIO 82. Escoger la respuesta correcta. Sean $X = \{1, 2, 3\}$ e $Y = \{0, 1\}$.

(a) Hay, exactamente, 3 aplicaciones sobreyectivas distintas de X a Y.
(b) Hay, exactamente, 6 aplicaciones sobreyectivas distintas de X a Y.
(c) Hay, exactamente, 4 aplicaciones sobreyectivas distintas de X a Y.
(d) Hay, exactamente, 8 aplicaciones sobreyectivas distintas de X a Y.

(e) Hay, exactamente, 1 aplicación sobreyectiva de X a Y.

EJERCICIO 83. Escoger la respuesta correcta. Sea A un dominio de ideales principales y $p \in A$ irreducible. Entonces:

(a) $\frac{A}{\langle p \rangle}[X]$ es un DIP que no es cuerpo.
(b) $\frac{A}{\langle p \rangle}[X]$ es un DIP y puede ser, para ejemplos concretos de A y p, un cuerpo.
(c) $\frac{A}{\langle p \rangle}[X]$ no tiene por qué ser un dominio de integridad.
(d) Ninguna de las otras afirmaciones es correcta.
(e) $\frac{A}{\langle p \rangle}[X]$ es un DFU, pero no necesariamente un DIP.

EJERCICIO 84. Escoger la respuesta correcta. Sea $X = \{1, 2, 4\}$ y la relación R definida en $X \times X$ por $(a, b)R(c, d)$ si, y sólo si, $ad = bc$, para $(a, b), (c, d) \in X \times X$. Entonces:

(a) R es una relación de equivalencia y $(X \times X)/R$ tiene 9 elementos.
(b) R es una relación de equivalencia y $(X \times X)/R$ tiene 5 elementos.
(c) R es una relación de equivalencia y $(X \times X)/R$ tiene 3 elementos.
(d) R no es una relación de equivalencia.
(e) R es una relación de orden parcial.

EJERCICIO 85. Escoger la respuesta correcta. Sea X un conjunto con 10 elementos y X_0 un subconjunto de X de cardinal 5. Definimos en $\mathcal{P}(X)$ la relación R dada por YRZ si, y sólo si, $Y \cup X_0 = Z \cup X_0$, para $Y, Z \in \mathcal{P}(X)$. Entonces:

(a) R es una relación de equivalencia y $[X_0]_R = \{X_0\}$.
(b) R es una relación de equivalencia y $[X_0]_R = \mathcal{P}(X_0)$.
(c) R no es una relación de equivalencia.
(d) R es una relación de equivalencia y $[X_0]_R = X$.
(e) Ninguna de las otras afirmaciones es correcta.

EJERCICIO 86. Escoger la respuesta correcta. Sea A un DFU y $f = a_0+a_1X+a_2X^2+a_3X^3+a_4X^4 \in A[X]$ un polinomio primitivo. Sea $\phi : A \to \mathbb{Z}$ un homomorfismo de anillos tal que $\phi(a_0) = 1, \phi(a_1) = -2, \phi(a_2) = -1, \phi(a_3) = -2, \phi(a_4) = 1$. Entonces:

(a) f es irreducible.
(b) f no tiene raíces en A.
(c) f no es irreducible.
(d) f tiene una raíz en el cuerpo de fracciones de A.
(e) No puede deducirse ninguna de las otras afirmaciones sobre f.

EJERCICIO 87. Escoger la respuesta correcta. Sean $a(X) = X^4 + X^3 + 3X^2 + 2X + 4$ y $b(X) = X^4 + 2X^3 + 2X^2 + 2X + 1$ dos polinomios de $\mathbb{Z}_5[X]$. El máximo común divisor de $a(X)$ y $b(X)$ es un polinomio de grado

(a) 0
(b) 1
(c) 2
(d) 3
(e) 4

EJERCICIO 88. Escoger la respuesta correcta. Sea

$$f = 3X^5 + 42X^3 - 147X^2 + 21 \in \mathbb{Z}[X].$$

Entonces:

(a) f no tiene raíces en $\mathbb{R}$.
(b) f es irreducible en $\mathbb{Z}[X]$
(c) f no es irreducible en $\mathbb{Q}[X]$.
(d) f tiene una raíz doble en $\mathbb{C}$.
(e) f es irreducible en $\mathbb{Q}[X]$.

EJERCICIO 89. Escoger la respuesta correcta. Las dos últimas cifras de 2^{100} son:

(a) 14
(b) 42
(c) 66
(d) 76
(e) Ninguna de las otras opciones es correcta.

EJERCICIO 90. Escoger la respuesta correcta. Sea $X = \{0, 2, 4\}$ y la relación R definida en $X \times X$ por $(a, b)R(c, d)$ si, y sólo si, $a + d = b + c$, para $(a, b), (c, d) \in X \times X$. Entonces:

(a) R es una relación de equivalencia y $(X \times X)/R$ tiene 9 elementos.
(b) R es una relación de equivalencia y $(X \times X)/R$ tiene 5 elementos.
(c) R es una relación de equivalencia y $(X \times X)/R$ tiene 3 elementos.
(d) R no es una relación de equivalencia.
(e) Ninguna de las otras opciones es correcta.

EJERCICIO 91. Escoger la respuesta correcta. Sea A un dominio de factorización única y $p \in A$ un elemento irreducible. Entonces:

(a) $A/\langle p\rangle$ es un cuerpo.
(b) $A/\langle p\rangle$ es un anillo cuyo grupo de unidades es finito.
(c) $A/\langle p\rangle$ es un dominio de integridad finito.
(d) $A/\langle p\rangle$ es un dominio de integridad infinito.
(e) Ninguna de las otras opciones es correcta.

EJERCICIO 92. Escoger la respuesta correcta. Sea $I = \{\emptyset\}$ e $II = I \cup \{I\}$. El número de aplicaciones distintas de II a $\mathcal{P}(II)$ es

(a) 8
(b) 12
(c) 14
(d) 4
(e) Ninguna de las otras opciones es correcta.

EJERCICIO 93. Escoger la respuesta correcta. Consideremos la relación R definida en conjunto $2\mathbb{Z}$ por aRb si, y sólo si, $a \equiv b \pmod 3$, para $a, b \in 2\mathbb{Z}$. Entonces:

(a) R no es una relación de equivalencia.
(b) R es una relación de equivalencia y $2\mathbb{Z}/R$ tiene 2 elementos.
(c) R es una relación de equivalencia y $2\mathbb{Z}/R$ tiene 3 elementos.
(d) R es una relación de equivalencia y $2\mathbb{Z}/R$ tiene 6 elementos.

(e) R es una relación de equivalencia y $2\mathbb{Z}/R$ tienen infinitos elementos.

EJERCICIO 94. Escoger la respuesta correcta. Sea $A = \mathbb{Z}[i]/\langle 2\rangle$. Entonces:

(a) A es un cuerpo con 4 elementos.
(b) A es un anillo isomorfo a $\mathbb{Z}_2[X]/\langle X^2\rangle$.
(c) A es un anillo isomorfo a $\mathbb{Z}_4$.
(d) A es un anillo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.
(e) Ninguna de las otras cuatro opciones es correcta.

EJERCICIO 95. Escoger la respuesta correcta. Sea $f = X^5 + 5X^4 + 7X^3 + X^2 - 3X - 11 \in \mathbb{Q}[X]$. Entonces:

(a) f es irreducible.
(b) f tiene un factor irreducible de grado 4.
(c) f tiene un factor irreducible de grado 3.
(d) f tiene un factor irreducible de grado 2.
(e) f tiene una raíz múltiple en $\mathbb{Q}$.

EJERCICIO 96. Escoger la respuesta correcta. El número de soluciones enteras en el intervalo $[-10000, 10000]$ de la ecuación diofántica

$$6783x + 613y = 3$$

es

(a) 1
(b) 2
(c) 3
(d) 4
(e) 5

EJERCICIO 97. Escoger la respuesta correcta. Consideremos $\varphi : \mathbb{Z}[i]/\langle 5\rangle \to \mathbb{Z}_5$ dada por $\varphi(a + bi + \langle 5\rangle) = a - b + 5\mathbb{Z}$ para $a + bi \in \mathbb{Z}[i]$. Entonces:

(a) φ no es una aplicación bien definida.
(b) φ es una aplicación bien definida pero no es un homomorfismo de grupos aditivos.
(c) φ es un homomorfismo de grupos aditivos pero no es homomorfismo de anillos.
(d) φ es un homomorfismo de anillos pero no es un isomorfismo.
(e) φ es un isomorfismo de anillos.

EJERCICIO 98. Escoger la respuesta correcta. Sean $f, g \in \mathbb{Z}_3[X]$ los polinomios $f = X^5 + 2X^3 + X^2 + X + 1$, $g = X^5 + X^4 + X^3 + 2$. El mínimo común múltiplo de f y g en $\mathbb{Z}_3[X]$ tiene grado

(a) 6
(b) 7
(c) 8
(d) 9
(e) 10

EJERCICIO 99. Dadas correspondencias C de X a Y y D de Y a Z, se define su composición $D \circ C$, que es una correspondencia de X a Z, declarando de $x(D \circ C)z$. para $x \in X$, $z \in Z$, si existe $y \in Y$ tal que xCy e yDz. Sea R una relación en un conjunto X. Demostrar que R es transitiva si, y sólo si, $R \circ R \subseteq R$.

EJERCICIO 100. Listar los elementos del grupo de unidades $U(\mathbb{Z}_4 \times \mathbb{Z}_8)$.

EJERCICIO 101. Sean A, B anillos. Dar, demostrándola a partir de los resultados vistos en clase, una fórmula para calcular la característica de $A \times B$ en función de las características de A y de B. Aplicar lo obtenido para calcular la característica de $\mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_9$.

EJERCICIO 102. Calcular todas las raíces de $X^2 + 7$ en $\mathbb{Z}_8[X]$.

EJERCICIO 103. Demostrar que el DFU $\mathbb{Z}[X]$ no es un DIP viendo que el ideal suyo generado por 2 y X no es principal.

EJERCICIO 104. Factorizar como producto de polinomios irreducibles en $\mathbb{Z}[X]$ el polinomio

$$f = X^5 + X^4 + X^3 + X^2 + X + 1$$

EJERCICIO 105. Estudiar si los siguientes polinomios son reducibles o irreducibles en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$:

1. $2X^5 - 6X^3 + 9X^2 - 15$
2. $X^4 + 15X^3 + 7$
3. $X^4 - 22X^2 + 1$
4. $X^3 + 17X + 36$
5. $X^5 - X^2 + 1$
6. $X^4 + 10X^3 + 5X^2 - 2X - 3$
7. $X^4 + 6X^3 + 4X^2 - 15X + 1$
8. $X^5 + 5X^4 + 7X^3 + X^2 - 3X - 11$
9. $X^4 + 6X^3 + 4X^2 - 15X + 1$
10. $X^6 + 3X^5 - X^4 + 3X^3 + 3X^2 + 3X - 1$
11. $X^7 + 5X^6 + X^2 + 6X + 5$
12. $3X^5 + 42X^3 - 147X^2 + 21$
13. $X^5 + 3X^4 + 10X^2 - 2$

EJERCICIO 106. Estudiar si los siguientes polinomios son reducibles o irreducibles en $\mathbb{Z}[X, Y]$ y en $\mathbb{Q}[X, Y]$:

: a) $Y^3 + X^2Y^2 + XY + X$
: b) $(Y^5 - Y^4 - 2Y^3 + Y - 1) + X(Y - 2Y^3) + X^2(Y^4 + Y^3 + 1) + X^3Y^3$
: c) $(X^4 + X + 1) + (1 - 2X - X^3)Y + (X^3 + X)Y^2$
: d) $YX^3 + (-Y^2 + Y - 1)X^2 + (-Y^2 + Y - 1)X + (Y^3 - Y^2 - 1)$
: e) $X^3Y^2 + (X^2 + 1)Y - X^2 - 1$
: f) $Y^2X + YX - Y^2 + X - Y - 1$

EJERCICIO 107. Demostrar que los polinomios $X^2 + Y^2 - 1, Y^3 - X^2 \in \mathbb{C}[X, Y]$ son irreducibles.

EJERCICIO 108. Demostrar que el subconjunto de $\mathbb{Z}[X]$ formado por los polinomios cuyo coeficiente de grado uno es par es un subanillo. Comprobar que en este subanillo los elementos 2 y $2X$ tienen m.c.d. y no tienen m.c.m.

EJERCICIO 109. Dado un anillo conmutativo R y un elemento $a \in R$ demostrar que la aplicación $\phi : R[X] \to R[X]$ dada por $\phi(f(X)) = f(X+a)$ es un isomorfismo de anillos. Aplicar este resultado y el criterio de Eisenstein para ver que el polinomio $f(X) = X^4 + 1$ es irreducible en $\mathbb{Z}[X]$ estudiando el polinomio $f(X+1)$.

EJERCICIO 110. Utilizar la fórmula de Taylor para demostrar que el polinomio $X^4 + 2pX - p^2 \in \mathbb{Z}[X]$, con p impar, es irreducible.

EJERCICIO 111. Sea $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{R}$. Demostrar que

$$I = \{f(x) \in \mathbb{Q}[X] : f(\alpha) = 0\}$$

es un ideal principal no nulo de $\mathbb{Q}[X]$. Decidir si $\mathbb{Q}[X]/I$ es un cuerpo.

EJERCICIO 112. Sea D un DFU y $a, b \in D$. Demostrar que si $ab \neq 0$ y $d \in D$ es un divisor de ab primo relativo con a, entonces d es un divisor de b.

EJERCICIO 113. Comprobar que los elementos $2, 3, 4+\sqrt{10}, 4-\sqrt{10}$ son irreducibles en $\mathbb{Z}[\sqrt{10}]$, pero no son primos. Deducir que $\mathbb{Z}[\sqrt{10}]$ no es un DFU, exhibiendo un elemento con dos factorizaciones distintas como producto de irreducibles.

EJERCICIO 114. Decidir razonadamente si existen isomorfismos de anillos

$$\frac{\mathbb{Z}[i]}{\langle 1+i \rangle} \cong \mathbb{Z}_2, \qquad \frac{\mathbb{Z}[i]}{\langle i \rangle} \cong \mathbb{Z}$$

EJERCICIO 115. En $\mathbb{Z}[i]$ se consideran $x = 1+3i, y = 3+4i$. Factorizar x e y como producto de irreducibles y calcular su máximo común divisor y su mínimo común múltiplo.

EJERCICIO 116. Resolver el siguiente sistema de congruencias en $\mathbb{Z}[i]$:

$$\begin{aligned} x &\equiv i \pmod{3} \\ x &\equiv 2 \pmod{(2+i)} \\ x &\equiv 1+i \pmod{(3+2i)} \\ x &\equiv 3+2i \pmod{(4+i)} \end{aligned}$$

EJERCICIO 117. Demostrar que el subconjunto de $\mathbb{Q}$ formado por las fracciones n/m con $n, m \in \mathbb{Z}$ y m impar es un DIP (entendemos que las fracciones n/m están expresadas en forma reducida, esto es, con n, m coprimos).

EJERCICIO 118. Dar la solución general de la siguiente ecuación en $\mathbb{Z}[i]$:

$$4x + (3 + 3i)y = -1 + 5i$$

EJERCICIO 119. Sea $I = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}, a \equiv b \pmod{2}\}$. Demostrar que:

1. I es un ideal de $\mathbb{Z}[\sqrt{-5}]$;
2. I está generado por 2 y $1 + \sqrt{-5}$;
3. I es un ideal maximal;
4. $I^2 \subseteq \langle 2 \rangle$;
5. I no es un ideal principal.

EJERCICIO 120. Razonar que $\mathbb{Z}[i]/\langle 1 + i \rangle$ es un cuerpo que tiene un número finito de elementos.

EJERCICIO 121. Factorizar 2 en $\mathbb{Z}[i]$ y calcular el número de elementos de $\mathbb{Z}[i]/\langle 2 \rangle$.

EJERCICIO 122. Resolver en $\mathbb{Z}[\sqrt{2}]$ la congruencia $(2 + \sqrt{2})x \equiv 3 - \sqrt{2} \pmod{3}$.

EJERCICIO 123. Sea $a + bi \in \mathbb{Z}[i]$ con $ab \neq 0$. Demostrar que $a + bi$ es irreducible en $\mathbb{Z}[i]$ si, y sólo si, $a^2 + b^2$ es un número primo.

EJERCICIO 124. En el anillo $\mathbb{Z}[\sqrt{-2}]$ resolver el siguiente sistema de congruencias

$$\begin{aligned} x &\equiv 1 + 2\sqrt{-2} \pmod{2 - 3\sqrt{-2}} \\ x &\equiv 3 \pmod{1 + \sqrt{-2}} \end{aligned}$$

EJERCICIO 125. En el anillo $\mathbb{Z}[\sqrt{5}]$ comprobar que $4 = 2 \cdot 2$ y $4 = (1 + \sqrt{5})(-1 + \sqrt{5})$ son dos factorizaciones en irreducibles no equivalentes. ¿Es $1 + \sqrt{5}$ primo?.

EJERCICIO 126. Sea $\alpha = 1 + \sqrt{2} \in \mathbb{R}$. Razonar que el conjunto

$$\{f \in \mathbb{Q}[X] : f(\alpha) = 0\}$$

es un ideal principal de $\mathbb{Q}[X]$ y calcular un generador suyo.

EJERCICIO 127. Consideremos el anillo $A = \mathbb{Z}[\sqrt{3}]/\langle 3 \rangle$.

1. Calcular, si existe, el inverso en A de $a = (2 - \sqrt{3}) + \langle 3 \rangle$.
2. Sea $e \in A$ tal que $e^2 = e$. Demostrar que o bien $e = 0 + \langle 3 \rangle$, o bien $e = 1 + \langle 3 \rangle$.

EJERCICIO 128. Escoger la respuesta correcta. Sea $X = \{0, 1, 2, 3, 4\}$ y R la relación definida en $X \times X$ por $(a, b)R(c, d)$ si $a + 2d = c + 2b$ para $(a, b), (c, d) \in X \times X$. Entonces:

(a) R es una relación de orden.

(b) R no es una relación de equivalencia.
(c) R es una relación de equivalencia y $\{(0,0),(2,1),(4,2),(0,1),(2,2)\}$ es una clase de equivalencia bajo R.
(d) R es una relación de equivalencia y $\{(0,0),(2,1),(4,2),(0,1),(2,2)\}$ es una unión de dos clases de equivalencia bajo R.
(e) Ninguna de las otras afirmaciones es correcta.

EJERCICIO 129. Escoger la respuesta correcta. Sea X un conjunto con 6 elementos y $S \subseteq X$ un subconjunto de cardinal 3. Definimos la aplicación $f : X \to \mathcal{P}(X)$ declarando que $f(x) = S \cup \{x\}$ para $x \in X$. Sea $\sim_f$ la relación de equivalencia en X definida por f. Entonces

(a) El conjunto cociente $X/\sim_f$ tiene cardinal 2.
(b) El conjunto cociente $X/\sim_f$ tiene cardinal 3.
(c) El conjunto cociente $X/\sim_f$ tiene cardinal 4.
(d) El conjunto cociente $X/\sim_f$ tiene cardinal 6.
(e) El conjunto cociente $X/\sim_f$ tiene cardinal 1.

EJERCICIO 130. Escoger la respuesta correcta. Sea A un dominio de ideales principales y $p \in A$ irreducible. Entonces:

(a) $\frac{A}{\langle p \rangle}[X]$ es un Dominio Euclídeo.
(b) $\frac{A}{\langle p \rangle}[X]$ es un DIP y puede ser, para ejemplos concretos de A y p, un cuerpo.
(c) $\frac{A}{\langle p \rangle}[X]$ no tiene por qué ser un dominio de integridad.
(d) Ninguna de las otras afirmaciones es correcta.
(e) $\frac{A}{\langle p \rangle}[X]$ es un DFU, pero no necesariamente un DIP.

EJERCICIO 131. Escoger la respuesta correcta. Para $\alpha = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i \in \mathbb{C}$ definimos el conjunto $A = \{n \in \mathbb{Z} \mid \alpha^n = 1\}$.

(a) A es vacío.
(b) A tiene 8 elementos.
(c) $A = \mathbb{Z}_8$.
(d) $A = 8\mathbb{Z}$.
(e) Ninguna de las otras afirmaciones es correcta.

EJERCICIO 132. Escoger la respuesta correcta. El número de ideales del anillo $\mathbb{Z}_{24}$ es

(a) 1
(b) 4
(c) 6
(d) 8
(e) Ninguna de las otras afirmaciones es correcta.

EJERCICIO 133. Escoger la respuesta correcta. Sea A un DFU y $f = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 \in A[X]$ un polinomio primitivo. Supongamos que existe un homomorfismo de anillos $\phi : A \to \mathbb{Z}$ tal que $\phi(a_0) = 1, \phi(a_1) = 2, \phi(a_2) = 3, \phi(a_3) = 2, \phi(a_4) = 1$. Entonces:

(a) f es irreducible.
(b) f no tiene raíces en A.
(c) f no es irreducible.

(d) f tiene una raíz en el cuerpo de fracciones de A.
(e) No puede deducirse ninguna de las otras afirmaciones sobre f.

EJERCICIO 134. Escoger la respuesta correcta. Sean $a(X) = X^4 + X^3 + X + 1$ y $b(X) = X^4 + 2X^3 + X^2 + X + 1$ dos polinomios de $\mathbb{Z}_3[X]$. El máximo común divisor de $a(X)$ y $b(X)$ es un polinomio de grado

(a) 0
(b) 1
(c) 2
(d) 3
(e) 4

EJERCICIO 135. Escoger la respuesta correcta. Consideremos el anillo $R = \mathbb{Z}_2[X]/\langle X^3 + 1\rangle$. El cardinal del grupo de unidades $U(R)$ es

(a) 5
(b) 2
(c) 3
(d) 6
(e) 7

EJERCICIO 136. Escoger la respuesta correcta. Sea $A = \mathbb{Z}[\sqrt{2}]/\langle\sqrt{2}\rangle$. Entonces:

(a) A es un dominio euclídeo pero no es un cuerpo.
(b) A es un cuerpo finito.
(c) A es un dominio de integridad pero no es un cuerpo.
(d) A es un cuerpo infinito.
(e) A no es un cuerpo.

Bibliografía

1. J. B. Fraleigh, *Álgebra Abstracta*, Addison-Wesley Iberoamericana, Wilmington, Delaware, 1987.
2. J. Gómez Torrecillas, *Álgebra I*, apuntes curso 2018/2019. Universidad de Granada. http://digibug.ugr.es/handle/10481/54837
3. N. Jacobson, *Basic Algebra I*, Freeman and Co. San Francisco, 1980.
4. M. Queysanne, *Álgebra Básica*, Ed. Vicens-Vives, Barcelona, 1971.