Álgebra I

Curso 2018/2019 [1] **.**

José Gómez Torrecillas
Departamento de Álgebra
Universidad de Granada

[1] versión: 15 de diciembre de 2018

Índice general

Capítulo 1

Fundamentos

1.1. Conjuntos

Es notorio que una cualidad fundamental de las Mátemáticas es la precisión de los enunciados. Para ello, 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. La relación entre ambos conceptos está regulada por la *pertenencia* según las siguientes reglas.

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 "$a \in a$" para cualquier objeto a.

R4 Dado un objeto a, podemos formar el conjunto $\{a\}$ definido por las 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.

Con estas reglas, ya podemos comenzar a construir objetos matemáticos. Con tal fin, las definiciones son cruciales. Aquí está la primera.

DEFINICIÓN 1.1. Dados conjuntos X, Y, definimos su *unión* como el conjunto $X \cup Y$ determinado por los elementos a tales que $a \in X$ o bien $a \in Y$. Observemos que $X \cup Y = Y \cup X$.

EJEMPLO 1.2. 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 1.1, 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 1.3. De acuerdo con las reglas 5 y 4, podemos formar el conjunto $\{\emptyset\}$. Y ahora, según el Ejemplo 1.2, podemos formar el conjunto $\{\emptyset, \{\emptyset\}\}$. Éste ya tiene dos elementos distintos, ¿verdad?.

EJERCICIO 1.4. Sea X un conjunto. Demostrar que $X \cup \{\emptyset\} = X$ si, y sólo si, $\emptyset \in X$.

OBSERVACIÓN 1.5. La noción de unión de subconjuntos se extiende de manera obvia 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 $Y \in \Gamma$.

DEFINICIÓN 1.6. 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 $X \subseteq Y$.

Observemos que tener que $X \subseteq Y$ e $Y \subseteq X$ es lo mismo que decir que $X = Y$. Observemos también que $\emptyset \subseteq X$ cualquiera sea el conjunto X.

EJERCICIO 1.7. Sean X, Y conjuntos. Demostrar que $X \cup Y = Y$ si, y sólo si, $X \subseteq Y$.

EJERCICIO 1.8. Mostrar tres conjuntos X, Y, Z que verifiquen que $X \in Y \in Z$ y, al mismo tiempo, $X \subseteq Y \subseteq Z$.

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

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

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

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

DEFINICIÓN 1.9. Dados dos conjuntos X, Y, definimos su *intersección* como el conjunto $X \cap Y$ determinado por los elementos 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 1.10. Si X, Y son conjuntos, demostrar que $X \cap Y = Y$ si, y sólo si, $Y \subseteq X$.

OBSERVACIÓN 1.11. 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 1.12. Dado $X \subseteq Y$, definimos el *complemento* de X en Y 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, se suele escribir $\overline{X}$ para referirse a $Y \setminus X$.

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

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

1.2. Correspondencias y aplicaciones

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

EJERCICIO 1.14. Sean $I = \{\emptyset\}, II = I \cup \{I\}$. Describir explícitamente $II \times II$.

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 siguiente definición.

DEFINICIÓN 1.16. 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 1.17. En el conjunto II definido en el Ejercicio 1.14, definimos la relación $C \subseteq II \times II$ dada por xCy si, y sólo si, $x \in y$. Describir explícitamente todos los pares ordenados que pertenecen a C.

Volveremos más tarde sobre las relaciones, ahora nos vamos a concentrar en un tipo especial de correspondencias, las aplicaciones.

DEFINICIÓN 1.18. 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 $y \in Y$ tal que $(x, y) \in f$. Escribiremos $y = f(x)$, y diremos que y es la imagen de x por (o bajo) f. También diremos que f asigna y al x

La notación casi universalmente aceptada para denotar una aplicación es escribir $f : X \to Y$. El conjunto X es denominado *dominio* de f, en tanto que Y se denomina *rango* de f. En algunos textos se usa la palabra "función" como sinónimo de "aplicación".

EJEMPLO 1.19. Todo conjunto X da lugar automáticamente a una aplicación $id_X : X \to X$ llamada *identidad en* X, definida por $id_X(x) = x$ para todo $x \in X$.

DEFINICIÓN 1.20. Dadas aplicaciones $f : X \to Y$ y $g : Y \to Z$, definimos su *composición* $g \circ f : X \to Z$ 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:

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

Para una aplicación $f : X \to Y$, también usaremos la notación $X \xrightarrow{f} Y$.

EJERCICIO 1.21. Poner un ejemplo que demuestre que la composición de dos aplicaciones no siempre es posible.

PROPOSICIÓN 1.22. *Sean* $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$ *aplicaciones. Entonces* $(h \circ g) \circ f = h \circ (g \circ h)$.

DEMOSTRACIÓN. Se deja como ejercicio. □

EJERCICIO 1.23. Sea X un conjunto. ¿Cuántas aplicaciones hay de $\emptyset$ a X? ¿Cuántas aplicaciones hay de X a $\emptyset$?

DEFINICIÓN 1.24. 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 $y = f(x)$.

EJERCICIO 1.25. Poner un ejemplo de aplicación inyectiva que no sea sobreyectiva, y otro de aplicación sobreyectiva que no sea inyectiva.

DEFINICIÓN 1.26. Una aplicación se dice *biyectiva* si es inyectiva y sobreyectiva.

PROPOSICIÓN 1.27. *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. Definimos entonces 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 1.18. 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 $f \circ g = id_Y$. Por último, 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 $f \circ g = id_Y$. Como, 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 1.28. Dada una aplicación biyectiva (o biyección) $f : X \to Y$, la aplicación $g : Y \to X$ proporcionada por la Proposición 1.27 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 1.22, obtenemos

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

DEFINICIÓN 1.29. La aplicación $g : Y \to X$ dada por la Proposición 1.27 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 1.28) . 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 1.30. *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 1.27 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 1.28, de nuevo las ecuaciones anteriores implican que $(f^{-1})^{-1} = f$. □

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

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

EJERCICIO 1.31. 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 1.32. Demostrar que una aplicación $f : X \to Y$ es inyectiva si, y sólo si, existe $g : Y \to X$ tal que $g \circ f = id_X$.

1.3. Monoides. Los números naturales

Admitiremos 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, $n + 1$. Tal y como lo hemos expresado, estamos aceptando también 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 mediante $+$ se denotará como $m + n$.

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

DEFINICIÓN 1.33. Sea X un conjunto no vacío. Toda aplicación $* : X \times X \to X$ 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 requieren, para su manejo, de una simplificación en la notación general que usamos para las aplicaciones. Concretamente, si $* : X \times X \to X$ es una operación binaria, entonces, dado $(a, b) \in X \times X$, su imagen por $*$ habría de ser denotada por $*((a, b))$. Una primera simplificación, en la que no perdemos información, es prescindir de dos paréntesis, y escribir $*(a, b)$ en lugar $*((a, b))$. Pero, ya puestos, podemos suprimir, sin menguar la información, los paréntesis e incluso la coma, y escribir $a * b$ en lugar de $*((a, b))$. 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 1.34. Un *semigrupo* es un par $(S, *)$, donde S es un conjunto no vacío y $* : S \times S \to S$ es una aplicación (una operación binaria) tal que

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

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

DEFINICIÓN 1.35. Un semigrupo $(S, *)$ es un *monoide* si existe un *elemento neutro* para $*$, esto es, existe $e \in S$ tal que $e * a = a = a * e$ para todo $a \in S$. Diremos que $(S, *, e)$ es un monoide.

EJEMPLO 1.36. 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 1.37. Demostrar que, en un monoide, el elemento neutro es único.

DEFINICIÓN 1.38. Un semigrupo $(S, *)$ se dice *conmutativo* si $a*b = b*a$ para todo $a, b \in S$.

EJEMPLO 1.39. $(\mathbb{N}, +, 0)$ es un monoide conmutativo.

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

EJEMPLO 1.40. $(\mathbb{N}, \cdot, 1)$ es un monoide conmutativo.

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

EJEMPLO 1.41. Dado X un conjunto, $(\mathcal{P}(X), \cup, \emptyset)$ y $(\mathcal{P}(X), \cap, X)$ son monoides conmutativos.

Volvamos con los números naturales. Es difícil poner un límite de qué podemos suponer conocido o qué no sobre los mismos. Los ejemplos 1.39 y 1.40 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 estas asunciones nos parecen bastante obvias. Vamos a aceptar también una propiedad que, para algunas personas, puede no parecer tan obvia.

1.42. **Principio de inducción.** Sea $X \subseteq \mathbb{N}$ tal que $0 \in X$ y 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 1.43. 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 1.44 (Buena ordenación de los naturales). *Todo conjunto no vacío de números naturales tiene mínimo. Esto es, si* $X \subseteq \mathbb{N}$ *verifica que* $X \neq \emptyset$*, entonces existe* $m \in X$ *tal que* $x \geq m$ *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, 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

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

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. □

Recordemos que 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 $n \neq 0, 1$ es compuesto si no es primo. El número 1 ni es primo ni es compuesto. Euclides demostró hace 2.200 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 1.45. *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 1.44. 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 1.46. *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 tres elementos de* $\{a, b, c\}$*, entonces los divide a los tres.*

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, $da' = db' + c \geq db'$. Por tanto, $a' \geq b'$, 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. □

TEOREMA 1.47. *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 $p_1, \ldots, p_n$. Formemos el número $N = p_1 \cdots p_n + 1$. Observemos que $N \neq 0, 1$, luego, de acuerdo con el Lemma 1.45, 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 1.46, p es un divisor de 1. Esta contradicción demuestra que $p_1, \ldots, p_n$ no puede ser una lista completa de todos los números primos. Luego hay infinitos. □

Aquí va otro teorema atribuido a Euclides.

TEOREMA 1.48 (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 1.49. Es posible demostrar[1] que los números naturales q, r que aparecen en en el Teorema 1.48 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 $r = \mathrm{rem}(a, b)$, $q = \mathrm{quot}(a, b)$.

OBSERVACIÓN 1.50. 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 1.46, 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 de manera rápida?

1.4. Relaciones de equivalencia y orden. Construcción de los enteros.

Vamos a estudiar aspectos básicos de dos tipos de relaciones en un conjunto, las relaciones de equivalencia y las relaciones de orden, que están entre los fundamentos de muchas construcciones matemáticas. Comenzamos con dos propiedades comunes a ambas.

DEFINICIÓN 1.51. Sea R una relación en un conjunto no vacío X. Diremos que R es *reflexiva* si xRx para todo $x \in X$. Diremos que R es *transitiva* si para todo $x, y, z \in X$ las condiciones xRy e yRz implican xRz.

[1] Usando números enteros, es bastante fácil. Si sólo nos permitimos, en este momento, números naturales la demostración es algo más sutil. Puedes intentarlo.

Estamos preparados para definir qué es una relación de equivalencia. Las relaciones de equivalencia se darán siempre en conjuntos no vacíos, se diga esto o no explícitamente.

DEFINICIÓN 1.52. Sea R una relación en un conjunto X. Diremos que R es *simétrica* si para todo $x, y \in X$ la condición xRy implica yRx. La relación R es *de equivalencia* si es reflexiva, simétrica y transitiva.

EJEMPLO 1.53. Sea $n \in \mathbb{N}$, $n \neq 1$. 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 R_n en $\mathbb{N}$ por la condición aR_nb si $\mathrm{rem}(a, n) = \mathrm{rem}(b, n)$ para $a, b \in \mathbb{N}$. Se trata de una relación de equivalencia. El respeto a la tradición sugiere que escribamos $a \equiv b \pmod{n}$ para indicar aR_nb.

DEFINICIÓN 1.54. Sea R una relación de equivalencia en un conjunto 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 de X se dirá una clase de equivalencia bajo R si es de la forma $[x]_R$ para algún $x \in X$.

EJEMPLO 1.55. Consideremos la relación de equivalencia R_n en $\mathbb{N}$ descrita en la Definición 1.53. Para $r \in \{0, 1, \ldots, n-1\}$, tenemos que

$$[r]_{R_n} = \{qn + r \mid q \in \mathbb{N}\}.$$

Se suele escribir $\overline{r} = [r]_{R_n}$.

PROPOSICIÓN 1.56. *Sea* R *una relación de equivalencia en* X, $x, y \in X$. *Las siguientes condiciones son equivalentes.*

1. xRy;
2. $y \in [x]_R$;
3. $x \in [y]_R$;
4. $[x]_R \cap [y]_R \neq \emptyset$;
5. $[x]_R = [y]_R$.

DEMOSTRACIÓN. (1) $\Rightarrow$ (2). Por definición de $[x]_R$.
(2) $\Rightarrow$ (3). Como $y \in [x]_R$, tenemos que xRy. Al ser R simétrica, deducimos que yRx, lo que da que $x \in [y]_R$.
(3) $\Rightarrow$ (4). Como R es reflexiva, tenemos que $x \in [x]_R$. Así que, si $x \in [y]_R$, deducimos que $x \in [x]_R \cap [y]_R$.
(4) $\Rightarrow$ (5). Demostremos que $[x]_R \subseteq [y]_R$. Sea $t \in [x]_R$. Entonces xRt, de donde, por ser R simétrica, tRx. Por hipótesis, podemos tomar $z \in [x]_R \cap [y]_R$. Así, xRz y, por la propiedad transitiva, deducimos que tRz. Pero también tenemos que yRz, de donde zRy y, de nuevo por ser R transitiva, tRy. De donde, por la propiedad simétrica una vez más, yRt, esto es, $t \in [y]_R$. Análogamente, $[y]_R \subseteq [x]_R$.
(5) $\Rightarrow$ (1). Como R es reflexiva, $y \in [y]_R$. Así, $y \in [x]_R$, lo que da xRy. □

DEFINICIÓN 1.57. Con la notación de la Proposición 1.56, cualquier elemento $y \in [x]_R$ determina completamente la clase de equivalencia $[x]_R$. Cada uno de estos elementos y es un *representante* de $[x]_R$. Obviamente, x es también un representante de $[x]_R$, pero, normalmente, hay muchos para cada clase de equivalencia.

Ahora queremos explicar cómo hay una forma alternativa de ver una relación de equivalencia, a través de la noción de partición.

DEFINICIÓN 1.58. 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 1.59. Sea $X = \{1, 2, 3\}$. Calcular todas las particiones de X.

Cada relación de equivalencia en X da una partición de X. Para explicar esto, introducimos primero la noción de imagen de una aplicación. Así, si $f : A \to B$ es una aplicación, definimos su *imagen* como el conjunto $\mathrm{Im}(f) = \{f(a) \mid a \in A\}$. Observemos que $\mathrm{Im}(f)$ es un subconjunto de B.

PROPOSICIÓN 1.60. *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* $\mathrm{Im}(p_R)$ *es una partición de* X*.*

DEMOSTRACIÓN. Obviamente, $\mathrm{Im}(p_R)$ es un subconjunto no vacío de $\mathcal{P}(X)$. 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 1.58. 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 1.56, $\emptyset = [x]_R \cap [y]_R = \mathcal{C} \cap \mathcal{D}$. □

La partición determinada por una relación de equivalencia tiene un nombre especial.

DEFINICIÓN 1.61. Sea R una relación de equivalencia en un conjunto X. El conjunto $\mathrm{Im}(p_R) \subseteq \mathcal{P}(X)$ definido en la Proposición 1.60 se llama *conjunto cociente de* X *bajo (o con respecto de)* R, y se denota X/R.

Sintéticamente, se suele decir que el conjunto cociente X/R definido en 1.61 es el "conjunto de las clases de equivalencia" de X bajo R. Pero, si releemos con cuidado desde la Definición 1.58, vemos que X/R no es sino **la partición** de X definida por R. En particular, los elementos de X/R no son elementos de X, sino subconjuntos de X. La aplicación "corestricción" 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 $x \in X$.

EJEMPLO 1.62. Continuamos con el Ejemplo 1.55. El conjunto cociente es, en este caso,

$$\mathbb{N}/R_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Obsérvese que, a pesar de ser $\mathbb{N}$ infinito, el conjunto cociente $\mathbb{N}/R_n$ tiene n elementos. Claro, que cada elemento es un conjunto infinito.

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 1.63. Sea $f : X \to C$ 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.

EJERCICIO 1.64. Sea $f : X \to Y$ una aplicación entre conjuntos no vacíos, y $\sim_f$ la relación de equivalencia en X definida por f. Denotemos por $\pi_{\sim_f} : X \to X/\sim_f$ la proyección canónica. Demostrar que existe una aplicación inyectiva $\widehat{f} : X/\sim_f \to Y$ tal que $f = \widehat{f} \circ \pi_{\sim_f}$. Deducir que la correstricción de $\widehat{f}$ da una biyección $\widetilde{f} : X/\sim_f \to \mathrm{Im}(f)$.

DEFINICIÓN 1.65. 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 $\sim_{p^\Gamma}$ 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 1.66. *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. □

EJERCICIO 1.67. 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 1.63). 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 $X/\sim_f$.

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.

EJEMPLO 1.68. Consideremos la relación R en $\mathbb{N} \times \mathbb{N}$ definida, para $(n, m), (n', m') \in \mathbb{N} \times \mathbb{N}$, por la condición $(n, m)R(n'm')$ si (y sólo si) $n + m' = m + n'$. Se trata de una relación de equivalencia. En efecto, es muy fácil ver que es reflexiva y simétrica. Para comprobar que es transitiva, tomemos $(n, m), (n', m'), (n'', m'') \in \mathbb{N}\times\mathbb{N}$ tales que $(n, m)R(n', m')$ y $(n', m')R(n'', m'')$. Entonces $n + m' = m + n'$ y $n' + m'' = m' + n''$. Sumando los miembros al mismo lado de cada igualdad, obtenemos $n+m'+n'+m'' = m+n'+m'+n''$. De donde[2] $n + m'' = m + n''$, esto es, $(n, m)R(n'', m'')$.

DEFINICIÓN 1.69. El conjunto cociente

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

definido por la relación de equivalencia expuesta en el Ejemplo 1.68 se llama *conjunto de los números enteros*.

Vamos a ver que el conjunto $\mathbb{N}$ se puede identificar con un subconjunto de $\mathbb{Z}$ y que el éste último puede ordenarse de manera compatible con el orden de $\mathbb{N}$. Daremos primero la noción de relación de orden.

DEFINICIÓN 1.70. Una relación R en un conjunto X se dice *antisimétrica* si para todo $x, y \in X$, la condición xRy e yRx implica $x = y$.

DEFINICIÓN 1.71. Una relación en un conjunto X se dice *de orden* si es reflexiva, antisimétrica y transitiva. Es usual denotar a tal relación por símbolos como $\preceq$, y se suele decir que $(X, \preceq)$ es un *conjunto ordenado*. La relación de orden $\preceq$ se *total* si para todo $x, y \in X$, ocurre que $x \preceq y$ o bien $y \preceq x$. Una relación de orden no total se llama a veces *parcial*.

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

EJEMPLO 1.72. Se tiene un conjunto (parcialmente) ordenado $(\mathcal{P}(X), \subseteq)$ para todo conjunto X.

EJEMPLO 1.73. Un conjunto con un orden total es $(\mathbb{N}, \leq)$, donde $\leq$ es el orden natural.

EJEMPLO 1.74. Para $a, b \in \mathbb{N}_+ = \mathbb{N} \setminus \{0\}$, escribamos $a \mid b$ cuando a sea un divisor de b. Es claro que $(\mathbb{N}_+, \mid)$ es un conjunto ordenado. Este orden es parcial.

Para comparar conjuntos ordenados, se usa la noción de homomorfismo de conjuntos ordenados (a veces, se llaman aplicaciones no decrecientes).

DEFINICIÓN 1.75. Sean $(X, \preceq), (Y, \leq)$ conjuntos ordenados. Una aplicación $f : X \to Y$ es un *homomorfismo de conjuntos ordenados* si para todo $x, x' \in X$ la condición $x \preceq x'$ implica que $f(x) \leq f(x')$. El homomorfismo f es un *isomorfismo de conjuntos ordenados* si es biyectiva y su inversa $f^{-1} : Y \to X$ es homomorfismo de conjuntos ordenados.

EJEMPLO 1.76. La aplicación $\mathrm{id}_{\mathbb{N}_+} : \mathbb{N}_+ \to \mathbb{N}_+$ es un homomorfismo del conjunto ordenado $(\mathbb{N}_+, |)$ al conjunto ordenado $(\mathbb{N}_+, \leq)$. Esta aplicación no es un isomorfismo de conjuntos ordenados. ¿Por qué?

EJEMPLO 1.77. Si $(X, \preceq)$ es un conjunto ordenado, todo subconjunto $Y \subseteq X$ es un conjunto ordenado con la restricción de la relación $\preceq$.

PROPOSICIÓN 1.78. *La aplicación $\iota : \mathbb{N} \to \mathbb{Z}$ definida por $\iota(n) = [(n, 0)]_R$ para todo $n \in \mathbb{N}$ es inyectiva. Existe una relación de orden total en $\mathbb{Z}$ tal que ι es un homomorfismo de conjuntos ordenados y su correstricción $\iota : \mathbb{N} \to \mathrm{Im}(\iota)$ es un isomorfismo de conjuntos ordenados.*

DEMOSTRACIÓN. Veamos primero que ι es inyectiva: si $n, m \in \mathbb{N}$ son tales que $\iota(n) = \iota(m)$, entonces $[(n, 0)]_R = [(m, 0)]_R$. Según la Proposición 1.56, $(n, 0)R(m, 0)$, de donde $n + 0 = 0 + m$, esto es, $n = m$. Vamos a definir ahora la relación de orden $\preceq$ en $\mathbb{Z}$. Dados $[(a, b)]_R, [(c, d)]_R \in \mathbb{Z}$, declaramos que $[(a, b)]_R \preceq [(c, d)]_R$ si y sólo si $a + d \leq b + c$, donde esta última desigualdad es de números naturales. Ahora tenemos un problema: aparentemente, la definición que hemos dado de $\preceq$ depende de los representantes de las clases de equivalencia escogidos. Concretamente, si tenemos que

$$[(a, b)]_R = [(a', b')]_R \text{ y } [(c, d)]_R = [(c', d')]_R, \tag{1.3}$$

tendremos que ver que la condición $a + d \leq b + c$ es equivalente a la condición $a' + d' \leq b' + c'$, para que la definición de $\preceq$ sea coherente. Supongamos, pues, que $a + d \leq b + c$. Entonces $a' + d' + b + c = a + b' + d + c' \leq b + c + b' + c'$, donde, en la primera igualdad, hemos usado (1.3). Por tanto, $a' + d' \leq b' + c'$. La implicación recíproca se demuestra igual.

Es bastante fácil comprobar que esta relación $\preceq$ es de orden, es decir, reflexiva, transitiva y antisimétrica, y se deja como ejercicio.

Supongamos ahora que $m, n \in \mathbb{N}$. Es bastante obvio que $n \leq m$ si, y sólo si, $\iota(n) \preceq \iota(m)$. En particular, ι es un homomorfismo de conjuntos ordenados. Hemos de demostrar ahora que $\iota^{-1} : \mathrm{Im}(\iota) \to \mathbb{N}$ es un homomorfismo de conjuntos ordenados. Tomados $x \preceq y \in \mathrm{Im}(\iota)$, existen $n, m \in \mathbb{N}$ tales que $[(n, 0)]_R = x, [(m, 0)]_R = y$. Así que $n \leq m$ y, por otra parte, $n = \iota^{-1}(x), m = \iota^{-1}(y)$. □

La Proposición 1.78 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 $\mathbb{Z}$.

Capítulo 2

Anillos

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

Un anillo combina dos estructuras de monoide. Una de ellas disfruta, además, de una propiedad adicional que la hace un grupo. Como los grupos son objetos fundamentales en Matemáticas, definamos esta noción.

DEFINICIÓN 2.1. 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 2.2. 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 2.3. 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 $-a + a = 0$, que se suele llamar *opuesto* de a. Se suele usar 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 Geometría.

OBSERVACIÓN 2.4. 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.

EJERCICIO 2.5. 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 $k, l \in \mathbb{N}$.

DEFINICIÓN 2.6. 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 2.7. Dado un conjunto X, consideremos

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

Es claro que $(\mathrm{Sym}(X), \circ, \mathrm{id}_X)$ es un submonoide de $(\mathrm{Map}(X, X), \circ, \mathrm{id}_X)$. Se deduce de la Proposición 1.27 que $\mathrm{Sym}(X)$ es un grupo, llamado *grupo de permutaciones* de X.

TEOREMA 2.8. *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 $n + k = m$.*

DEMOSTRACIÓN. Consideremos la relación de equivalencia R en $\mathbb{N} \times \mathbb{N}$ del Ejemplo 1.68. 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 $[(a,b)]_R = [(a',b')]_R$ y $[(c,d)]_R = [(c',d')]_R$. Usando las propiedades conmutativa y asociativa de $+$, 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. Recordemos que teníamos 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, como se caracteriza ahora el orden en $\mathbb{Z}$ que introdujimos en la Proposición 1.78. Recordemos que $[(a,b)]_R \leq [(c,d)]_R$ si, y sólo si, $a+c \leq b+c$. 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 2.9. Con la notación del Ejercicio 2.5, supongamos ahora que A es un grupo. Usamos notación multiplicativa (ver Observación 2.4). 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 $x, y \in \mathbb{Z}$.

DEFINICIÓN 2.10. 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 2.11. 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 2.12. 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 2.13. Sean A, B anillos. En el producto cartesiano $A \times B$ definimos las operaciones $(a, b) + (a', b') = (a + a', b + b')$ y $(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$. Demostrar que, con estas operaciones, $A \times B$ es un anillo.

EJERCICIO 2.14. 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 2.15. *El grupo conmutativo* $(\mathbb{Z}, +, 0)$ *admite una estructura 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:

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

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 $\mathbb{Z}$. □

EJERCICIO 2.16. Con la notación del Ejercicio 2.9, demostrar que $(a^x)^y = a^{xy}$ para todo $x, y \in \mathbb{Z}$.

OBSERVACIÓN 2.17. 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.

DEFINICIÓN 2.18. Sea $(A, *, e)$ un grupo y $B \subseteq A$ un submonoide. Diremos que B es un *subgrupo* si $(B, *, e)$ es un grupo.

EJERCICIO 2.19. 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 2.20. *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 2.19, $n\mathbb{Z}$ 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 2.8, 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 $\mathbb{N}$, podemos tomar el mínimo n de $I \cap \mathbb{N}_+$. Observemos[1] que $n\mathbb{Z} \subseteq I$. Para demostrar la inclusión recíproca, 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 $r = 0$. 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 2.20 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 2.21. 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 2.22 (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 2.20 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 2.23. Los números q y r que aparecen en el Teorema 2.22 se llaman, respectivamente, *cociente* y *resto* de la división de m entre n. Usaremos la notación $\mathrm{quot}(a, b) = q$ y $r = \mathrm{rem}(a, b)$.

OBSERVACIÓN 2.24. 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 2.25. 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. Comencemos fijando alguna nomenclatura.

DEFINICIÓN 2.26. 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.

[1] En realidad, esto requiere una pequeña demostración por inducción

OBSERVACIÓN 2.27. 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 2.28. *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 2.29. *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 $mcd(a, b)$.*

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 2.19, $ka + lb - (k'a + l'b) = (k - k')a + (l - l')b \in I$. Por el Teorema 2.20, existe $d \in \mathbb{N}$ tal que $I = d\mathbb{Z}$. Bien, como $a\mathbb{Z} \subseteq d\mathbb{Z}$, deducimos del Lema 2.28 que $d|a$. Análogamente, $d|b$. Ahora, supongamos que $d'|a$ y $d'|b$. Por el Lema 2.28, 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 2.28 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 2.30. Si a o b es no nulo, entonces $mcd(a, b)$ 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, $mcd(0, 0) = 0$, 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 a 0.

He aquí una consecuencia de la demostración de la Proposición 2.29.

TEOREMA 2.31 (Identidad de Bezout). *Dados $a, b \in \mathbb{N}$, y $d = mcd(a, b)$, existen $u, v \in \mathbb{Z}$ tales que $d = ua + vb$.*

DEMOSTRACIÓN. Hemos visto en la demostración de la Proposición 2.29 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.

PROPOSICIÓN 2.32. *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 $mcm(a, b)$.*

DEMOSTRACIÓN. Observemos que $I = a\mathbb{Z} \cap b\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$. Por el Teorema 2.20, existe $m \in \mathbb{N}$ tal que $I = m\mathbb{Z}$. Ahora, la demostración sigue una línea argumental similar a la de la Proposición 2.29, y se deja su completación como ejercicio. □

OBSERVACIÓN 2.33. 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 2.34. Completar la demostración de la Proposición 2.32.

Vamos ahora a exponer un algoritmo fundamental en la aritmética entera.

TEOREMA 2.35. *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*

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

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[2] 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 definidos $u_i, v_i, u_{i-1}, v_{i-1}$, 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,

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

□

De la demostración del Teorema 2.35, deducimos el Algoritmo 1, que se llama *Algoritmo de Euclides Extendido*.

TEOREMA 2.36. *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 2.35. □

[2] Ponemos $r = \mín\{r_i \mid i \geq 1\}$. 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.

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 $i = 0, 1, \dots, h, h+1$,
$r_{h+1} = 0$,
$r_h = mcd(a, b)$,
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**
  $q \leftarrow \text{quot}(r_{i-1}, r_i)$
  $r \leftarrow \text{rem}(r_{i-1}, r_i)$
  $r_{i+1} \leftarrow r$
  $u_{i+1} \leftarrow q u_{i-1} - u_i$
  $v_{i+1} \leftarrow q v_{i-1} - v_i$
  $i \leftarrow i + 1$
return $\{u_i, v_i, r_i\}_{i=0,\dots,h,h+1}$

OBSERVACIÓN 2.37. Como demostraremos en un contexto más general, $mcm(a, b) = a|u_{h+1}| = b|v_{h+1}|$.

EJEMPLO 2.38. 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, $mcd(2018, 1918) = 2$ y $2 = 211 \times 2018 - 222 \times 1918$. Además, según la Observación 2.37, $mcm(2018, 1918) = 1935262$.

Observemos que, de acuerdo con las demostraciones de las proposiciones 2.29 y 2.32, tenemos que

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

y

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

Ahora nos dirigimos a demostrar el Teorema Fundamental de la Aritmética, que afirma que todo número natural es producto, de manera esencialmente única, de números primos.

LEMA 2.39. *Sean* $a, b, n, m \in \mathbb{N}$ *tales que* $na = mb$. *Si* $mcd(a, b) = 1$, *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. □

LEMA 2.40. *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. Pongamos $d = mcd(p, a)$. Por ser p primo, tenemos que $d = p$ o bien $d = 1$. En el primer caso, p divide a a. En el segundo, $mcd(p, a) = 1$ y $pc = ab$ para algún $c \in \mathbb{N}$. Por el Lema 2.39, b es un múltiplo de p. □

TEOREMA 2.41. *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 1.45, 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 el Lema 2.40, p_1 ha de ser divisor de algún q_j. Al ser éste último 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. □

EJEMPLO 2.42 (Ecuaciones Diofánticas). 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 2.44.) 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 $d = mcd(a, b)$. 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 $d = mcd(a, b)$.

Ahora, veamos cómo se calculan 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 una parte, que $a'(x - x_0) = b'(y_0 - y)$, y, de otra, $1 = a'u + b'v$. Por tanto, $mcd(a', b') = 1$.

Por el Lema 2.39, $|x-x_0|$ es un múltiplo de b' e $|y-y_0|$ es un múltiplo de a'. Esto es, existen $k, l \in \mathbb{Z}$ tales que $x-x_0 = kb'$ e $y-y_0 = la'$. De manera que $a'b'k = -a'b'l$, 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 2.43. Resolvamos la ecuación diofántica

$$2018x + 1918y = 100$$

Usaremos los datos calculados en el Ejemplo 2.38. Como $\mathrm{mcd}(2018, 1918) = 2$, que es un divisor de 100, la ecuación tiene soluciones enteras. Siguiendo la notación del Ejemplo 2.42, 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

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

OBSERVACIÓN 2.44. Aunque el procedimiento discutido en el Ejemplo 2.42 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 permite 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 a otros ámbitos importantes, como por ejemplo los espacios vectoriales cocientes.

Dado un subgrupo I de un grupo abeliano $(A, +, 0)$, y $a \in I$, 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 2.45. *Sea I un subgrupo de un grupo abeliano $(A, +, 0)$. La relación R en A definida, para $a, b \in I$, por aRb si, y sólo si, $a - b \in A$ 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 $a, b, c \in R$ 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 conluimos que es de equivalencia.

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

PROPOSICIÓN 2.46. *Dado un subgrupo* I *de un grupo aditivo* $(A,+,0)$*, denotemos por* A/I *el conjunto cociente de* A *bajo la relación de equivalencia descrita en el Lema 2.45. Entonces* A/I *es un grupo con la suma definida por*

$$(a+I)+(b+I)=(a+b)+I, \qquad a+I, b+I \in A/I. \tag{2.4}$$

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 (2.4) 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 (2.4) es asociativa y conmutativa, que el elemento neutro es I, y que si $a+I$, entonces su opuesto es $-a+I$. En definitiva, A/I es un grupo conmutativo. □

EJERCICIO 2.47. Completar la demostración de la Proposición 2.46.

EJEMPLO 2.48. 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 n elementos.

Recordemos que la $\mathbb{Z}$ 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 conmutativa. La construcción general es la siguiente.

DEFINICIÓN 2.49. 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 2.50. *Sea* I *un ideal de un anillo* A*. Entonces el grupo* A/I *tiene estructura de anillo, con la multiplicación dada por*

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

Este anillo se llama anillo cociente de A módulo I.

DEMOSTRACIÓN. Como de costumbre, hemos de comprobar que la multiplicación dada por (2.5) 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. □

EJERCICIO 2.51. Terminar la demostración de la Proposición 2.50.

EJERCICIO 2.52. Si A es un grupo conmutativo finito, e I un subgrupo de A, demostrar que $\mathtt{card}(A) = \mathtt{card}(I)\mathtt{card}(A/I)$, donde $\mathtt{card}(X)$ denota el cardinal (número de elementos) de un conjunto finito X.

EJEMPLO 2.53. 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 2.50, 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 $z \in \mathbb{Z}$, usemos la notación simplificada $\overline{z} = z + n\mathbb{Z}$.

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,

$$a \equiv b \pmod{I} \Leftrightarrow a + I = b + I \Leftrightarrow a - b \in I. \tag{2.6}$$

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 2.54. Consideremos la *ecuación en congruencias o modular*

$$ax \equiv b \pmod{n}, \tag{2.7}$$

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 (2.7) si y sólo si existe $k \in \mathbb{Z}$ tal que $ax - b = kn$. Equivalentemente, $ax - kn = b$. Así que (2.7) se reduce a una ecuación diofántica (ver Observación 2.44). Así que tiene solución si, y sólo si, $\mathtt{mcd}(a, n)|b$, y su resolución se puede extraer resolviendo la ecuación diofántica. También podemos usar una procedimiento que describimos seguidamente.

Observemos que, en caso de existir solución de (2.7), tomamos $a', b' \in \mathbb{Z}$ y $n' \in \mathbb{N}$ tales que $a = a'd$, $b = b'd$, $n = n'd$, para $d = \mathtt{mcd}(a, n)$. Así, $ax - kn = b$ es equivalente a $a'x - b' = kn'$, esto es, (2.7) es equivalente a

$$a'x \equiv b' \pmod{n'}. \tag{2.8}$$

La ventaja ahora es que $\mathtt{mcd}(a', n') = 1$. Si calculamos $u, v \in \mathbb{Z}$ tal que $1 = a'u + n'v$, entonces (2.8) es equivalente a

$$x \equiv ub' \pmod{n'}, \tag{2.9}$$

ya que, operando en $\mathbb{Z}_{n'}$, tenemos que (2.8) 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 (2.8) por $\overline{u}$, tenemos que $\overline{x} = \overline{ub'}$ en $\mathbb{Z}_{n'}$. Esto es equivalente a (2.9). Por tanto, la solución general de (2.7), cuando existe, es

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

Antes de abordar la resolución de sistemas de ecuaciones en congruencias (2.7), 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 2.55. *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. □

EJERCICIO 2.56. 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 2.57. 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 2.58. *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* $I_1, \ldots, I_t$ *son ideales de* A, *con* $t \geq 2$, *se tiene que* $I_1 + I_j = A$ *para todo* $j = 2, \ldots, t$ *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, $I + K = A$.

Para el caso general, observemos que $t = 2$ es trivial. Razonando inductivamente sobre $t \geq 2$ supongamos como hipótesis de inducción que $I_1 + I_j = A$ para todo $j = 2, \ldots, t$ implica que $I_1 + \bigcap_{j=2}^{t} I_j = A$. Partiendo de $I + I_j = A$ para todo $j = 2, \ldots, t + 1$, pongamos $I = I_1, J = \bigcap_{j=2}^{t} I_j, K = I_{t+1}$. Tenemos entonces que $I + J = A$ e $I + K = A$. Como hemos demostrado antes, esto implica 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. □

TEOREMA 2.59 (Teorema Chino del Resto, versión abstracta.). *Sean* $I_1, \ldots, I_t$ *ideales de un anillo* A, *con* $t \geq 2$. *Cada sistema de congruencias*

$$\begin{cases} x \equiv b_1 \pmod{I_1} \\ x \equiv b_2 \pmod{I_2} \\ \cdots\cdots\cdots\cdots \\ x \equiv b_t \pmod{I_t} \end{cases} \tag{2.10}$$

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

DEMOSTRACIÓN. Supongamos primero que $I_i + I_j = A$ para cualesquiera $i \neq j$. Por el Lema 2.58, para todo $i = 1, \ldots t$, tenemos que $I_i + \bigcap_{j \neq i} I_j = A$. Para cada $i = 1, \ldots, t$, 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 $b_1, b_2, \ldots, b_t \in A$, pongamos $x = \sum_{i=1}^{t} b_i p_i \in A$. Así, para cada $j = 1, \ldots, t$, tenemos

$$x + I_j = \sum_{i=1}^{t} b_i p_i + I_j \overset{(*)}{=} b_j p_j + I_j = b_j(1 - a_j) + I_j = b_j - b_j a_j + I_j \overset{(**)}{=} b_j + I_j, \tag{2.11}$$

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 (2.11) dice que $x \equiv b_j \pmod{I_j}$ para $j = 1, \ldots, t$, concluimos que (2.10) tiene solución.

Recíprocamente, supongamos que cada sistema de congruencias (2.10) tiene solución en A. Dado $i = 1, \ldots, t$, 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 2.58, $I_j + I_i = A$ para todo $j \neq i$. □

COROLARIO 2.60 (Teorema Chino del Resto). *Supongamos números naturales* $n_1, n_2, \ldots, n_t$. *Cada sistema de congruencias*

$$\text{(2.12)} \qquad \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \cdots\cdots\cdots\cdots \\ x \equiv b_t \pmod{n_t} \end{cases}$$

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

OBSERVACIÓN 2.61. Es posible que, sin la condición $\mathrm{mcd}(n_i, n_j) = 1$ para $i \neq j$, el sistema (2.12) tenga solución para algunos $b_1, b_2, \cdots, b_t \in \mathbb{Z}$ **concretos**.

EJEMPLO 2.62. 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

$$\text{(2.13)} \qquad x = 2 + 5k, \qquad k \in \mathbb{Z}.$$

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 (2.13), 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 (2.13), obtenemos

$$\text{(2.14)} \qquad x = 2 + 15m, \qquad m \in \mathbb{Z},$$

que es la solución general del sistema. De hecho, hemos deducido que cualquier solución es de la forma descrita en (2.14), y es fácil comprobar, sustituyendo, que todo número entero de la forma descrita en (2.14) es, realmente, solución del sistema.

EJERCICIO 2.63. Sean I y J subgrupos de un grupo aditivo A tales que $I \subseteq J$. Demostrar que J/I es un subgrupo de A/J. Si, además, A es un anillo e I, J son ideales de A, entonces J/I es un ideal de A/I.

EJERCICIO 2.64. 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 2.65. 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

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

DEFINICIÓN 2.66. 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. $1 \in S$.

EJEMPLO 2.67. 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 $0, 1 \neq D \in \mathbb{N}$, libre de cuadrados[3], 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, en realidad, para definir $\mathbb{Z}[\sqrt{D}]$ no es necesario en realidad admitir antes $\mathbb{R}$, como veremos más adelante.

EJEMPLO 2.68. Ya que hemos aceptado $\mathbb{R}$, podemos aceptar también 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

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \tag{2.15}$$

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 (2.15), 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.

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

[3]Es decir, en la factorización de D como producto de primos todos éstos son distintos.

DEFINICIÓN 2.69. 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 $a, a' \in A$.

EJERCICIO 2.70. 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 $a \in A$.

Por *grupo aditivo* entendemos un grupo conmutativo denotado aditivamente.

EJEMPLO 2.71. 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 2.72. *Sea $f : A \to B$ un homomorfismo de grupos, donde A y B son grupos conmutativos denotados aditivamente. Entonces $\mathrm{Im}(f)$ es un subgrupo de B*

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

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

$$\widetilde{f} : A/\mathrm{Ker}(f) \to \mathrm{Im}(f) \tag{2.16}$$

que verifica

$$\widetilde{f}(a + \mathrm{Ker}(f)) = f(a), \qquad \textit{para todo } a \in A. \tag{2.17}$$

DEMOSTRACIÓN. Veamos primero que $\mathrm{Im}(f)$ es un subgrupo de B. Tomemos dos elementos de $\mathrm{Im}f(f)$, que son de la forma $f(a), f(a')$ para $a, a' \in A$. Usando el Ejercicio 2.70, 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 2.70. 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 del Ejercicio 1.64 existe una biyección $\widetilde{f} : A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ que verifica (2.17). Por último,

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

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

EJEMPLO 2.73. 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 2.74. 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 2.72 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 2.75. 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 $f(\overline{x}) = \overline{dx}$, para $\overline{x} \in \mathbb{Z}_n$ está bien definida, y es un homomorfismo inyectivo de grupos.

Vayamos con los homomorfismos de anillos.

DEFINICIÓN 2.76. Sean A y B. 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, para los 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 2.77. Si I es un ideal de un anillo conmutativo A, entonces la proyección canónica $\pi : A \to A/I$ es un homomorfismo de anillos.

EJEMPLO 2.78. Consideremos, en el ejercicio 2.75, que $n \neq m \neq 1$. Entonces el homomorfismo de grupos f allí definido no es homomorfismo de anillos ya que, por ejemplo, $f(\overline{1}) = \overline{d} \neq \overline{1}$.

Bien, para formular la versión para anillos del Teorema 2.72, necesitamos primero dar la noción de subanillo.

TEOREMA 2.79. *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 2.72 es un isomorfismo de anillos.*

DEMOSTRACIÓN. En vista de lo afirmado en el Teorema 2.72, 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:

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

□

EJEMPLO 2.80. Consideremos el anillo $\mathbb{Z}[x]$ de funciones polinómicas con coeficientes enteros definido en el Ejemplo 2.68. 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 2.79, $\mathrm{Im}(ev_r)$ 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 $\mathbb{Z}[x]$.

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 2.81. 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 2.82. Calcular todos los homomorfismos de anillos de $\mathbb{Z}_n$ a $\mathbb{Z}_m$, para $n, m \in \mathbb{N}$.

En este curso, vamos a dar varios métodos para construir nuevos anillos a partir de anillos conocidos. El primero ha sido el anillo cociente A/I definido a partir de un ideal I de un anillo conmutativo A. Veamos un segundo método, el producto de anillos.

DEFINICIÓN 2.83. Sean $A_1, A_2, \ldots, A_t$ anillos. Consideremos el producto cartesiano

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

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

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

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

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

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 $(1, 1, \ldots, 1)$. Este anillo se llama *anillo producto* de $A_1, A_2, \ldots, A_t$. Es conmutativo si cada uno de los A_i's lo es.

EJEMPLO 2.84. 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 para expresar precisamente qué es "esencialmente".

DEFINICIÓN 2.85. Sean A y B anillos. Un isomorfismo de anillos de A a B es un homomorfismo biyectivo de anillos $f : A \to B$. En tal caso, $f^{-1} : B \to A$ es también un isomorfismo de anillos. Si existe un isomorfismo de anillos de A a B,diremos que A y B son *isomorfos*, y escribiremos abreviadamante $A \cong B$, cuando el contexto descarte toda ambigüedad.

TEOREMA 2.86 (Teorema Chino del Resto, versión homomorfismo). *Sean $I_1, I_2, \ldots, I_t$ ideales de un anillo A. Entonces la aplicación*

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

definida por $f(a) = (a + I_1, a + I_2, \ldots, a + I_t)$ 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, induce en el cociente A/I un homomorfismo inyectivo de anillos

$$\widetilde{f} : A/I \to A/I_1 \times A/I_2 \times \cdots \times A/I_t, \qquad \widetilde{f}(a + I) = (a + I_1, a + I_2, \ldots, a + I_t).$$

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 $a \in \mathrm{Ker}(f)$ si, y sólo si $a + I_i = I_i$ para todo $i = 1, \ldots, t$, esto es, $a \in I_i$ para todo $i = 1, \ldots, t$. Por tanto, $\mathrm{Ker}(f) = I$. El Teorema 2.79 da ahora el homomorfismo inyectivo $\widetilde{f}$. Cuándo éste es sobreyectivo y, por tanto, un isomorfismo, es consecuencia del Teorema 2.59. □

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

DEFINICIÓN 2.87. 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.

EJEMPLO 2.88. Volvamos a $\mathbb{Z}_n$. La ecuación modular (2.7) es equivalente a la ecuación en $\mathbb{Z}_n$

$$\overline{a}\,\overline{x} = \overline{b}. \tag{2.18}$$

Si tomamos $\overline{b} = \overline{1}$, tenemos que la ecuación (2.18) 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 2.89. Un anillo conmutativo no trivial A es un *cuerpo* si $U(A) = A \setminus \{0\}$.

EJEMPLO 2.90. Se sigue del Ejemplo 2.88 que el anillo $\mathbb{Z}_n$ es un cuerpo si, y sólo si, n es un número primo.

EJEMPLO 2.91. El anillo $\mathbb{R}$ es un cuerpo.

EJERCICIO 2.92. Demostrar que si $A_1, \ldots, A_t$ 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 2.93. *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* $m, n \in \mathbb{N}_+$ *son coprimos entre sí, 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* $p_1, \ldots, p_t$ *son primos distintos y* $e_1, \ldots, e_t \in \mathbb{N}_+$, *entonces*

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

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 2.86, 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 $mcm(m,n) = mn$, 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 2.88, $\varphi(k)$ 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 $mcd(u, p_1^{e_1}) = 1$. Es más fácil contar aquellos u tales que $mcd(u, p_1^{e_1}) \neq 1$. 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 uk, 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 inmediatamente del apartado anterior teniendo en cuenta que $n = p_1^{e_1} \cdots p_t^{e_t}$. □

Vamos a concluir con un teorema de Euler que tiene importancia tanto teórica como práctica[4]

LEMA 2.94. *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 $Ker(f)$ es un subgrupo de $\mathbb{Z}$, por lo que, de acuerdo con el Teorema 2.20, existe $n \in \mathbb{N}$ tal que $Ker(f) = n\mathbb{Z}$. Por el Teorema 2.72, $Im(f) \cong \mathbb{Z}_n$. Como G es finito, deducimos que $n > 0$. Por el Ejercicio 2.52, n es un divisor de m. Por tanto, $e = f(\overline{0}) = f(\overline{m}) = g^m$. □

TEOREMA 2.95. *Sea $n \in \mathbb{N}$, $n \neq 0, 1$. Entonces, para todo $a \in \mathbb{Z}$ tal que $mcd(a,n) = 1$, tenemos que*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{2.19}$$

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 2.94 que $\overline{a}^{\varphi(n)} = \overline{1}$ en $\mathbb{Z}_n$. Esta igualdad es equivalente a (2.19). □

EJEMPLO 2.96. 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.

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

EJERCICIO 2.97. Sean I, J subgrupos de un grupo aditivo A tales que $I \subseteq J$. Dar un isomorfismo de grupos

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

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

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 $\iota : \mathbb{R} \to \mathbb{R}$, 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 tal que cualquier elemento no nulo $f \in P$ se representa de manera única como*

$$f = f_0 + f_1 X + \cdots + f_n X^n, \tag{3.1}$$

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

$$S = \mathrm{Map}(\mathbb{N}, A),$$

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 $f = (f_n)_{n\geq 0}, g = (g_n)_{n\geq 0} \in P$, 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 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 $f(hg)$ es

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

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, que no es tampoco difícil.

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 tales que 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 $f, g \in P$ y $f_i = 0$ existen $n, m \in \mathbb{N}$ 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, 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. □

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

OBSERVACIÓN 3.5. 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 3.6 (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* $\phi(X) = b$.

DEMOSTRACIÓN. Veamos primero que, de existir, $\widehat{\phi}$ ha de ser único. Para ello, tomamos $f = f_0 + f_1 X + \cdots + f_n X^n \in A[X]$ y le aplicamos $\widehat{\phi}$, que se supone homomorfismo de anillos, por lo que

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

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 $f = \sum_i f_i X^i$. 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. Bien, dados $f, g \in A[X]$, tenemos

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

y

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

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.

COROLARIO 3.7. *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*

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

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

EJEMPLO 3.8. 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 $f = f_0 + f_1 X + \cdots + f_n X^n \in Ker(ev_x)$ con $f_n \neq 0$, 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[1] que $f_n = 0$. Lo que es una contradicción.

[1] Si esto no nos parece evidente, podemos usar un poco de Cálculo Diferencial y calcular la n–ésima derivada de $f(x)$, que ha de ser nula también. Más adelante, veremos que no es necesario usar Cálculo Diferencial para justificar esto.

3.2. División con resto de polinomios

Comencemos definiendo algunos parámetros asociados a un polinomio. Sea A una anillo conmutativo, y tomemos un polinomio no nulo $f \in A[X]$,

$$f = f_0 + f_1X + \cdots + f_nX^n,$$

con $f_i \in A$ para $i = 0, 1, \ldots, n$ y $f_n \neq 0$. Cada f_iX^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 $\mathrm{lm}(f) = f_nX^n$.

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 3.9. *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,* $\deg(f) = \deg(g)$ *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 $f = f_nX^n + f_\downarrow$ y $g = g_mX^m + g_\downarrow$, con $n = \deg(f)$ y $m = \deg(g)$.

1 y 2. Podemos suponer, sin pérdida de generalidad, que $n \leq m$. Tenemos que

$$f + g = f_nX^n + f_\downarrow + g_mX^m + g_\downarrow.$$

Si $n < m$, entonces en los polinomios $f_\downarrow, g_mX^m, g_\downarrow$ 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 $f_n + g_n = 0$, entonces $\deg(f + g) = \deg(f_\downarrow + g_\downarrow) < n$.

3 y 4. Tenemos que

$$fg = (f_nX^n + f_\downarrow)(g_mX^m + g_\downarrow) = f_ng_mX^{n+m} + f_nX^ng_\downarrow + g_mX^mf_\downarrow + f_\downarrow g_\downarrow. \tag{3.6}$$

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,

$$\deg(f_nX^ng_\downarrow) \leq n + \deg(g_\downarrow) < n + m.$$

Análogamente, $\deg(g_mX^mf_\downarrow) < n+m$ y $\deg(f_\downarrow g_\downarrow) < n+m$. Así que, si $f_ng_m \neq 0$, deducimos que de (3.6) que $\deg(fg) = n + m = \deg(f) + \deg(g)$. En tanto que si $f_ng_n = 0$, deducimos que

$$\begin{aligned}\deg(fg) &= \deg(f_nX^ng_\downarrow + g_mX^mf_\downarrow + f_\downarrow g_\downarrow)\\ &\leq \max\{\deg(f_nX^ng_\downarrow), \deg(g_mX^mf_\downarrow), \deg(f_\downarrow g_\downarrow)\} < n + m\end{aligned}$$

Lo que completa la inducción. □

Esta función grado permite dar un algoritmo de división con resto para polinomios. Antes de dar ésta, vamos a demostrar un lema que usaremos un par de veces.

LEMA 3.10. *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

$$\begin{aligned}
&\mathrm{lc}(g)f - \mathrm{lc}(f)X^m g \\
&\qquad = \mathrm{lc}(g)(\mathrm{lc}(f)X^{\deg(g)} + f_\downarrow) - \mathrm{lc}(f)(X^m \mathrm{lc}(g)X^{\deg(g)} + X^m g_\downarrow) \\
&\qquad = \mathrm{lc}(g)\mathrm{lc}(f)X^{\deg(f)} + \mathrm{lc}(g)f_\downarrow - \mathrm{lc}(f)\mathrm{lc}(g)X^{m+\deg(g)} - \mathrm{lc}(f)X^m g_\downarrow \\
&\qquad\qquad = \mathrm{lc}(g)f_\downarrow - \mathrm{lc}(f)X^m g_\downarrow.
\end{aligned}$$

Por otra parte,

$$\begin{aligned}
&\deg(\mathrm{lc}(g)f_\downarrow - \mathrm{lc}(f)X^m g_\downarrow) \\
&\qquad \leq \max\{\deg(\mathrm{lc}(g)f_\downarrow), \deg(\mathrm{lc}(f)X^m g_\downarrow)\} \\
&\qquad\qquad \leq \max\{\deg(f_\downarrow), m + \deg(g_\downarrow)\} < \deg(f).
\end{aligned}$$

□

TEOREMA 3.11 (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 $\mathrm{lc}(g)^0 = 1$). En particular, 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 $\deg(g) = 0 = \deg(f)$, 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 3.10, $\deg\left(\mathrm{lc}(g)f - \mathrm{lc}(f)X^m g\right) < \deg(f)$. 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. □

Reorganizando las ideas de la demostración del Teorema 3.11 obtenemos el Algoritmo 2.

TEOREMA 3.12. *El Algoritmo 2 calcula correctamente una división libre de fracciones de* f *entre* g*.*

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

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". 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 del 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 la salida del bucle $r_{\ell+1}, q_{\ell+1}$ siguen verificando la 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 3.10,

$$\deg r_{\ell+1} = \deg(\mathrm{lc}(g)r_\ell - \mathrm{lc}(r_\ell)X^{\deg r_\ell - \deg g}g) < \deg r_\ell.$$

Por tanto, la condición que abre el bucle 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 3.11.

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	q
0	$3X^3 + 5X + 1$	0
1	$6X^3 + 10X + 2$ $-6X^3 - 3X^2$ $-3X^2 + 10X + 2$	$3X^2$
2	$-6X^2 + 20X + 4$ $6X^2 + 3X$ $23X + 4$	$6X^2 - 3X$
3	$46X + 8$ $-46X - 23$ -15	$12X^2 - 6X + 23$

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 coefientes. 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.

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 3.11, ya que $\mathrm{lc}(g)^\ell \in U(A)$ para todo $\ell \geq 0$. □

Mientras que el Corolario 3.16 se deduce del enunciado del Teorema 3.11, de la demostración del Teorema 3.12, convenientemente adaptada, se deduce la corrección del Algoritmo 3.

EJEMPLO 3.17. El siguiente cuadro contiene los cálculos de la división libre de fracciones en $\mathbb{Q}[X]$ de $f = 3X^3 + 5X + 1$ entre $g = 2X + 1$ mediante el

Algoritmo 3 División Euclídea de Polinomios

Input: $f, g \in A[X]$ con $lc(g) \in U(A)$, 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**
    $q \leftarrow q + lc(g)^{-1}lc(r)X^{\deg r - \deg g}$
    $r \leftarrow r - lc(g)^{-1}lc(r)X^{\deg r - \deg g}g$
  return q, r

Algoritmo 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 3.18. Consideremos el homomorfismo evaluación

$$ev_{\sqrt{2}} : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{2}],$$

que es claramente sobreyectivo. Además, $X^2 - 2 \in Ker(ev_{\sqrt{2}})$. Supongamos ahora $f \in Ker(ev_{\sqrt{2}})$. 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 $Ker(ev_{\sqrt{2}})$ consiste, precisamente, en todos los múltiplos de $X^2 - 2$.

3.3. Dominios de ideales principales y divisibilidad

Un tipo de anillo conmutativo fundamental está constituido por los dominios de integridad.

DEFINICIÓN 3.19. 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 3.20. El anillo $\mathbb{Z}$ es un dominio de integridad.

EJEMPLO 3.21. 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 3.22. 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 3.9, $\deg(fg) = \deg(f) + \deg(g) \geq 0$, 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 2.20, 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 $a \in A$ 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 denotar esta situación, usaremos la notación $a|b$.

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. Observemos primero que $a|b$ 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 (DI), 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 3.32. 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 3.33. 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 3.34. Demostrar que, si A es un DI, entonces $U(A[X]) = U(A)$.

DEFINICIÓN 3.35. Sean $a_1, \ldots, a_n \in A$, donde A es un dominio de integridad. Diremos que $d \in A$ es un divisor común de $a_1, \ldots, a_n$ si $d|a_1, \ldots, d|a_n$. Un *máximo común divisor* de $a_1, \ldots, a_n$ es un divisor común d de $a_1, \ldots, a_n$ y tal que si d' es cualquier otro divisor común de $a_1, \ldots, a_n$, entonces $d'|d$.

LEMA 3.36. *Sean $a_1, \ldots, a_n \in A$, donde A es un DI. Un elemento d de A 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, $\langle a_1, \ldots, a_n \rangle \subseteq \langle a \rangle$. Supngamos 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 $\langle d \rangle$ es 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 3.37. *Si A es un dominio de ideales principales y $a_1, \ldots, a_n \in A$, entonces existe un máximo común divisor de $a_1, \ldots, a_n$. De hecho, $d = \mathrm{mcd}(a_1, \ldots, a_n)$ para cualquier $d \in A$ tal 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 3.36 que $d = \mathrm{mcd}(a_1, \ldots, a_n)$. □

El siguiente corolario se sigue inmediatamente.

COROLARIO 3.38 (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 3.39. 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 cuando manejamos elementos de un DIP.

DEFINICIÓN 3.40. 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 3.41. *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 $a_1, \ldots, a_n$ si, y sólo si, $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle \supseteq \langle a \rangle$. Supngamos que m es un mcm de $a_1, \ldots, a_n$, 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 $a_1, \ldots, a_n$, deducimos que $m|m'$. Por tanto, $\langle m' \rangle \subseteq \langle m \rangle$, y $\langle m \rangle$ es 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 $a_1, \ldots, a_n$, entonces $m' \in A$ es mcm de $a_1, \ldots, a_n$ 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 3.42. *Si A es un dominio de ideales principales y $a_1, \ldots, a_n \in A$, entonces existe un mínimo común múltiplo de $a_1, \ldots, a_n$. De hecho, $m = \mathrm{mcm}(a_1, \ldots, a_n)$ para cualquier $m \in A$ tal 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 3.36 que $m = mcm(a_1, \ldots, a_n)$. □

EJERCICIO 3.43. Supongamos $a, b, c \in A$, donde A es un DI, tales que los mínimos comunes múltiplos involucrados en la igualdad

$$mcm(mcm(a, b), c) = mcm(a, mcm(b, c))$$

existen. Demostrar que la citada igualdad es correcta.

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 3.44. 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 3.45. Los elementos irreducibles de $\mathbb{Z}$ son los números naturales primos y sus opuestos.

EJEMPLO 3.46. 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 $g \in U(K)$ o bien $h \in U(K)$. Como $U(K[X]) = U(K)$, concluimos que f es irreducible.

EJEMPLO 3.47. 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 $\alpha = -b/a$ es una raíz de g y, por tanto, de $X^2 + 1$. Así que $\alpha^2 + 1 = 0$, lo que es imposible, porque $\alpha^2 \geq 0$.

DEFINICIÓN 3.48. Un elemento p de un DI 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 3.49. 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 3.50. *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, $b \in \langle p\rangle$. De aquí, $\langle p\rangle = \langle b\rangle$, luego $b = up$, 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 que $b \in U(A)$. Así que p es irreducible. □

TEOREMA 3.51. *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) $\Rightarrow$ (II). Evidente.

(II) $\Rightarrow$ (III). Ejercicio 3.49.

(III) $\Rightarrow$ (IV). Lema 3.50.

(III) $\Rightarrow$ (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 $d = mcd(p, b)$. Como p es irreducible, deducimos que o 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, $1 = mcd(p, b)$ (recordemos que esta notación significa "1 es un mcd de p y b"). Por Bezout, 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. □

EJEMPLO 3.52. Estamos en condiciones de afirmar, en vista del Ejemplo 3.47 y del Teorema 3.51, 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

$$a + b(X + \langle X^2 + 1\rangle).$$

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,

$$i^2 = (X + \langle X^2 + 1\rangle)^2 = X^2 + \langle X^2 + 1\rangle = -1 + \langle X^2 + 1\rangle = -1,$$

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 distributivas 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 fundamentales 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[2], que deja fijos los

[2] se suele decir que es un automorfismo de cuerpos

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 del plano real de componentes (a, b). 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.

EJERCICIO 3.53. 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 3.54. Sean $a, b, x, y \in A$, con A un DIP, tales que $xa = yb$. Demostrar que, si $\mathrm{mcd}(x, y) = 1$, entonces a es un múltiplo de y y b es un múltiplo de x. (Sugerencia: usar la identidad de Bezout).

EJERCICIO 3.55. 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 3.56. 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 3.57. Construir cuerpos con 4 y 8 elementos.

EJERCICIO 3.58. Sea $m \in A$, con $m \neq 0$, donde A es un DIP. Sea $a \in A$. Demostrar que $a + \langle m \rangle \in \mathcal{U}(A/\langle m \rangle)$ si, y sólo si, $\mathrm{mcd}(a, m) = 1$.

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 3.59. 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 3.60. El anillo $\mathbb{Z}$ de los números enteros en un dominio euclídeo con la función euclídea valor absoluto.

EJEMPLO 3.61. Si K es un cuerpo, entonces la aplicación que asigna a cada polinomio no nulo de en $K[X]$ su grado es una función es una función euclídea. Por tanto, $K[X]$ es un dominio euclídeo.

EJEMPLO 3.62. 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 3.63. Si $a, b \in A$ con $b \neq 0$, para A un DE con función euclídea ϕ. Sea $a = qb + r$ 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 $\phi(r) = \phi((c - q)b) \geq \phi(b)$. Por tanto, $r = 0$.

TEOREMA 3.64. *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, 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 $r = rem(a, b)$ y $q = quot(a, b)$, bien entendido que dichos elementos no son, en general, únicos.

Algoritmo 4 `Algoritmo Extendido de Euclides general`

Input: $a, b \in A$ con $b \neq 0$, donde A es un dominio euclídeo.
Output: $\{u_i, v_i, r_i\}_{i=0,\ldots,h,h+1}$ tales que $r_i = au_i + bv_i$ para $i = 0, 1, \ldots, h, h+1$,
$r_{h+1} = 0$,
$r_h = mcd(a, b)$,
$u_{h+1}a = mcm(a, b)$.
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**
  $q \leftarrow \text{quot}(r_{i-1}, r_i)$
  $r \leftarrow \text{rem}(r_{i-1}, r_i)$
  $r_{i+1} \leftarrow r$
  $u_{i+1} \leftarrow u_{i-1} - u_i q$
  $v_{i+1} \leftarrow v_{i-1} - v_i q$
  $i \leftarrow i + 1$
return $\{u_i, v_i, r_i\}_{i=0,\ldots,h,h+1}$

TEOREMA 3.65. *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

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

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 definidos $u_i, v_i, u_{i-1}, v_{i-1}$, 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,

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

Veamos, por último, que $u_{h+1} a mcm(a, b)$. 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 $u_{h+1} a = mcm(a, b)$, demostremos que

$$-u_{i+1} v_i + u_i v_{i+1} = 1$$

para todo $0 \leq i \leq h$. Dicha igualdad es clara para $i = 0$. Para $i = 0$, la igualdad es clara. Si $1 \leq i \leq h$, supuesta la igualdad demostrada parar $i - 1$, tenemos

$$-u_{i+1} v_i + u_i v_{i+1} = -(u_{i-1} - q_i u_i) v_i + u_i (v_{i-1} - q_i v_i) = -u_{i-1} v_i + u_i v_{i-1} = 1.$$

En particular, $u_{h+1} v_h - u_h v_{h+1} = 1$. De aquí, $mcd(u_{h+1}, v_{h+1}) = 1$.

Por el Ejercicio 3.53, $mcm(a, b) = a u_{h+1}$. □

Seguidamente, vamos a ver algunos ejemplos adicionales de dominios euclídeos. 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[3] 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[4] de $\mathbb{Q}(\sqrt{D})$.

Como es un subanillo de un cuerpo, $\mathbb{Z}[\sqrt{D}]$ es un dominio de integridad. Para algunos valores de D, se trata de un dominio euclídeo. Queremos conocer algunos de ellos.

[3] Comprobar. Algo más adelante, veremos que, de hecho, se trata de un subcuerpo.

[4] comprobar

LEMA 3.66. *Si* $x + y\sqrt{D} = 0$ *para* $x, y \in \mathbb{Q}$*, entonces* $x = y = 0$.

DEMOSTRACIÓN. Primero, escribamos $\sqrt{D} = n\sqrt{d}$, donde $n \in \mathbb{N}$ y d es libre de cuadrados, lo cual es posible porque D no es un cuadrado, a la vista de la factorización única de D como producto de primos proporcionada por el Teorema Fundamental de la Aritmética (TFA). Observemos que $x + y\sqrt{D} = x + yn\sqrt{d}$. Obviamente, $y = 0$ si, y sólo si, $ny = 0$, de donde deducimos que podemos asumir, sin pérdida de generalidad, que D es libre de cuadrados, y así lo hacemos.

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 existirán $a, b \in \mathbb{Z}$, ambos no nulos, tales que $a = \sqrt{D}b$. Queremos demostrar queno obstante, $a = b = 0$, lo que es una contradicción. Notemos que $a^2 = b^2D$. Si $D < 0$, entonces $b^2D \leq 0$, lo que implica $b^2D = 0$, de donde $b^2 = 0$. De aquí, $b = 0$ y $a = 0$. Si $D > 0$, entonces $D \neq 1$ y podemos tomar un divisor primo p de D. Entonces p es un divisor primo de a^2 y, por tanto, p^2 es un divisor de a^2. Si $a \neq 0$, tomamos $e \geq 2$ el mayor número natural tal que p^e divide a a^2. Por el Teorema Fundamental de la Aritmética, e es par. Ahora, de nuevo por el Teorema Fundamental de la Aritmética, como p^e divide a b^2D, hemos de admitir que p^{e-1} divide a b^2. Como $e - 1$ es impar, hemos de admitir que p^e también divide a b^2. Luego p^{e+1} divide a a^2, lo que es una contradicción. Así que $a = b = 0$ y $z = 0$. □

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 $\bar{z} = x - y\sqrt{D}$, entonces podemos reescribir la norma de z como

$$N(z) = z\bar{z}.$$

EJERCICIO 3.67. Demostrar que la aplicación $\alpha : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}(\sqrt{D})$ definida por $\alpha(z) = \bar{z}$ 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 3.68. *Sea* $z \in \mathbb{Z}(\sqrt{D})$*. Entonces* $z = 0$ *si, y sólo si,* $N(z) = 0$*.*

DEMOSTRACIÓN. Pongamos $z = x + y\sqrt{D}$. Si $z = 0$, entonces, por el Lema 3.66, $x = y = 0$ y, por tanto, $N(z) = 0$. Recíprocamente, si $N(z) = 0$, entonces $z\bar{z} = 0$. Esto implica que, o bien $z = 0$, o bien $\bar{z} = 0$. En el segundo caso, $x - y\sqrt{D} = 0$, lo que implica, de nuevo por el Lema 3.66, que $x = y = 0$. □

Como consecuencia del Lema 3.68, si $z \in \mathbb{Q}(\sqrt{D})$ es no nulo, su inverso en $\mathbb{C}$ se calcula por la fórmula

$$z^{-1} = \frac{\bar{z}}{N(z)}. \tag{3.8}$$

Como consecuencia, 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 $\mathbb{Z}[\sqrt{D}]$ no lo es, como resultará evidente tras ver la siguiente proposición.

PROPOSICIÓN 3.69. *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 3.70. *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 $q = a + b\sqrt{D}$ y $r = w - qz$. Obviamente, $q, r \in \mathbb{Z}[\sqrt{D}]$. Ahora,

$$\begin{aligned} |N(rz^{-1})| = |N((w - qz)z^{-1})| &= |N(wz^{-1} - q)| \\ &= |N(a - x + (b - y)\sqrt{D})| = |(a - x)^2 - (b - y)^2 D|. \end{aligned}$$

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 3.71. 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.

LEMA 3.72. *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,* $\mathrm{mcd}(a, b)$ *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 $d = \mathrm{mcd}(a, c)$, 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:

$$a \equiv b \pmod{m}, \tag{3.10}$$

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 (2.6).

LEMA 3.73. *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* $\mathrm{mcd}(a, m)$ *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 del Lema 3.72. □

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 $d = \mathrm{mcd}(a, m)$, 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, (2.7) 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 $\overline{u}\overline{a'} = \overline{1}$. Como (3.11) es equivalente a la ecuación $\overline{a'}\overline{x} = \overline{b'}$, podemos despejar $\overline{x} = \overline{u}\overline{b'}$. Esto es,

$$x = ub' + km'$$

para $k \in A$.

EJERCICIO 3.74. 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 3.75. Sean $\alpha_0, \alpha_1, \ldots, \alpha_n \in A$ 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 3.76. Sean $x_0, x_1, \ldots, x_n \in K$, con K un cuerpo. Supongamos que, para $0 \leq i < j \leq n$, $x_i \neq x_j$, y sean $y_0, y_1, \ldots, y_n \in K$ 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 $y_0, y_1 \ldots, y_n$ en los nodos $x_0, x_1, \ldots, x_n$. 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

Comencemos viendo que hay dominios de integridad "sencillos" que no son dominios de ideales principales.

EJEMPLO 4.1. Vamos a demostrar que no es $\mathbb{Z}[\sqrt{-5}]$ no es un DIP exhibiendo un par de elementos suyos para los que no existe mínimo común múltiplo. Tomemos $z = 2, w = 1 + \sqrt{-5}$, y supongamos que existe $m = mcm(z, w)$. Escribamos $m = a+b\sqrt{-5}$, para $a, b \in \mathbb{Z}$. Como $m|zw = 2+2\sqrt{-5}$, tomando normas, tenemos que $a^2 + 5b^2$ es un divisor de 24. Observemos que $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, por lo que es un múltiplo común de z y w. Así que $m|6$. Tomando normas de nuevo, $a^2 + 5b^2$ divide a 36. Por tanto, $a^2 + 5b^2$ divide a 12. Por otra parte, m ha de ser un múltiplo de z y de w, 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.

Como veremos, la existencia de mínimo común múltiplo influye 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 $mcm(a, b)$, y tomamos $d \in A$ tal que $ab = d \cdot mcm(a, b)$, entonces $d = mcd(a, b)$.*

DEMOSTRACIÓN. Bien, escribamos $m = mcm(a, b)$, 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.

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 "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 $p_1, \ldots, p_r \in A$, y naturales $e_1, \ldots, e_r \geq 1$ tales que $a \sim p_1^{e_1} \cdots p_r^{e_r}$.

2. Si $q_1, \ldots, q_s \in A$ son irreducibles no asociados entre sí tales que $a \sim q_1^{f_1} \cdots q_s^{f_s}$ para ciertos naturales $f_1, \ldots, f_s \geq 1$, entonces $r = s$ y, tras eventual reordenación, $f_i = e_i$ y $q_i \sim p_i$ para todo $i = 1, \ldots, r$.

Si se da la primera condición, diremos que a *admite factorización*, y que $p_1^{e_1} \cdots p_r^{e_r}$ es una factorización 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 $p = uq_1^{f_1} \ldots q_s^{f_s}$ para $u \in U(A)$, 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 4.5. Si a admite factorización única y b es asociado con a, entonces b admite factorización única.

DEFINICIÓN 4.6. 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.

TEOREMA 4.7. *Sea A un DI tal que todo elemento no nulo y no unidad admite factorización. 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 $p|ab$. Luego $pc = ab$ para cierto $p \in A$. 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 únicas 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, obtenemos que, o bien $p \sim p_i$ para algún $i \in \{1, \ldots, r\}$, o bien $p \sim y_j$ para algún $j \in \{1, \ldots, s\}$. 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 $a \sim p_1^{e_1} \cdots p_r^{e_r}$ le asociamos su *peso* $\sum_{i=1}^{r} e_i$. Definimos $\mu(a)$ como el mínimo de los pesos de las factorizaciones de a. Demostraremos la unicidad de las factorizaciones 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 supongamos que todo elemento b con $\mu(b) < \mu(a)$ tiene unicidad en sus factorizaciones. Bien, supongamos 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, 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 $p_1^{e_1-1} \cdots p_r^{e_r} \sim q_1^{f_1-1} \cdots q_s^{f_s}$. Como el peso del primer elemento es $\mu(a)-1$, podemos aplicar la hipótesis de inducción y deducir que $r = s$ y, tras eventual reordenación, $p_i \sim q_i$ para todo $i = 1, \ldots, r$ y $e_i = f_i$. En realidad, $e_1 - 1 = f_1 - 1$, pero esto implica, obviamente, que $e_1 = f_1$. □

OBSERVACIÓN 4.8. Observemos que, durante la prueba del Teorema 4.7, hemos demostrado que todas las factorizaciones de un elemento a de un DFU tienen el mismo peso, concretamente, el peso mínimo $\mu(a)$.

TEOREMA 4.9. *Todo DIP es un DFU.*

DEMOSTRACIÓN. Puesto que, en un DIP, cada irreducible es primo (ver Teorema 3.51), sólo hemos de demostrar que cada elemento admite una

factorización. 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 $X = B \cup M$, 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 lleva 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 de esta propiedad de M, podemos definir, a partir de $a_0 \in M$, una sucesión $a_0, a_1, \ldots, a_n \cdots$ 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 $a \in A$ tal que $I = \langle a \rangle$. Así, $a \in \langle a_n \rangle$ para algún $n \geq 0$. Por tanto,

$$I = \langle a \rangle \subseteq \langle a_n \rangle \subseteq I,$$

lo que sólo es posible si $\langle a_n \rangle = \langle a_m \rangle$ para todo $m \geq n$. Contradicción. □

EJEMPLO 4.10. Veamos que $\mathbb{Z}[\sqrt{-5}]$ no es un DFU. 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 3.69, $N(w) > 1$. 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 $a^2 = 1$. Así que $r = 1$ 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.

PROPOSICIÓN 4.11. *Sea A un DFU, y $a, b \in A$. Entonces existen $\mathrm{mcm}(a, b)$ y $\mathrm{mcd}(a, b)$.*

DEMOSTRACIÓN. Comencemos discutiendo los casos triviales. Si $a = b = 0$, entonces $\mathrm{mcm}(0, 0) = \mathrm{mcd}(0, 0) = 0$. Supongamos ahora $a \neq 0$ pero $b = 0$, entonces $\mathrm{mcm}(a, 0) = 0$ y $\mathrm{mcd}(a, 0) = a$. Discutamos el caso general, es decir $ab \neq 0$. Tomemos los irreducibles $p_1, \ldots, p_r \in A$ 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 $e_1, \ldots, e_r, f_1, \ldots, f_r \in \mathbb{N}$. Estamos entendiendo que $p_i^0 = 1$, claro. Sea, para cada $i = 1, \ldots, r$, $g_i = \max\{e_i, f_i\}$. Afirmamos que $\mathrm{mcm}(a, b) = p_1^{g_1} \cdots p_r^{g_r}$. Es bastante obvio que $up_1^{g_1} \cdots p_r^{g_r}$ es múltiplo común de a y b para una unidad adecuada u. Supongamos ahora m un múltiplo común de a y b. Entonces, para cada $i = 1, \ldots, r$, puesto que $p_i^{e_i} | a$, tenemos que $p_i^{e_i} | m$. Análogamente, $p_i^{f_i} | m$ y, por cómo

está definido cada g_i, tenemos que $p_i^{g_i}|m$. En particular, entre los irreducibles que aparecen en una factorización de m están $p_1, \dots, p_r$. Por tanto, existen $h_1, \dots, h_r \geq 1$ tales que $m = p_1^{h_1} \cdots p_r^{h_r} x$, donde p_i no divide a x para todo $i = 1, \dots, r$. Ahora, tenemos que $p_i^{g_i}|p_1^{h_1} \cdots p_r^{h_r} x$, para cada $i = 1, \dots, r$. Supongamos que existiera un índice i tal que $h_i < g_i$. Salvo reenumeración de los índices, podemos suponer que $i = 1$. Así, $p_1^{g_i - h_i}$ sería un divisor de $p_2^{g_2} \cdots p_r^{g_r} x$. Como $g_i - h_i > 0$, esto significa que el irreducible p_1 tiene que dividir a x, ya que sabemos que todo irreducible de A es primo. Esto no puede ser, por lo que $h_i \geq g_i$ para todo $i = 1, \dots, r$ y $p_1^{g_1} \cdots p_r^{g_r}$ resulta ser un divisor de m. Obtenemos, por tanto, que

$$mcm(a, b) = p_1^{g_1} \cdots p_r^{g_r}.$$

la existencia de $mcd(a, b)$ viene garantizada por la Proposición 4.2. Además, de allí obtenemos también que

$$mcd(a, b) = p_1^{k_1} \cdots p_r^{k_r},$$

donde $k_i = \min\{e_i, f_i\}$ 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 y por $\langle a \rangle$ 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 $\phi : A \to (A/Aa)[X]$ definido por $\phi(a) = b + Aa$ 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 $\widetilde{\phi} : A[X] \to (A/a)[X]$ dado por $\widetilde{\phi}(\sum_i f_i X^i) = \sum_i (f_i + Aa)X^i$, que es obviamente sobreyectivo. Observemos que $\sum_i f_i X^i \in Ker\widetilde{\phi}$ si, y sólo si, $f_i \in Aa$ para todo i. Esto es, $Ker\widetilde{\phi} = \langle a \rangle$. 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 3.49, 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

$$c(f) = mcd(f_0, f_1, \dots, f_n) \in A.$$

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 $p \in A$ 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. □

LEMA 4.18. *Si A es un DFU, $a \in A$ y $f \in A[X]$ es primitivo, entonces $c(af) = a$.*

DEMOSTRACIÓN. Pongamos $f = f_0 + f_1X + \cdots + f_nX^n$, con $f_i \in A$, para $i = 0, \ldots, n$. Como $1 = mcd(f_0, f_1, \ldots, f_n)$, tenemos 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 $(a, s)R(b, t)$ si $at = bs$.*

1. *La relación R es de equivalencia. Denotemos por $Q = A/R$ 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*
$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}, \qquad (\frac{a}{s}, \frac{b}{t} \in Q).$$
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. □

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.

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 $c(f) \notin U(A) = U(A[X])$. 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. Supongamos una factorización $f = gh$, con $g, h \in Q[X]$. Tomemos $a, b \in A$ tales que $ag, bh \in A[X]$. Por la Proposición 4.19, $ab = c(abf) = c(agbh) = c(ag)c(bh)$. Así si tomamos $g_1, h_1 \in A[X]$ primitivos tales que $ag = c(ag)g_1$, $bh = c(bh)h_1$, como $abf = c(ag)c(bh)g_1h_1$, deducimos que $f = g_1h_1$. Al ser f irreducible en $A[X]$, tenemos que $g_1 \in U(A[X])$ o bien $h_1 \in U(A[X])$. Como $U(A[X]) = U(A) \subseteq Q^*$, deducimos que 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 $q \sim c(q) \in U(A)$, por lo que $q \in U(A)$. 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, entonces $f|g$ en $A[X]$.*

DEMOSTRACIÓN. Supongamos que $g = hf$ para $h \in Q[X]$. Tomemos $a \in A$ 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 $g = c(g)g^*$ y $ah = c(ah)h_1$ para ciertos polinomios (primitivos) $g^*, h_1 \in A[X]$, tenemos que $ac(g)g^* = ac(g)h_1f$, 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. 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 4.7, 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 4.7, 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 del Teorema 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

$$f = \sum_{i,j} f_{ij} X^i Y^j.$$

De modo que f viene a ser un polinomio en las indeterminadas X, Y con coeficientes en A, 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[1], 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 $Q[X]$.

De hecho, cada raíz en Q de un polinomio proporciona un factor irreducible:

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 $A[X]$.

PROPOSICIÓN 4.29. *Sea* $f = f_0 + f_1 X + \cdots + f_n X^n \in A[X]$ *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

$$0 = f_0 + f_1 \frac{a}{b} + \cdots + f_n (\frac{a}{b})^n.$$

De aquí,

$$0 = f_0 b^n + f_1 a b^{n-1} + \cdots + f_n a^n.$$

[1]Mantendremos durante toda esta sección la hipótesis de que A es un DFU.

Esta igualdad implica que $b|f_n a^n$. Como $mcd(a,b)=1$, deducimos que $b|f_n$. Análogamente, $a|f_0$. □

EJEMPLO 4.30. Veamos que $X^3 - 1/2X + 2 \in \mathbb{Q}[X]$ 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 $\mathbb{Z}[X]$.

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* $\varphi(\sum_i s_i X^i) = \sum_i \phi(s_i) X^i$. *Supongamos que* $f = f_0 + f_1 X + \cdots + f_n X^n \in S[X]$ *con* $\phi(s_n) \neq 0$, *y que* B *es un DI. Si* $f = hg$ *con* $g, h \in S[X]$, *entonces* $\deg(g) = \deg(\varphi(g))$ *y* $\deg(h) = \deg(\varphi(h))$.

DEMOSTRACIÓN. Es claro que $\deg(\varphi(g)) \leq \deg(g)$ y $\deg(\varphi(h)) \leq \deg(h)$. Ahora,

$$\begin{aligned} n = \deg(f) \geq \deg(g) + \deg(h) &\geq \deg(\varphi(g)) + \deg(\varphi(h)) \\ &= \deg(\varphi(gh)) = \deg(\varphi(f)) = n. \end{aligned}$$

□

El siguiente es un criterio clásico de irreducibilidad.

PROPOSICIÓN 4.32 (Criterio de Eisenstein). *Sea* $f = f_0 + f_1 X + \cdots f_n X^n \in A[X]$, *con* $f_n \neq 0$. *Suponemos que* A *es un DFU. 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* a_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 $\overline{a_n} X^n = \varphi(f) = \varphi(g)\varphi(h)$ en $(A/Ap)[X]$. Si vemos esta factorización en $K[X]$, donde K es el cuerpo de fracciones de A/Ap, tenemos que $\overline{g} = uX^k$ y $\overline{h} = vX^{n-k}$ 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 $\overline{g}(0) = 0 = \overline{h}(0)$. 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, y $n \in \mathbb{N}$, $n \geq 2$. Si tomamos un divisor primo p de a, podemos 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 Eisestein 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. □

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 $f \in \mathbb{Z}$ 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[2] 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. 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[3] $\overline{f(0,1)} = \overline{1} \neq 0$, $\overline{f(1,1)} = \overline{1} \neq 0$ y $\overline{f(-1,1)} = \overline{-1} \neq 0$. En conclusión $\overline{f(X,1)}$ es irreducible en $\mathbb{Z}_3[X]$, lo que implica que lo es $f(X,1)$ en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$, y, de aquí, $f(X,Y)$ es irreducible en $\mathbb{Q}[X,Y]$,

EJEMPLO 4.38. 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

[2] Es fácil listar todos los polinomios cuadráticos en $\mathbb{Z}_2[X]$ y comprobar si tienen raíces.

[3] 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...

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 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 4.39. 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 uno de estos polinomios 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 $f(X), g(X) \in \mathbb{C}[X]$ tales que $\mathrm{mcd}(f,g) = 1$. Así,

$$\left(\frac{f(X)}{g(X)}\right)^3 - X^2 = 0.$$

De modo que $f(X)^3 = g(X)^3X^2$. Razonando en el DFU $\mathbb{C}[X]$, tenemos que el primo X divide a $f(X)$. Por tanto, $f(X) = Xh(X)$, pra cierto $h(X) \in \mathbb{C}[X]$. Luego $X^3h(X)^3 = g(X)^3X^2$. Así que $Xh(X)^3 = g(X)^3$. Luego X es un divisor de $g(X)$ y, así, $\mathrm{mcd}(f,g) \neq 1$, lo que es una contradicción. Esto prueba que $Y^3 - X^2$ no tiene raíces en $\mathbb{C}(X)$, con lo que concluimos 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 $\alpha_1, \ldots, \alpha_k \in A$ distintos. Dado un polinomio $f \in A[X]$ no constante, tenemos que $f(\alpha_i) = 0$ para todo $i = 1, \ldots, k$ 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 $i = 1, \ldots, k$. 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 $i = 2, \ldots, k$. 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 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

$$f' = \sum_{i \geq 1} i f_i X^{i-1}.$$

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, 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, aunque el desarrollo es fácilmente extendible a series formales de potencias[4]. Cuando se está en un contexto en que es posible hablar de series convergentes, es el fundamento algebraico del estudio de funciones analíticas.

Volvamos a nuestro contexto algebraico. 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

[4]Ver Observación 3.5

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 $\frac{i!}{(i-k)!} \in \mathbb{N}$.

PROPOSICIÓN 4.46. *Sea K un cuerpo de característica 0, y $f \in K[X]$. Entonces, si Y denota otra indeterminada, se verifica:*

$$f(X+Y) = \sum_i \frac{1}{i!}f^{(i)}(X)Y^i. \tag{4.1}$$

DEMOSTRACIÓN. Comencemos demostrando (4.1) para cada monomio $m_i = X^i$. Tenemos el siguiente cálculo:

$$m_i(X+Y) = (X+Y)^i = \sum_{k=0}^{i}\binom{i}{k}X^{i-k}Y^k = \frac{i!}{(i-k)!k!}X^{i-k}Y^k = \sum_{k=0}^{i}\frac{1}{k!}m_i^{(k)}(X)Y^k.$$

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 $\alpha \in K$. Entonces*

$$f = \sum_i \frac{1}{i!}f^{(i)}(\alpha)(X-\alpha)^i. \tag{4.2}$$

DEMOSTRACIÓN. Pongamos en (4.1) $X = \alpha$. 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 (4.2) como ejercicio. □