Capítulo 3
Aritmética

Una gran parte del álgebra y en general de las matemáticas importantes del fin del siglo XIX fue desarrollada para generalizar la aritmética de los números enteros a dominios, o investigar las obstrucciones que aparecen en este intento. Esto se estudia en detalles en la teoría de números algebraica, y en este capítulo vamos a introducir algunas nociones básicas. En particular, vamos a definir ciertas clases importantes de anillos:

$$\text{dominios euclidianos} \subsetneq \text{dominios de ideales principales} \subsetneq \text{dominios de factorización única}$$

También vamos a introducir los **ideales de anillos**, que tendrán papel muy importante en el resto del curso. El material de este capítulo generaliza los resultados clásicos sobre los números enteros.

3.1 Divisibilidad

3.1.1. Definición. Sea A un anillo conmutativo. Para elementos $a, b \in A$ se dice que a **divide** a b si $b = ca$ para algún $c \in A$. En este caso también se dice que a es un **divisor** de b y que b es un **múltiplo** de a y se escribe "$a \mid b$".

Se dice que a y b son **asociados** si $a \mid b$ y $b \mid a$. En este caso se escribe "$a \sim b$".

Hagamos primero algunas observaciones triviales.

3.1.2. Observación.

1) *$1 \mid a$ para cualquier $a \in A$,*

2) *$a \mid 1$ si y solamente si $a \in A^\times$,*

3) *$a \mid 0$ para cualquier $a \in A$,*

4) *$0 \mid a$ si y solamente si $a = 0$.* □

La relación $a \sim b$ significa precisamente que a y b son iguales salvo un múltiplo invertible.

3.1.3. Proposición. *Sea A un dominio.*

1) *Se cumple $a \sim b$ si y solamente si $b = ua$ para algún $u \in A^\times$.*

2) *Si $c \neq 0$, entonces $ac \mid bc$ implica $a \mid b$.*

Demostración. En 1), si tenemos $a \sim b$, entonces $a \mid b$ e $b \mid a$; es decir, $a = vb$ y $b = ua$ para algunos $u, v \in A$. Luego, $a = uva$, así que $a(1 - uv) = 0$. Esto implica que $a = 0$, y en este caso $b = 0$ y se tiene $b = 1 \cdot a$; o $uv = 1$, y en este caso $u \in A^\times$.

Viceversa, si $b = ua$ donde $u \in A^\times$, entonces $a = u^{-1} b$, así que $a \mid b$ y $b \mid a$.

En 2), si $bc = dac$ para algún d, entonces, puesto que $c \neq 0$, podemos cancelarlo y obtener $b = da$. ■

Notamos que la relación de divisibilidad es reflexiva y transitiva: para cualesquiera $a, b, c \in A$

$$a \mid a,$$
$$a \mid b,\ b \mid c \Longrightarrow a \mid c.$$

La relación $\sim$ es una relación de equivalencia: para cualesquiera $a, b, c \in A$ se cumple

$$a \sim a,$$
$$a \sim b \Longrightarrow b \sim a,$$
$$a \sim b,\ b \sim c \Longrightarrow b \sim c.$$

3.1.4. Comentario (♣). La relación de divisibilidad es una relación de **preorden** sobre A. Para que esto sea una relación de **orden**, falta la propiedad de antisimetría: $a \mid b$ y $b \mid a$ no implica $a = b$, sino que $a \sim b$ (por la definición). Esto significa que la divisibilidad es una relación de orden sobre las clases $A/\sim$.

3.2 Elementos primos e irreducibles

Notamos que todo elemento $b \in A$ es divisible por 1 y por sí mismo, y en consecuencia por todo a tal que $a \sim 1$ (es decir, $a \in A^\times$) o $a \sim b$. Estos divisores de b son triviales. Un elemento que no tiene divisores no triviales se llama **irreducible**.

3.2.1. Definición. Un elemento $p \in A$ es **irreducible** si

1) $p \neq 0$ y $p \notin A^\times$,

2) $a \mid p$ implica que $a \in A^\times$ o $a \sim p$.

Se dice que un elemento $a \in A$ tal que $a \neq 0$ y $a \notin A^\times$ es **reducible** si existe un divisor no trivial $b \mid a$; es decir, $b \notin A^\times$ y $b \not\sim a$. Tenemos entonces cuatro clases disjuntas de elementos:

$$A = \{0\} \sqcup A^\times \sqcup \{\text{irreducibles}\} \sqcup \{\text{reducibles}\}.$$

3.2.2. Ejemplo. Un polinomio $f \in k[X]$ es irreducible si y solo si f no es constante y f no puede ser escrito como $f = gh$, donde $\deg g, \deg h < \deg f$. Se tiene $f \sim g$ si y solo si $f = cg$ para una constante $c \neq 0$. ▲

Un momento delicado de la teoría general es la distinción entre los elementos primos e irreducibles.

3.2.3. Definición. Un elemento $p \in A$ es **primo** si

1) $p \neq 0$ y $p \notin A^\times$,

2) para cualesquiera $a, b \in A$, si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.

3.2.4. Ejemplo. En el anillo de los números enteros $\mathbb{Z}$ los elementos invertibles son ± 1. Se cumple $a \sim b$ si y solo si $a = \pm b$. Las clases de equivalencia módulo $\sim$ pueden ser representadas por los números no negativos.

Los elementos irreducibles son $\pm p$ donde $p = 2, 3, 5, 7, 11, \ldots$ es primo. Los elementos primos son los mismos (esto se demuestra en el curso de la teoría de números elemental, pero vamos a probarlo otra vez más en las siguientes secciones). ▲

3.2.5. Observación. *Todo elemento primo es irreducible.*

Demostración. Supongamos que $p \in A$ es un elemento que no es irreducible. Esto significa que $p = ab$, donde $a, b \notin A^\times$ y $a \not\sim p$, $b \not\sim p$. Entonces, $p \mid ab$, pero $p \nmid a$ y $p \nmid b$, así que p no es primo. ■

En general, un elemento irreducible no tiene por qué ser primo.

3.2.6. Ejemplo. En el anillo $\mathbb{Z}[\sqrt{-3}]$ el número 2 es irreducible. Para verlo, para $\alpha = a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{3}]$ definamos la **norma** mediante

$$N(\alpha) := \alpha\,\overline{\alpha} = (a + b\sqrt{-3})\,(a - b\sqrt{-3}) = a^2 + 3\,b^2 \in \mathbb{Z}.$$

Para cualesquiera $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$ se tiene

$$N(\alpha\beta) = N(\alpha)\,N(\beta).$$

Notamos que $N(\alpha) \ge 0$. Si α es invertible, entonces aplicando la norma a la identidad $\alpha\alpha^{-1} = 1$ se obtiene

$$N(\alpha)\,N(\alpha^{-1}) = 1 \Longrightarrow N(\alpha) = 1.$$

Los únicos elementos de norma 1 son ± 1, y son obviamente invertibles, así que

$$\mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}.$$

En general, para cualquier $n = 1, 2, 3, \ldots$ la ecuación $a^2 + 3b^2 = n$ define un elipse, y por ende hay un número finito de elementos $\alpha \in \mathbb{Z}[\sqrt{-3}]$ con $N(\alpha) = n$. Basta notar que

$$|a| \le \sqrt{n}, \quad |b| \le \sqrt{n/3}.$$

Hagamos una pequeña lista de elementos de diferente norma (véase la figura 3.1 en p. 8):

$$\begin{array}{rl}
N = 0: & 0, \\
N = 1: & \pm 1, \\
N = 3: & \pm\sqrt{-3}, \\
N = 4: & \pm 2,\ \pm(1 + \sqrt{-3}),\ \pm(1 - \sqrt{3}), \\
N = 7: & \pm(2 + \sqrt{-3}),\ \pm(2 - \sqrt{-3}), \\
N = 9: & \pm 3, \\
N = 12: & \pm(3 + \sqrt{-3}),\ \pm(3 - \sqrt{-3}),\quad \pm 2\sqrt{-3}, \\
& \ldots
\end{array}$$

Todo elemento $\alpha \in \mathbb{Z}[\sqrt{-3}]$ con $N(\alpha) = 4$ es irreducible: si $\alpha = \beta\gamma$, entonces $N(\beta)\,N(\gamma) = 4$, lo que nos deja dos posibilidades:

1) $N(\beta) = 1$, $N(\gamma) = 4$, así que $\beta = \pm 1$, $\gamma = \pm\alpha$;

2) $N(\beta) = 4$, $N(\gamma) = 1$, así que $\gamma = \pm 1$, $\beta = \pm\alpha$.

Ahora tenemos

$$2 \mid 4 = (1 + \sqrt{-3})\,(1 - \sqrt{-3}),$$

aunque los números $1 + \sqrt{-3}$ y $1 - \sqrt{-3}$ no son divisibles por 2. Entonces, 2 es irreducible, pero no es primo en $\mathbb{Z}[\sqrt{-3}]$.

En general, las mismas consideraciones demuestran que para cualquier $n \le -3$ libre de cuadrados, 2 es irreducible pero no es primo en $\mathbb{Z}[\sqrt{n}]$ (véase el ejercicio 3.4). ▲

3.3 Elementos invertibles en $\mathbb{Z}[\sqrt{n}]$

Sea n un número entero libre de cuadrados. En esta sección vamos a investigar cuáles elementos del anillo

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

son invertibles. Para un elemento $a + b\sqrt{n}$ denotemos

$$\sigma(a + b\sqrt{n}) := a - b\sqrt{n}.$$

Un pequeño cálculo demuestra que para cualesquiera $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$ se cumple

$$\sigma(\alpha\beta) = \sigma(\alpha)\,\sigma(\beta).$$

Para encontrar los elementos invertibles, definamos la **norma** de un elemento de $\mathbb{Z}[\sqrt{n}]$ mediante

$$N(\alpha) := \alpha\,\sigma(\alpha).$$

Notamos que la norma es **multiplicativa** en el sentido de que para cualesquiera $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$ se cumple

$$N(\alpha\beta) = N(\alpha)\,N(\beta).$$

La norma es un número entero:

$$N(a + b\sqrt{n}) = (a + b\sqrt{n})\,(a - b\sqrt{n}) = a^2 - nb^2 \in \mathbb{Z}.$$

3.3.1. Lema. *Se tiene $\alpha \in \mathbb{Z}[\sqrt{n}]^\times$ si y solamente si $N(\alpha) = \pm 1$.*

Demostración. Si α es invertible, entonces

$$N(\alpha)\,N(\alpha^{-1}) = N(\alpha\,\alpha^{-1}) = N(1) = 1,$$

así que necesariamente $N(\alpha) = \pm 1$. Viceversa, si $N(\alpha) = \pm 1$, entonces de la ecuación $\alpha \cdot \sigma(\alpha) = N(\alpha)$ se deduce que

$$\alpha^{-1} = \frac{\sigma(\alpha)}{N(\alpha)}.$$ ■

Entonces, para encontrar los elementos invertibles en el anillo $\mathbb{Z}[\sqrt{n}]$, necesitamos encontrar las soluciones enteras $(a, b) \in \mathbb{Z}^2$ de la ecuación

$$a^2 - nb^2 = \pm 1.$$

Esto es fácil si $n < 0$: en este caso hay un número finito de elementos invertibles porque la ecuación $a^2 - nb^2 = -1$ no tiene soluciones, mientras que $a^2 - nb^2 = 1$ define un elipse que puede tener solo un número finito de puntos enteros. A saber (véase la figura 3.2 en p. 8),

- si $n = -1$, la ecuación es $a^2 + b^2 = 1$ y hay cuatro soluciones $(\pm 1, 0)$, $(0, \pm 1)$, de donde podemos concluir que
$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{1, \zeta_4, \zeta_4^2, \zeta_4^3\};$$

- si $n < -1$, entonces la ecuación $a^2 - nb^2 = 1$ tiene solamente dos soluciones $(\pm 1, 0)$, y por lo tanto
$$\mathbb{Z}[\sqrt{n}]^\times = \{\pm 1\}.$$

Ahora si $n > 1$, la ecuación $a^2 - nb^2 = \pm 1$ define una hipérbola y no es tan fácil describir sus puntos enteros. Fijémonos en el caso de $n = 2$, donde hay que encontrar las soluciones enteras de la ecuación

$$a^2 - 2b^2 = \pm 1.$$

Esta se conoce como la **ecuación de Pell**[*]. Se encuentran muchas soluciones, por ejemplo (véase la figura 3.3 en p. 9),

$$(a,b) = (\pm 1, 0),\ (\pm 1, \pm 1),\ (\pm 3, \pm 2),\ (\pm 7, \pm 5),\ \ldots$$

que corresponden a las unidades

$$\begin{gathered} \pm 1 = \pm(1-\sqrt{2})^0, \\ \pm(1+\sqrt{2}),\ \pm(1-\sqrt{2}) = \mp(1+\sqrt{2})^{-1}, \\ \pm(3+2\sqrt{2}) = \pm(1+\sqrt{2})^2,\ \pm(3-2\sqrt{2}) = \pm(1+\sqrt{2})^{-2}, \\ \pm(7+5\sqrt{2}) = \pm(1+\sqrt{2})^3,\ \pm(7-5\sqrt{2}) = \mp(1+\sqrt{2})^{-3}, \\ \ldots \end{gathered}$$

Note que todas las soluciones de arriba son de la forma $\pm(1+\sqrt{2})^n$ para algún $n \in \mathbb{Z}$. Se puede probar que son todos los elementos invertibles en $\mathbb{Z}[\sqrt{2}]^\times$.

3.3.2. Lema. *En $\mathbb{Z}[\sqrt{2}]$ no existe un elemento invertible α tal que*

$$1 < \alpha < 1 + \sqrt{2}.$$

Demostración. Si tal α existe, entonces

$$N(\alpha) = \alpha \cdot \sigma(\alpha) = \pm 1.$$

1) Si $\alpha \cdot \sigma(\alpha) = +1$, entonces

$$\sqrt{2} - 1 = (1+\sqrt{2})^{-1} < \sigma(\alpha) = \sigma^{-1} < 1.$$

Luego,

$$\sqrt{2} < \alpha + \sigma(\alpha) < 2 + \sqrt{2},$$

Pero para $\alpha = a + b\sqrt{n}$ se tiene $\alpha + \sigma(\alpha) = 2a$ y el único entero par que puede estar entre $\sqrt{2}$ y $2 + \sqrt{2}$ es 2, así que

$$\alpha + \sigma(\alpha) = 2, \quad \alpha \cdot \sigma(\alpha) = 1,$$

de donde $\alpha = \sigma(\alpha) = 1$. Contradicción.

2) Si $\alpha \cdot \sigma(\alpha) = -1$, entonces de modo similar, se obtiene la desigualdad

$$-1 < \sigma(\alpha) < 1 - \sqrt{2},$$

de donde

$$0 < \alpha + \sigma(\alpha) < 2.$$

Pero siendo un entero par, el número $\alpha + \sigma(\alpha)$ no puede estar entre 0 y 2. ∎

3.3.3. Teorema. *Todos los elementos invertibles en $\mathbb{Z}[\sqrt{2}]$ son de la forma $\pm(1+\sqrt{2})^n$ para $n \in \mathbb{Z}$.*

Demostración. El número $1 + \sqrt{2}$ es invertible en $\mathbb{Z}[\sqrt{2}]$, y por lo tanto $\pm(1+\sqrt{2})^n$ es invertible para cualquier n. El problema es probar que todos los elementos invertibles tienen esta forma. Sea entonces $\alpha \in \mathbb{Z}[\sqrt{2}]$ un elemento invertible.

[*] John Pell (1611–1685), matemático inglés. No hay documentos que demuestren que Pell trabajó en algún momento de su vida en la “ecuación de Pell”; la atribución del nombre se debe a Euler. Así que como matemático, Pell es conocido por una ecuación que nunca estudió.

0) Los casos $\alpha = \pm 1$ son triviales: se tiene $\pm 1 = \pm(1+\sqrt{2})^0$.

1) Asumamos que $\alpha > 1$. Entonces, por el lema anterior, tenemos $\alpha \ge 1+\sqrt{2}$. Se sigue que existe un número $n = 1,2,3,\ldots$ tal que
$$(1+\sqrt{2})^n \le \alpha < (1+\sqrt{2})^{n+1}.$$
Luego,
$$1 \le \alpha\,(1+\sqrt{2})^{-n} < 1+\sqrt{2},$$
donde $\alpha\,(1+\sqrt{2})^{-n}$ es invertible, así que por el lema anterior
$$\alpha = (1+\sqrt{2})^n.$$

2) Si $0 < \alpha < 1$, entonces $\alpha^{-1} > 1$, así que $\alpha^{-1} = (1+\sqrt{2})^n$ para algún $n = 1,2,3,\ldots$ por el caso anterior, y luego $\alpha = (1+\sqrt{2})^{-n}$.

3) Si $\alpha < 0$, entonces $-\alpha > 0$, así que $\alpha = -(1+\sqrt{2})^n$ para algún $n \in \mathbb{Z}$ por los casos anteriores. ■

En general, el anillo $\mathbb{Z}[\sqrt{n}]$ para $n > 1$ libre de cuadrados tiene un número infinito de elementos invertibles: son de la forma $\pm u^n$ para algún $u \in \mathbb{Z}[\sqrt{n}]^\times$ que es precisamente el mínimo elemento invertible $u > 1$. Para la prueba y el modo de encontrar este u, véase por ejemplo [AW2004, Chapter 11].

n:	2	3	5	6	7	10
$u \in \mathbb{Z}[\sqrt{n}]^\times$:	$1+\sqrt{2}$	$2+\sqrt{3}$	$2+\sqrt{5}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$

Ahora si $n \equiv 1 \pmod 4$, el anillo $\mathbb{Z}[\sqrt{n}]$ está contenido en el anillo más grande $\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$. Para encontrar las unidades en este caso, también podemos considerar la norma
$$N(\alpha) := \alpha\cdot\sigma(\alpha), \quad \sigma\left(a + b\,\frac{1+\sqrt{n}}{2}\right) := a + b\,\frac{1-\sqrt{n}}{2} = a + b - b\,\frac{1+\sqrt{n}}{2}.$$
De nuevo, para cualesquiera $\alpha,\beta \in \mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$ se cumple $\sigma(\alpha\beta) = \sigma(\alpha)\,\sigma(\beta)$, y por lo tanto
$$N(\alpha\beta) = N(\alpha)\,N(\beta).$$
Calculamos que
$$N\left(a + b\,\frac{1-\sqrt{n}}{2}\right) = a^2 + ab - \frac{n-1}{4}\,b^2 \in \mathbb{Z},$$
así que las unidades corresponden a las soluciones enteras de la ecuación (véase la figura 3.4 en p. 10)

$$a^2 + ab - \frac{n-1}{4}\,b^2 = \pm 1. \tag{3.1}$$

Para $n < 0$ (es decir, $n = -3,-7,-11,-15,-19,-23$), la ecuación $a^2+ab-\frac{n-1}{4}\,b^2 = -1$ no tiene soluciones, mientras que $a^2+ab-\frac{n-1}{4}\,b^2 = +1$ define un elipse que tiene un número finito de puntos enteros. A saber, se puede verificar que para $n = -3$ la ecuación correspondiente
$$a^2 + ab + b^2 = 1$$
tiene seis soluciones $(\pm1,0), (0,\pm1), (\pm1,\mp1)$ que corresponden a las raíces sextas de la unidad:
$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]^\times = \left\{\pm1, \pm\frac{1+\sqrt{-3}}{2}, \pm1\mp\frac{1+\sqrt{-3}}{2}\right\} = \{1, \zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5\},$$
mientras que para $n < -3$ las únicas soluciones son triviales:
$$\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]^\times = \{\pm1\}, \quad \text{si } n < -3.$$

De nuevo, si $n > 1$, entonces la ecuación (3.1) define una hipérbola que tendrá un número infinito de puntos enteros. Por ejemplo, para $n = 5$ se pueden encontrar muchos puntos enteros en la hipérbola (véase la figura 3.5 en p. 11)

$$a^2 + ab - b^2 = \pm 1.$$

Las unidades correspondientes son

$$\mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big]^\times = \Big\{\pm\Big(\frac{1+\sqrt{5}}{2}\Big)^n \Bigm| n \in \mathbb{Z}\Big\}.$$

En general, para $n > 0$ siempre existe $u \in \mathbb{Z}\Big[\frac{1+\sqrt{n}}{2}\Big]^\times$ tal que las unidades en $\mathbb{Z}\Big[\frac{1+\sqrt{n}}{2}\Big]$ son de la forma $\pm u^n$ para $n \in \mathbb{Z}$.

n:	5	13	17	21	29	33
$u \in \mathbb{Z}\Big[\frac{1+\sqrt{n}}{2}\Big]^\times$:	$\frac{1+\sqrt{5}}{2}$	$1 + \frac{1+\sqrt{13}}{2}$	$3 + 2\,\frac{1+\sqrt{17}}{2}$	$2 + \frac{1+\sqrt{21}}{2}$	$2 + \frac{1+\sqrt{29}}{2}$	$19 + 8\,\frac{1+\sqrt{33}}{2}$

3.3.4. Comentario (♣). El resultado de la teoría de números algebraica que explica y generaliza nuestros cálculos se llama el **teorema de las unidades de Dirichlet**.

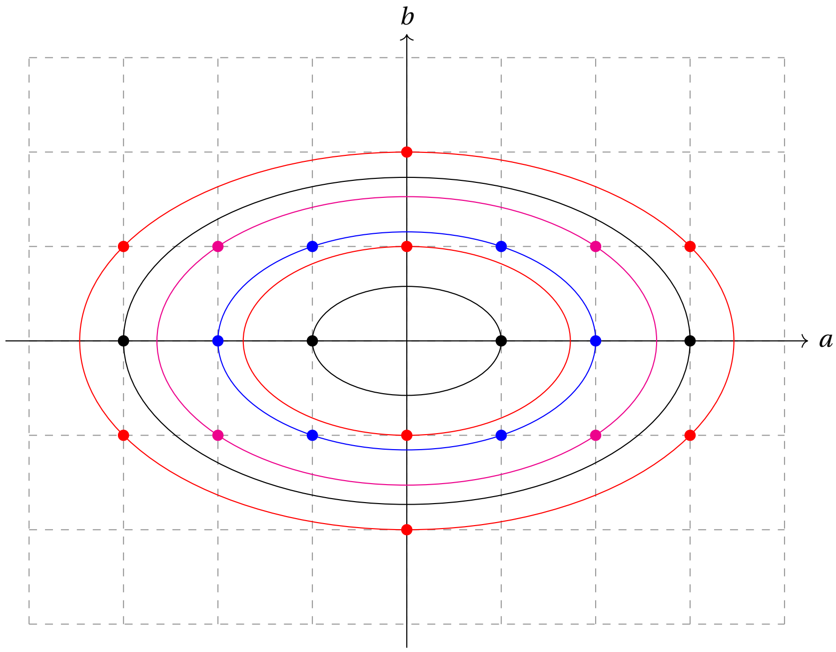

Figura 3.1: Puntos enteros en los elipses $a^2 + 3b^2 = n$ para $n = 1, 3, 4, 7, 9, 12$

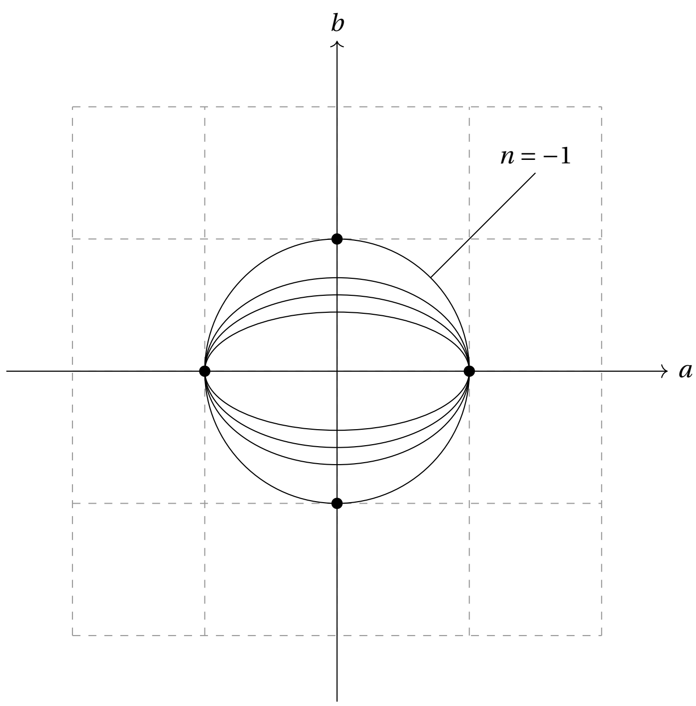

Figura 3.2: Puntos enteros en los elipses $a^2 - nb^2 = 1$ para $n = -1, -2, -3, -5$

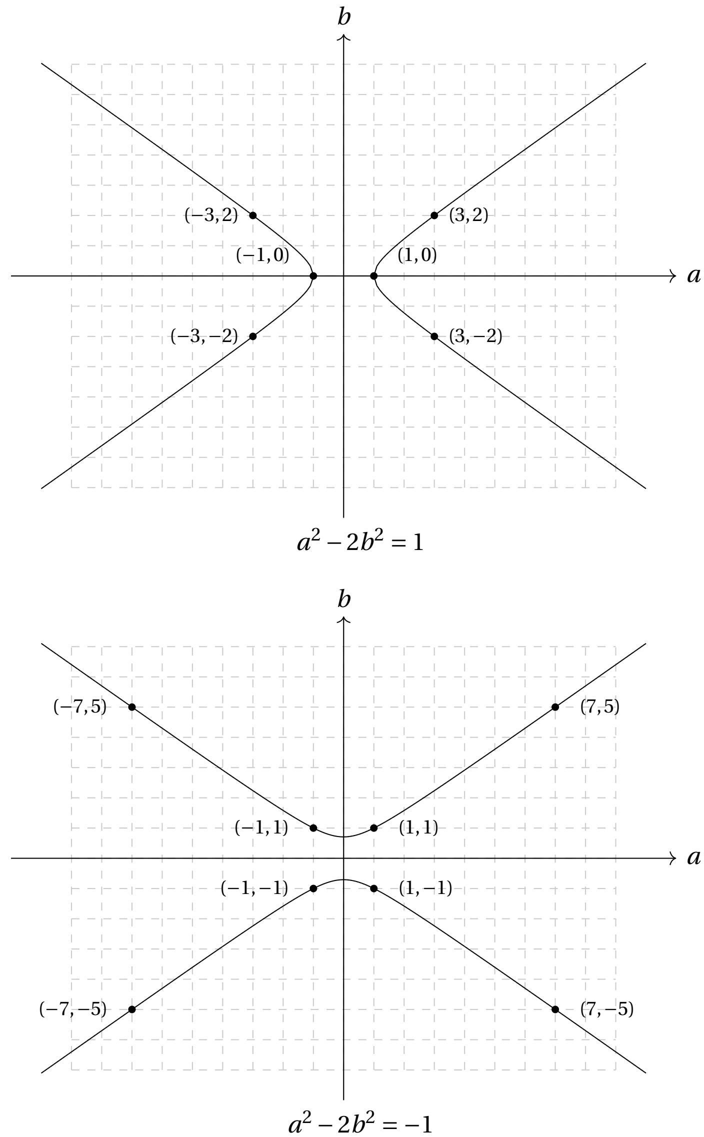

Figura 3.3: Algunos puntos enteros en las hipérbolas $a^2 - 2b^2 = \pm 1$

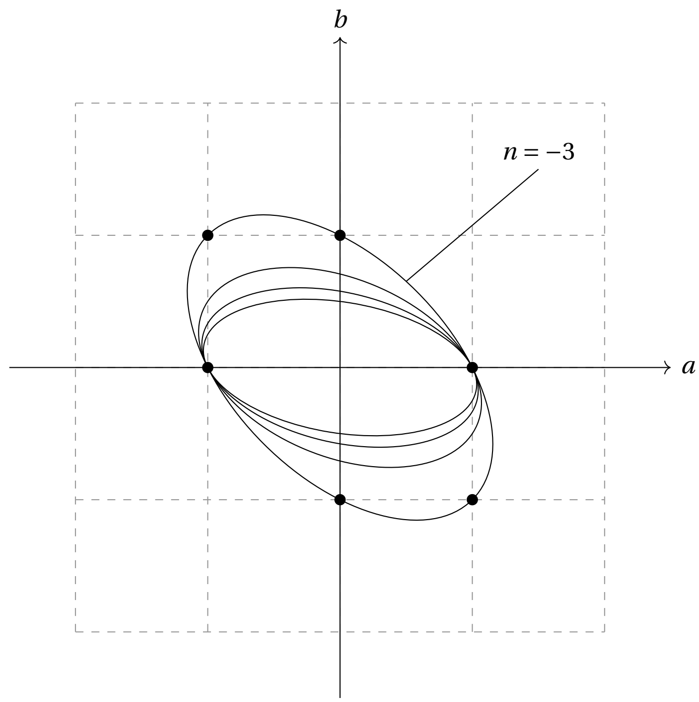

Figura 3.4: Puntos enteros en los elipses $a^2 + ab - \frac{n-1}{4} b^2 = 1$ para $n = -3, -7, -11, -15$

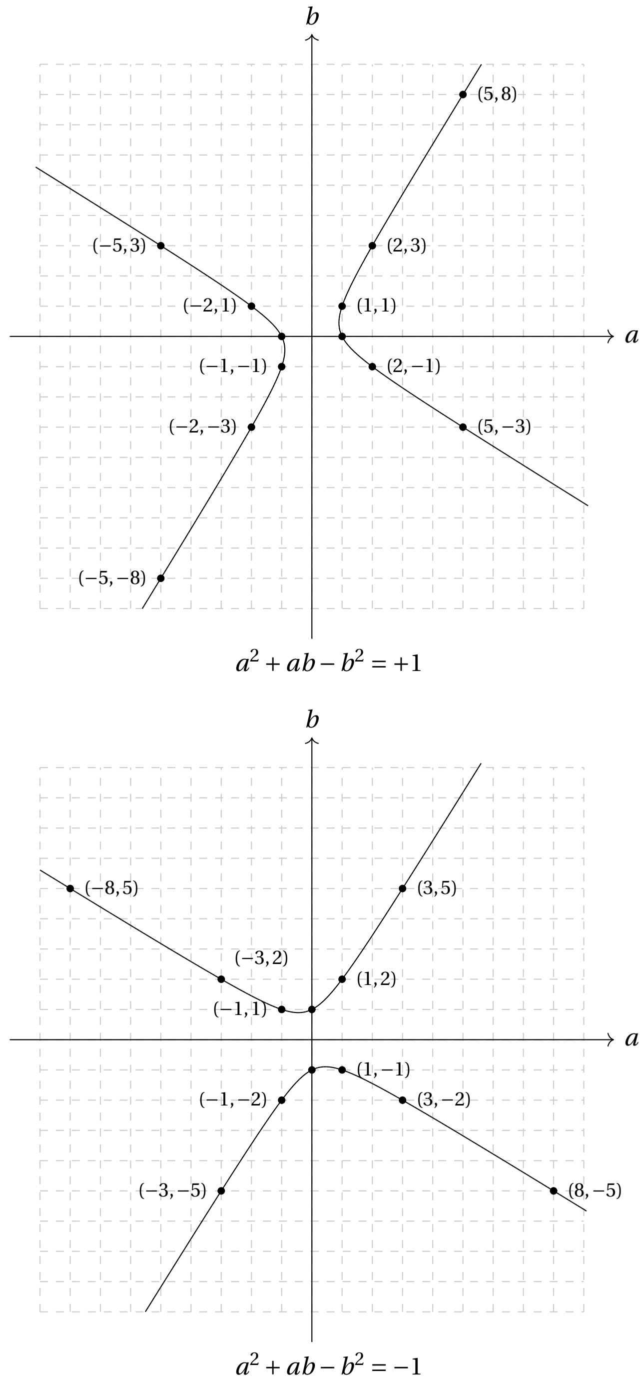

Figura 3.5: Algunos puntos enteros en las hipérbolas $a^2 + ab - b^2 = \pm 1$

3.4 Ideales en anillos conmutativos

3.4.1. Definición. Sea A un anillo conmutativo. Se dice que un subconjunto $\mathfrak{a} \subseteq A$ es un **ideal** en A si se cumplen las siguientes propiedades.

0) $\mathfrak{a} \neq \emptyset$.

1) $\mathfrak{a}$ es cerrado respecto a la suma: para cualesquiera $x, y \in \mathfrak{a}$ se tiene $x + y \in \mathfrak{a}$.

2) $\mathfrak{a}$ es cerrado respecto a la multiplicación por los elementos de A: para cualesquiera $x \in \mathfrak{a}$, $a \in A$ se tiene $ax \in \mathfrak{a}$.

Notamos que las condiciones de arriba implican que $0 \in \mathfrak{a}$: en efecto, ya que $\mathfrak{a} \neq \emptyset$, entonces existe un elemento $x \in \mathfrak{a}$, y luego $0 = 0 \cdot x \in \mathfrak{a}$. De la misma manera, la definición implica que $\mathfrak{a}$ está cerrado respecto a los elementos opuestos: para todo $x \in \mathfrak{a}$ tenemos $-x = (-1) \cdot x \in \mathfrak{a}$.

Un ideal no es lo mismo que un subanillo: primero, no se pide que $1 \in \mathfrak{a}$ (de hecho, en este caso la condición 2) implicaría que $a = a \cdot 1 \in \mathfrak{a}$ para todo $a \in A$, y luego $\mathfrak{a} = A$, que no es muy interesante); segundo, en lugar de la condición $x, y \in \mathfrak{a} \Rightarrow xy \in \mathfrak{a}$ se pide la condición 2) que es más fuerte.

3.4.2. Comentario. Vamos a denotar los ideales por las $\mathfrak{letras\ góticas}$ minúsculas $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$. He aquí el alfabeto gótico completo.

$$
\begin{array}{ccccccccccccc}
\mathfrak{A}\mathfrak{a} & \mathfrak{B}\mathfrak{b} & \mathfrak{C}\mathfrak{c} & \mathfrak{D}\mathfrak{d} & \mathfrak{E}\mathfrak{e} & \mathfrak{F}\mathfrak{f} & \mathfrak{G}\mathfrak{g} & \mathfrak{H}\mathfrak{h} & \mathfrak{I}\mathfrak{i} & \mathfrak{J}\mathfrak{j} & \mathfrak{K}\mathfrak{k} & \mathfrak{L}\mathfrak{l} & \mathfrak{M}\mathfrak{m} \\
\mathfrak{N}\mathfrak{n} & \mathfrak{O}\mathfrak{o} & \mathfrak{P}\mathfrak{p} & \mathfrak{Q}\mathfrak{q} & \mathfrak{R}\mathfrak{r} & \mathfrak{S}\mathfrak{s} & \mathfrak{T}\mathfrak{t} & \mathfrak{U}\mathfrak{u} & \mathfrak{V}\mathfrak{v} & \mathfrak{W}\mathfrak{w} & \mathfrak{X}\mathfrak{x} & \mathfrak{Y}\mathfrak{y} & \mathfrak{Z}\mathfrak{z}
\end{array}
$$

3.4.3. Comentario (♣). Si A es un anillo no conmutativo, hay que considerar tres diferentes tipos de ideales: izquierdos, derechos y bilaterales. Las condiciones 0) y 1) son siempre las mismas, pero la condición 2) es diferente. A saber, un ideal $\mathfrak{a} \subseteq A$ es

- **izquierdo** si $x \in \mathfrak{a},\ a \in A \Longrightarrow ax \in \mathfrak{a}$;
- **derecho** si $x \in \mathfrak{a},\ a \in A \Longrightarrow xa \in \mathfrak{a}$;
- **bilateral** si es izquierdo y derecho a la vez.

Note que si A es conmutativo, entonces $ax = xa$ y las tres nociones coinciden. Por ejemplo, en el anillo de matrices $M_2(k)$ las matrices de la forma

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}, \quad x, y \in k$$

forman un ideal izquierdo que no es derecho, mientras que las matrices de la forma

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}, \quad x, y \in k$$

forman un ideal derecho que no es izquierdo. Para simplificar la exposición, en este curso no vamos a hablar de ideales en anillos no conmutativos. El lector interesado puede formular y probar nuestros los resultados para ideales derechos, izquierdos y bilaterales, o también consultar algún libro de texto que trabaja con anillos no conmutativos.

3.4.4. Ejemplo. $0 := \{0\}$ y A son ideales en cualquier anillo conmutativo A. Un ideal $\mathfrak{a} \subseteq A$ tal que $\mathfrak{a} \neq A$ se llama un **ideal propio**. ▲

3.4.5. Ejemplo. Consideremos el anillo de los números enteros $\mathbb{Z}$. Para un número fijo $n = 0, 1, 2, \ldots$ los múltiplos de n forman un ideal

$$n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\}.$$ ▲

El último ejemplo puede ser generalizado a los múltiplos en cualquier anillo conmutativo.

3.4.6. Observación. *Sea A un anillo conmutativo y $x \in A$ un elemento fijo. Entonces, los múltiplos de x forman un ideal*

$$(x) := \{ax \mid a \in A\}$$

*que se llama el **ideal principal generado por** x.* □

En particular, notamos que $(0) = 0$ es el ideal nulo y $(1) = A$.

La relación de divisibilidad $x \mid y$ puede ser interpretada en términos de ideales principales (x) e (y).

3.4.7. Observación (Divisibilidad e ideales principales). *Sean A un anillo conmutativo y $x, y \in A$.*

1) $x \mid y$ si y solamente si $(x) \supseteq (y)$.

2) $x \sim y$ si y solamente si $(x) = (y)$.

3) $x \in A^\times$ si y solamente si $(x) = A$.

4) si $x \mid y$, pero $y \nmid x$, entonces $(x) \supsetneq (y)$. □

3.4.8. Observación. *Sea A un anillo conmutativo.*

1) Para un ideal $\mathfrak{a} \subseteq A$ se tiene $\mathfrak{a} = A$ si y solo si $u \in \mathfrak{a}$ para algún elemento invertible $u \in A^\times$.

2) A es un cuerpo si y solo si 0 y A son los únicos ideales en A.

Demostración. En 1), notamos que si $\mathfrak{a} = A$, entonces $1 \in \mathfrak{a}$ y $1 \in A^\times$. Viceversa, si $u \in A^\times$ es un elemento tal que $u \in \mathfrak{a}$, entonces para todo $a \in A$

$$a = a \cdot 1 = a\,(u^{-1}\,u) = (a\,u^{-1})\,u \in \mathfrak{a}.$$

En 2), si A es un cuerpo, entonces todo ideal no nulo $\mathfrak{a} \neq 0$ contiene un elemento $x \in \mathfrak{a}$, $x \neq 0$, y luego $x \in A^\times$ y $\mathfrak{a} = A$ según la parte 1). Viceversa, si 0 y A son los únicos ideales en A, para $x \neq 0$ podemos considerar el ideal

$$(x) := \{ax \mid a \in A\}.$$

Tenemos $(x) \neq 0$, así que $(x) = A$. En particular, $ax = 1$ para algún $a \in A$, y este elemento a es el inverso de x. ■

3.4.9. Observación. *Sea A un anillo conmutativo.*

1) Si $\mathfrak{a}_i \subseteq A$ es una familia de ideales en A, entonces $\bigcap_{i \in I} \mathfrak{a}_i$ es un ideal en A.

2) Si $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots \subseteq A$ es una cadena de ideales en A, entonces $\bigcup_{i \in I} \mathfrak{a}_i$ es un ideal en A. □

En práctica los ideales se especifican por sus generadores.

3.4.10. Definición. Sea A un anillo conmutativo y $S \subset A$ un subconjunto. El **ideal generado por** S es el mínimo ideal que contiene a S:

$$(S) := \bigcap_{\substack{\text{ideal } \mathfrak{a} \subseteq A \\ S \subseteq \mathfrak{a}}} \mathfrak{a} = \Bigl\{ \text{sumas finitas } \sum_i a_i\,x_i \Bigm| a_i \in A, x_i \in S \Bigr\}. \tag{3.2}$$

Si $S = \{x_1, \ldots, x_n\}$ es un conjunto finito, se usa la notación

$$(x_1, \ldots, x_n) := (S).$$

Verifiquemos la igualdad en (3.2). Si $\mathfrak{a}$ es un ideal tal que $S \subseteq \mathfrak{a}$, entonces $\sum_i a_i x_i \in \mathfrak{a}$ para cualesquiera $a_i \in A$, $x_i \in S$. Además, se ve que el conjunto formado por las sumas finitas $\sum_i a_i x_i$ es un ideal.

3.4.11. Ejemplo. Consideremos el ideal $(2, 1+\sqrt{-3})$ en el anillo $\mathbb{Z}[\sqrt{-3}]$. Sus elementos son las combinaciones

$$\alpha \cdot 2 + \beta \cdot (1+\sqrt{-3}), \quad \alpha, \beta \in \mathbb{Z}[\sqrt{-3}].$$

Este ideal no puede ser generado por un elemento $\gamma \in \mathbb{Z}[\sqrt{-3}]$. En efecto, si

$$(2, 1+\sqrt{-3}) = (\gamma),$$

entonces 2 y $1+\sqrt{-3}$ son múltiplos de γ, pero esto es posible solo cuando $\gamma = \pm 1$ (los elementos 2 y $1 \pm \sqrt{-3}$ son irreducibles). En este caso tendríamos $(2, 1+\sqrt{-3}) = \mathbb{Z}[\sqrt{-3}]$ y en particular

$$1 = \alpha \cdot 2 + \beta \cdot (1+\sqrt{-3})$$

para algunos $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$. Luego, multiplicando todo por $1-\sqrt{-3}$, se obtiene

$$1-\sqrt{-3} = \alpha \cdot 2 \cdot (1-\sqrt{-3}) + \beta \cdot 4,$$

lo que implica que $2 \mid (1-\sqrt{-3})$ en $\mathbb{Z}[\sqrt{-3}]$, pero no es el caso. ▲

3.4.12. Ejemplo. En el anillo de polinomios con coeficientes enteros $\mathbb{Z}[X]$, consideremos el ideal (p, X) donde $p = 2, 3, 5, 7, 11, \ldots$ es un número primo, visto como un polinomio constante. Tenemos

$$(p, X) = \{f\,p + g\,X \mid f, g \in \mathbb{Z}[X]\} = \{a_n X^n + \cdots + a_1 X + a_0 \mid a_0, a_1, \ldots, a_n \in \mathbb{Z},\ p \mid a_0\}.$$

En particular, se ve que

$$(p, X) \subsetneq \mathbb{Z}[X].$$

Este ideal no puede ser generado por un elemento. Asumamos que $(p, X) = (f)$ para algún polinomio $f \in \mathbb{Z}[X]$. En particular, esto quiere decir que $f \mid p$ y $f \mid X$, lo que sucede solo para $f = \pm 1$, pero $(\pm 1) = \mathbb{Z}[X]$. Contradicción. ▲

3.4.13. Ejemplo. Sea k un cuerpo. El anillo de polinomios en dos variables $k[X, Y]$ es un dominio, y sus elementos invertibles son los polinomios constantes no nulos. Consideremos el ideal (X, Y). Se puede ver que este ideal consiste en los polinomios con término constante nulo:

$$(X, Y) = \{f\,X + g\,Y \mid f, g \in k[X, Y]\} = \{h \in k[X, Y] \mid h(0, 0) = 0\}.$$

Este ideal no puede ser generado por un solo elemento. En efecto, si $(X, Y) = (f)$, entonces $f \mid X$ y $f \mid Y$. Sin embargo, X e Y son irreducibles en $k[X, Y]$, así que esto es posible solo cuando $f = c \neq 0$ es un polinomio constante no nulo, pero $c \notin (X, Y)$. ▲

Existen ideales que no pueden ser generados por un número finito de elementos.

3.4.14. Ejemplo. Consideremos el anillo de las funciones continuas $f \colon \mathbb{R} \to \mathbb{R}$ respecto a las operaciones punto por punto. Para cada $a \in \mathbb{R}$, sea

$$I_a := \{\text{funciones continuas } f \colon \mathbb{R} \to \mathbb{R} \mid f(x) = 0 \text{ para } x \geq a\}.$$

Este es un ideal. Consideremos la función

$$f_a(x) := \begin{cases} 0, & \text{si } x \geq a, \\ a - x, & \text{si } x < a. \end{cases}$$

Tenemos $f_a \in I_a$. Ahora si $a < b$, entonces $I_a \subseteq I_b$. De hecho, la inclusión es estricta, puesto que $f_b \in I_b$, pero $f_b \notin I_a$. La unión

$$I := \bigcup_{a \in \mathbb{R}} I_a$$

es un ideal que consiste en las funciones continuas $f: \mathbb{R} \to \mathbb{R}$ tales que $f(x) = 0$ para x suficientemente grande. Este ideal no puede ser generado por un número finito de elementos: si tenemos

$$I = (g_1, \ldots, g_n),$$

entonces existe $a \in \mathbb{R}$ tal que $g_1(x) = \cdots = g_n(x) = 0$ para $x \ge a$. Pero en este caso para cualquier función

$$g = h_1 g_1 + \cdots + h_n g_n \in (g_1, \ldots, g_n)$$

se tiene $g(x) = 0$ para $x \ge a$, y entonces $f_b \notin (g_1, \ldots, g_n)$ para $b > a$. ▲

3.5 Dominios euclidianos

Un dominio euclidiano es un dominio que admite la división con resto.

3.5.1. Definición. Se dice que un dominio A es un **dominio euclidiano** si sobre A existe una función $\delta\colon A \setminus \{0\} \to \mathbb{N}$ (llamada **norma euclidiana**) que satisface la siguiente propiedad. Para todo $a, b \in A$, $b \ne 0$ existen $q, r \in A$ tales que $a = qb + r$, donde $r = 0$ o $\delta(r) < \delta(b)$.

El ejemplo primordial de dominios euclidianos fue estudiado por Euclides en sus "Elementos".

3.5.2. Ejemplo. El anillo de los enteros $\mathbb{Z}$ es un dominio euclidiano respecto al valor absoluto $\delta(a) := |a|$. En efecto, dados $a, b \in \mathbb{Z}$, $b \ne 0$, podemos considerar el conjunto

$$X := \{a - nb \mid n \in \mathbb{Z}\}.$$

Notamos que este conjunto contiene elementos no negativos. Sea $r = a - qb$ el elemento mínimo no negativo en X. Si tenemos $r \ge |b|$, podemos considerar dos casos:

1) si $b > 0$, entonces $r = a - qb \ge b$, así que

$$0 \le a - (q+1)\, b < r.$$

2) si $b < 0$, entonces $r = a - qb \ge -b$, así que

$$0 \le a - (q-1)\, b < r.$$

Pero ambos casos contradicen nuestra elección de r. Entonces, necesariamente $0 \le r < |b|$. ▲

3.5.3. Ejemplo. Sea k un cuerpo. El anillo de polinomios en una variable $k[X]$ es un dominio euclidiano respecto al grado $\delta(f) := \deg f$. Esto fue probado en el capítulo anterior. ▲

3.5.4. Ejemplo. El anillo de los enteros de Gauss $\mathbb{Z}[i]$ es un dominio euclidiano respecto a la norma

$$N(a + bi) := (a + bi)\,(a - bi) = a^2 + b^2.$$

En efecto, dados dos elementos $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \ne 0$, podemos dividir α por β en el cuerpo $\mathbb{Q}(i)$:

$$\frac{\alpha}{\beta} = x + yi \quad \text{para algunos } x, y \in \mathbb{Q}.$$

Ahora podemos escoger $a, b \in \mathbb{Z}$ tales que

$$|x - a| \le \frac{1}{2}, \quad |y - b| \le \frac{1}{2}.$$

Pongamos

$$q := a + bi \in \mathbb{Z}[i]$$

y

$$r := \alpha - q\beta = (x + yi)\,\beta - \beta\,(a + bi) = \beta\,(x - a + (y - b)\,i).$$

Por la multiplicatividad de la norma,

$$N(r) = N(\beta)\,N(x - a + (y - b)\,i) = N(\beta)\left((x - a)^2 + (y - b)^2\right) \le \frac{1}{2}\,N(\beta).$$

En particular,

$$\alpha = q\beta + r, \quad 0 \le N(r) < N(\beta).$$ ▲

3.5.5. Ejemplo. Las mismas consideraciones demuestran que el anillo $\mathbb{Z}[\sqrt{-2}]$ es un dominio euclidiano respecto a la norma

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

Dejo los detalles al lector. Sin embargo, para el anillo $\mathbb{Z}[\sqrt{-3}]$ con la norma $N(a + b\sqrt{-3}) = a^2 + 3b^2$ este argumento ya no va a funcionar (¿por qué?) y de hecho, más adelante veremos que $\mathbb{Z}[\sqrt{-3}]$ no es un dominio euclidiano. ▲

3.5.6. Ejemplo. Las mismas ideas nos permiten probar que el anillo $\mathbb{Z}[\sqrt{2}]$ es un dominio euclidiano respecto a la norma euclidiana

$$\delta(\alpha) := |N(\alpha)| = |a^2 - 2b^2|,$$

donde $\alpha = a + b\sqrt{2}$. ▲

3.5.7. Ejemplo. Consideremos los anillos

$$\mathbb{Z}[\omega], \quad \omega := \frac{1 + \sqrt{n}}{2}, \quad \text{donde } n = -3, -7, -11$$

con la norma

$$N(a + b\omega) := \left(a + b\,\frac{1 + \sqrt{n}}{2}\right)\left(a + b\,\frac{1 - \sqrt{n}}{2}\right) = a^2 + ab + \frac{1 - n}{4}\,b^2.$$

Para $\alpha, \beta \in \mathbb{Z}[\omega]$ con $\beta \ne 0$, podemos dividir α por β en el cuerpo $\mathbb{Q}(\omega)$:

$$\frac{\alpha}{\beta} = x + y\omega \quad \text{para algunos } x, y \in \mathbb{Q}.$$

Ahora existen $a, b \in \mathbb{Z}$ tales que

$$N((x - a) + (y - b)\,\omega) = (x - a)^2 + (x - a)\,(y - b) + \frac{1 - n}{4}\,(y - b)^2 < 1. \tag{3.3}$$

A saber, la desigualdad de arriba define un elipse centrado en (a, b) y tales elipses para $(a, b) \in \mathbb{Z}^2$ recubren el plano si $n = -3, -7, -11$. También se ve que para $n = -15$ ya no es el caso. Véase la figura 3.6.

Pongamos entonces

$$q := a + b\omega \in \mathbb{Z}[\omega], \quad r := \alpha - q\beta = \beta\,(x - a + (y - b)\,\omega).$$

Por la multiplicatividad de la norma,

$$N(r) = N(\beta)\,N(x - a + (y - b)\,\omega) < N(\beta).$$ ▲

Un truco con los elipses (3.3) fue necesario porque si nada más escojamos como arriba $a, b \in \mathbb{Z}$ tales que $|x - a| \le \frac{1}{2}$ y $|y - b| \le \frac{1}{2}$, entonces para $n = -7$ ya se obtiene

$$(x - a)^2 + (x - a)\,(y - b) + 2\,(y - b)^2 \le \frac{1}{4} + \frac{1}{4} + 2 \cdot \frac{1}{4} = 1,$$

que no nos ayuda.

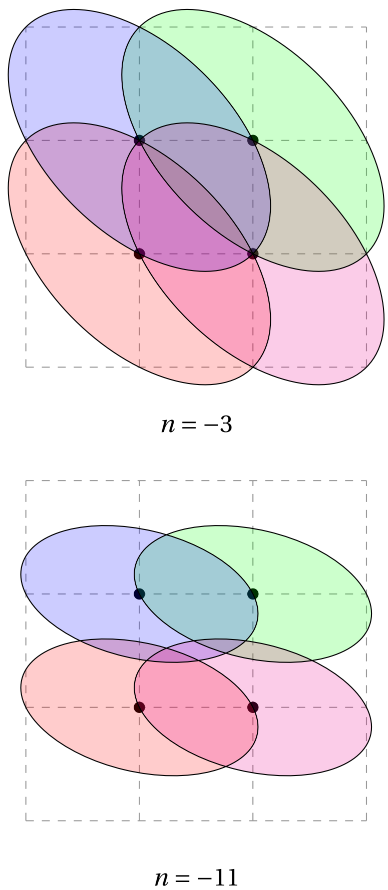

Figura 3.6: Recubrimiento del plano por los elipses $(x-a)^2 + (x-a)(y-b) + \frac{1-n}{4}(y-b)^2 < 1$ para $(a,b) \in \mathbb{Z}^2$ y $n = -3, -7, -11$. Para $n = -15$ ya no hay recubrimiento

3.5.8. Comentario. En la división con resto $a = qb+r$ no se supone que los elementos q y r son únicos. Aunque en el capítulo anterior hemos visto que son únicos para la división con resto en el anillo de polinomios $k[X]$, los elementos q y r no suelen ser únicos en otros casos.

Por ejemplo, la división con resto de 7 por -3 en $\mathbb{Z}$ nos da

$$7 = (-3)\cdot(-3) - 2 = (-2)\cdot(-3) + 1.$$

Podemos forzar la unicidad del cociente y resto pidiendo que $r \ge 0$, pero esta restricción es algo artificial.

Para dar otro ejemplo, en el anillo $\mathbb{Z}[i]$, la división con resto de $3+i$ por 2 nos da cuatro diferentes opciones:

$$\begin{aligned} 3+i &= 1\cdot 2 + (1+i) \\ &= (1+i)\cdot 2 + (1-i) \\ &= 2\cdot 2 + (-1+i) \\ &= (2+i)\cdot 2 + (-1-i), \end{aligned}$$

y no está claro cuál opción es más canónica que otras.

3.6 Dominios de ideales principales

3.6.1. Definición. Sea A un dominio tal que todo ideal $\mathfrak{a} \subseteq A$ es principal; es decir, $\mathfrak{a} = (x)$ para algún $x \in A$. En este caso se dice que A es un **dominio de ideales principales**.

3.6.2. Ejemplo. Todo cuerpo es obviamente un dominio de ideales principales: sus únicos ideales son (0) y (1). ▲

3.6.3. Ejemplo. Como hemos notado en 3.4.11, 3.4.12, 3.4.13, los anillos $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[X]$, $k[X,Y]$ no son dominios de ideales principales:

1) el ideal $(2, 1+\sqrt{-3})$ no es principal en $\mathbb{Z}[\sqrt{-3}]$,

2) el ideal (p, X) no es principal en $\mathbb{Z}[X]$,

3) el ideal (X, Y) no es principal en $k[X,Y]$. ▲

La razón de ser de la noción de dominio euclidiano es el siguiente resultado.

3.6.4. Teorema. *Todo dominio euclidiano es un dominio de ideales principales.*

Demostración. Sea A un dominio euclidiano y sea $\mathfrak{a} \subseteq A$ un ideal. Necesitamos probar que $\mathfrak{a}$ es un ideal principal. Si $\mathfrak{a} = (0)$, no hay que probar nada. Si $\mathfrak{a} \neq (0)$, sea $x \in \mathfrak{a}$ un elemento con la norma euclidiana $\delta(x)$ mínima posible. Tenemos $(x) \subseteq \mathfrak{a}$. Supongamos que existe un elemento $y \in \mathfrak{a}$ tal que $y \notin (x)$. Esto quiere decir que y no puede ser escrito como qx para algún $q \in A$. Podemos dividir y por x con resto: tenemos

$$y = qx + r, \quad r \neq 0,\ \delta(r) < \delta(x)$$

para algunos $q, r \in A$. Sin embargo, $r = y - qx \in \mathfrak{a}$, y luego $\delta(r) < \delta(x)$ contradice nuestra elección de x. Podemos concluir que $\mathfrak{a} = (x)$. ■

3.6.5. Ejemplo. Los siguientes anillos son dominios de ideales principales porque son dominios euclidianos:

1) $\mathbb{Z}$ (ejemplo 3.5.2),

2) $\mathbb{Z}[i]$ (ejemplo 3.5.4), $\mathbb{Z}[\sqrt{-2}]$ (ejercicio 3.16), $\mathbb{Z}[\sqrt{2}]$ (ejercicio 3.17),

3) $\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$ para $n = -3, -7, -11$ (ejemplo 3.5.7),

4) $k[X]$, donde k es cualquier cuerpo (capítulo anterior). ▲

3.6.6. Proposición. *En un dominio de ideales principales todo elemento irreducible es primo.*

Demostración. Sea $p \in A$ un elemento irreducible. Asumamos que para algunos $a, b \in A$ se tiene $p \mid ab$. Hay que probar que $p \mid a$ o $p \mid b$. Consideremos el ideal generado por p y a:

$$(p, a) := \{xp + ya \mid x, y \in A\}.$$

Puesto que A es un dominio de ideales principales, se tiene $(p, a) = (c)$ para algún $c \in A$. En particular, $c \mid p$ y $c \mid a$. Ahora dado que p es irreducible, se tiene $c \sim p$ o $c \in A^\times$.

1) Si $c \sim p$, entonces $p \mid c$ y $c \mid a$ implica que $p \mid a$.

2) Si $c \in A^\times$, entonces tenemos $c = xp + ya$ para algunos $x, y \in A$, y luego $bc = pbx + yab$. Dado que $p \mid ab$, esto implica que $p \mid bc$, y luego $p \mid bcc^{-1} = b$. ■

3.6.7. Ejemplo. Ya hemos observado en 3.2.6 que en el anillo $\mathbb{Z}[\sqrt{-3}]$ se tiene

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})\,(1 - \sqrt{-3}),$$

donde 2, $1 \pm \sqrt{-3}$ son irreducibles. Esto demuestra que 2 es irreducible, pero no es primo. Como ya notamos en 3.4.11, y como también nos dice el argumento de 3.6.6, el ideal $(2, 1 + \sqrt{-3})$ no es principal en $\mathbb{Z}[\sqrt{-3}]$.

Podemos considerar el anillo más grande

$$\mathbb{Z}[\omega] \supset \mathbb{Z}[\sqrt{-3}], \quad \omega := \frac{1 + \sqrt{-3}}{2}.$$

Como vimos en 3.5.7, este es un dominio euclidiano, así que todo elemento irreducible en $\mathbb{Z}[\omega]$ es primo. Los elementos 2 y $1 \pm \sqrt{-3}$ se vuelven asociados:

$$1 + \sqrt{-3} = 2\omega, \quad 1 - \sqrt{-3} = 2\,(1 - \omega),$$

donde ω y $1 - \omega$ son invertibles: tenemos $\omega\,(1 - \omega) = 1$. El ideal $(2, 1 + \sqrt{-3})$ que no era principal en $\mathbb{Z}[\sqrt{-3}]$ sí es principal en $\mathbb{Z}[\omega]$: se tiene

$$(2, 1 + \sqrt{-3}) = (2, 2\omega) = (2).$$ ▲

3.6.8. Ejemplo. En el anillo

$$\mathbb{Z}[\omega], \quad \omega := \frac{1 + \sqrt{-15}}{2},$$

analizando las normas

$$N(a + b\omega) = a^2 + ab + 4b^2,$$

se ve que los elementos 2, ω, $1 - \omega$ son irreducibles: sus normas son iguales a 4 y no hay elementos de norma 2. Notamos que

$$\omega\,(1 - \omega) = \omega - \omega^2 = 4.$$

Ahora $2 \mid \omega\,(1 - \omega)$, pero $2 \nmid \omega$ y $2 \nmid (1 - \omega)$. Esto demuestra que 2 es irreducible pero no es primo en $\mathbb{Z}[\omega]$. Por las mismas consideraciones de 3.6.6 se ve que el ideal $(2, \omega)$ no es principal en $\mathbb{Z}[\omega]$. ▲

3.6.9. Ejemplo. Consideremos el anillo $\mathbb{Z}[\sqrt{n}]$ para $n > 1$ libre de cuadrados y $n \equiv 1 \pmod 4$. La norma es

$$N(a + b\sqrt{n}) = (a + b\sqrt{n})\,(a - b\sqrt{n}) = a^2 - nb^2.$$

En este caso no hay elementos de la norma ± 2: tenemos

$$a^2 - nb^2 \equiv a^2 - b^2 \pmod 4,$$

pero las posibles diferencias de dos cuadrados módulo 4 son $0,1,3$. Ahora

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

pero $2 \nmid (\pm 1 + \sqrt{n})$ (los múltiplos de 2 son de la forma $a + b\sqrt{n}$ con a y b pares).

El anillo más grande $\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$ puede o no puede cumplir la propiedad que todo irreducible es primo. El argumento de arriba no va a funcionar porque $1+\sqrt{n} = 2\,\frac{1+\sqrt{n}}{2}$. ▲

En general, existen dominios de ideales principales que no son dominios euclidianos. Sin embargo, no es fácil encontrar un ejemplo específico: hay que probar que cierto dominio de ideales principales no admite *ninguna* norma euclidiana.

3.6.10. Ejemplo (♣). Sea A un dominio euclidiano que no es un cuerpo. Sea $a \in A$ un elemento no nulo y no invertible con el mínimo posible valor $\delta(a)$. Esto implica que para cualquier elemento $b \in A$ tenemos

$$b = qa + r, \quad \text{donde } r = 0 \text{ o } \delta(r) < \delta(a).$$

Por nuestra elección de a, esto significa que hay dos posibilidades: $a \mid b$ o $r \in A^\times$.

Ahora consideremos el anillo

$$\mathbb{Z}[\omega], \quad \omega := \frac{1+\sqrt{-19}}{2}.$$

Al analizar la norma

$$N(a+b\omega) := (a+b\omega)\,(a+b\overline{\omega}) = a^2 + ab + 5\,b^2$$

se ve que $\mathbb{Z}[\omega]^\times = \{\pm 1\}$ y que en $\mathbb{Z}[\omega]$ no hay elementos de norma 2 o 3. Esto implica que los números 2 y 3 son irreducibles en $\mathbb{Z}[\omega]$.

Ahora si $\mathbb{Z}[\omega]$ fuera un dominio euclidiano, entonces tendríamos algún elemento no nulo y no invertible $\alpha \in \mathbb{Z}[\omega]$ tal que para todo $\beta \in \mathbb{Z}[\omega]$ se cumple $\alpha \mid \beta$, o se puede escribir $\beta = q\alpha + r$ donde $r = \pm 1$. Es decir, α siempre debe dividir a β o $\beta \pm 1$. Primero tomemos $\beta = 2$.

1) Si $\alpha \mid 2$, entonces necesariamente $\alpha = \pm 2$ (como notamos, 2 es irreducible y α no es invertible).

2) Si $\alpha \mid (2+1)$, entonces $\alpha = \pm 3$ (de nuevo, 3 es irreducible y α no es invertible).

3) El caso $\alpha \mid (2-1)$ no es posible, puesto que α no es invertible.

Entonces, necesariamente $\alpha = \pm 2$ o ± 3, así que $N(\alpha) = 4$ o 9. Tomemos ahora $\beta = \omega$. Hay tres casos, pero cada uno de ellos se descarta:

1) $\alpha \nmid \omega$, puesto que $N(\omega) = 5$;

2) $\alpha \nmid (1+\omega)$, puesto que $N(1+\omega) = 7$;

3) $\alpha \nmid (-1+\omega)$, puesto que $N(-1+\omega) = 5$.

Podemos concluir que $\mathbb{Z}[\omega]$ no es un dominio euclidiano. Sin embargo, se puede probar que es un dominio de ideales principales. Para una prueba directa, véase [DF2004, §8.2], pero esto surge de ciertos cálculos en la teoría de números algebraica.

En efecto, en lugar de $\frac{1+\sqrt{-19}}{2}$ también funcionaría

$$\omega = \frac{1+\sqrt{-43}}{2}, \quad \frac{1+\sqrt{-67}}{2}, \quad \frac{1+\sqrt{-163}}{2}.$$ ▲

Los ejemplos como el de arriba nada más demuestran que la noción de dominio euclidiano no tiene ningún sentido profundo; es puramente utilitaria y se ocupa solo para probar que ciertos anillos son dominios de ideales principales. En práctica no es fácil demostrar que algo es un dominio euclidiano (salvo ciertos casos básicos como $\mathbb{Z}$ y $k[X]$), ni que no lo es.

3.7 MCD y MCM

3.7.1. Definición. Sean A un dominio y $a_1,\dots,a_n \in A$. Se dice que $d \in A$ es un **máximo común divisor** (**mcd**) de $a_1,\dots,a_n$ y se ecribe $d = \operatorname{mcd}(a_1,\dots,a_n)$ si

1) $d \mid a_1, \dots, d \mid a_n$,

2) si para otro elemento $c \in A$ se cumple $c \mid a_1, \dots, c \mid a_n$, entonces $c \mid d$.

Se dice que $m \in A$ es un **mínimo común múltiplo** (**mcm**) de $a_1,\dots,a_n$ y se escribe $m = \operatorname{mcm}(a_1,\dots,a_n)$ si

1) $a_1 \mid m, \dots, a_n \mid m$,

2) si para otro elemento $c \in A$ se cumple $a_1 \mid c, \dots, a_n \mid c$, entonces $m \mid c$.

3.7.2. Comentario. Note que la definición no afirma que mcd y mcm siempre existen. Esto depende del dominio A.

El lector probablemente conoce bien el concepto del mcd y mcm para los números enteros, así que veamos algún ejemplo donde el mcd no existe.

3.7.3. Ejemplo. En el anillo $\mathbb{Z}[\sqrt{-3}]$ consideremos los elementos

$$\alpha = 4 = 2 \cdot 2 = (1+\sqrt{-3})\,(1-\sqrt{-3}) \quad \text{y} \quad \beta = 2 \cdot (1+\sqrt{-3}).$$

Supongamos que existe $\delta = \operatorname{mcd}(\alpha,\beta)$. Notamos que 2 y $1+\sqrt{-3}$ son divisores comunes de α y β, así que se tiene

$$2 \mid \delta, \quad (1+\sqrt{-3}) \mid \delta, \quad \delta \mid \alpha, \quad \delta \mid \beta.$$

Pero $2 \nsim (1+\sqrt{-3})$ y $\alpha \nsim \beta$, así que la única opción que nos queda para la norma es $N(\delta) = 8$. Sin embargo, $a^2 + 3b^2 \neq 8$ para ningún $a,b \in \mathbb{Z}$. ▲

3.7.4. Observación. *Si para $a_1,\dots,a_n \in A$ existe su mcd (resp. mcm), entonces este está definido de modo único salvo la relación de equivalencia $\sim$.*

Demostración. Si d e d' son mcd de $a_1,\dots,a_n$, entonces la definición implica que $d \mid d'$ y $d' \mid d$. De la misma manera para mcm. ■

Debido a la última observación, todas las identidades con mcd y mcm se entienden salvo $\sim$.

3.7.5. Comentario. En el anillo de los números enteros $\mathbb{Z}$, normalmente como $\operatorname{mcd}(a_1,\dots,a_n)$ y $\operatorname{mcm}(a_1,\dots,a_n)$ se toma un número positivo. Para los polinomios $k[X]$, normalmente se toma un polinomio mónico.

3.7.6. Proposición. *El mcd y mcm tienen las siguientes propiedades para cualesquiera $a,b,c \in A$.*

1) $\operatorname{mcd}(a,0) = a$ *y* $\operatorname{mcm}(a,0) = 0$,

2) $\operatorname{mcd}(a,a) = \operatorname{mcm}(a,a) = a$

3) $\operatorname{mcd}(a,b) = a$ *si y solamente si* $a \mid b$.
$\operatorname{mcm}(a,b) = a$ *si y solamente si* $b \mid a$.

4) $\operatorname{mcd}(a,b) = \operatorname{mcd}(b,a)$.
$\operatorname{mcm}(a,b) = \operatorname{mcm}(b,a)$.

5) $\operatorname{mcd}(\operatorname{mcd}(a,b),c) = \operatorname{mcd}(a,\operatorname{mcd}(b,c)) = \operatorname{mcd}(a,b,c)$.
$\operatorname{mcm}(\operatorname{mcm}(a,b),c) = \operatorname{mcm}(a,\operatorname{mcm}(b,c)) = \operatorname{mcm}(a,b,c)$.

6) Si $a = qb + r$*, entonces* $\operatorname{mcd}(a,b) = \operatorname{mcd}(b,r)$.

7) $\operatorname{mcd}(ca,cb) = c\operatorname{mcd}(a,b)$.

Aquí todas las igualdades se entienden módulo la relación de equivalencia $\sim$. Las igualdades en 4)–7) se entienden de la siguiente manera: si uno de los mcd (resp. mcm) existe, entonces el otro también existe y son asociados.

Demostración. Las primeras dos propiedades son evidentes de la definición. Para 5) se puede observar que las propiedades que definen a $\operatorname{mcd}(\operatorname{mcd}(a,b),c)$ y $\operatorname{mcd}(a,\operatorname{mcd}(b,c))$ corresponden a la propiedad que define a $\operatorname{mcd}(a,b,c)$. Dejo los detalles como un ejercicio.

En la parte 6), basta notar que si $a = qb + r$, entonces

$$c \mid a,\ c \mid b \iff c \mid b,\ c \mid r.$$

En la parte 7), si $c = 0$, la afirmación es obvia y podemos asumir que $c \neq 0$. Sea $d = \operatorname{mcd}(a,b)$. Entonces, $cd \mid ca$ y $cd \mid cb$, así que $cd \mid \operatorname{mcd}(ca,cb)$.

Viceversa, puesto que $c \mid ca$ y $c \mid cb$, se tiene $c \mid \operatorname{mcd}(ca,cb)$. Escribamos $\operatorname{mcd}(ca,cb) = ce$ para algún $e \in A$. Esto significa que $ce \mid ca$ y $ce \mid cb$. Pero puesto que $c \neq 0$, esto implica que $e \mid a$ y $e \mid b$, así que $e \mid d$, y luego $ce = \operatorname{mcd}(ca,cb) \mid cd = c \cdot \operatorname{mcd}(a,b)$.

Entonces, hemos probado que $\operatorname{mcd}(ca,cb) \sim c \cdot \operatorname{mcd}(a,b)$. ■

3.7.7. Comentario (Algoritmo de Euclides). Las propiedades 1) y 6) de arriba implican que si A es un dominio euclidiano, entonces $\operatorname{mcd}(a,b)$ existe para cualesquiera $a,b \in A$. En efecto, esto es obvio cuando $b = 0$. Luego, asumiendo por inducción que el resultado es cierto para $\delta(b) < N$, para $\delta(b) = N$ podemos escribir

$$a = qb + r, \quad \text{donde } r = 0 \text{ o } \delta(r) < N,$$

y luego

$$\operatorname{mcd}(a,b) = \operatorname{mcd}(b,r).$$

3.7.8. Ejemplo. En el anillo de polinomios $\mathbb{Q}[X]$ calculemos $\operatorname{mcd}(f,g)$ para

$$f = X^4 + 4X^3 + 6X^2 + 5X + 2, \quad g = X^3 + 4X^2 + 4X + 3.$$

La división con resto nos da

$$f = X \cdot g + (2X^2 + 2X + 2).$$

Luego,

$$\operatorname{mcd}(f,g) = \operatorname{mcd}(X^3 + 4X^2 + 4X + 3,\, 2X^2 + 2X + 2).$$

Ahora

$$X^3 + 4X^2 + 4X + 3 = \left(\frac{1}{2}X + \frac{3}{2}\right) \cdot (2X^2 + 2X + 2) + 0.$$

Entonces,

$$\operatorname{mcd}(f,g) = \operatorname{mcd}(2X^2 + 2X + 2,\, 0) = 2X^2 + 2X + 2 \sim X^2 + X + 1.$$ ▲

3.7.9. Ejemplo. Calculemos $\operatorname{mcd}(13-9i,\, 8+6i)$ en el anillo de los enteros de Gauss $\mathbb{Z}[i]$. La división con resto nos da

$$13 - 9i = (1 - 2i) \cdot (8 + 6i) + (-7 + i).$$

Luego,

$$\operatorname{mcd}(13 - 9i,\, 8 + 6i) = \operatorname{mcd}(8 + 6i,\, -7 + i).$$

Ahora

$$8 + 6i = (-1 - i) \cdot (-7 + i) + 0.$$

Entonces,

$$\operatorname{mcd}(13 - 9i,\, 8 + 6i) = \operatorname{mcd}(8 + 6i,\, -7 + i) = -7 + i.$$ ▲

3.7.10. Proposición. *Si para $a, b \in A$ existe uno de los $\operatorname{mcd}(a,b)$ o $\operatorname{mcm}(a,b)$, entonces existe el otro y se cumple*

$$\operatorname{mcd}(a,b)\operatorname{mcm}(a,b) = ab.$$

Demostración. Supongamos por ejemplo que existe $d = \operatorname{mcd}(a,b)$. El caso de $a = b = 0$ es trivial y podemos descartarlo desde el principio. Entonces, se puede asumir que $d \neq 0$.

Tenemos en particular $d \mid a$ e $d \mid b$. Escribamos

$$a = d\,a', \quad b = d\,b'$$

para algunos $a', b' \in A$. Definamos

$$m := d\,a'\,b'.$$

Tenemos $dm = ab$ y nos gustaría probar que m satisface la propiedad de $\operatorname{mcm}(a,b)$. Primero,

$$m = a\,b' = a'\,b,$$

así que $a \mid m$ e $b \mid m$. Sea c otro elemento tal que $a \mid c$ y $b \mid c$. Necesitamos deducir que $m \mid c$. Notamos que

$$d = \operatorname{mcd}(a,b) = \operatorname{mcd}(d a', d b') = d \cdot \operatorname{mcd}(a', b'),$$

y luego

$$\operatorname{mcd}(a', b') = 1.$$

Pero en este caso

$$\operatorname{mcd}(ca', cb') = c\operatorname{mcd}(a', b') = c.$$

Luego, $m \mid ca'$ y $m \mid cb'$, y por lo tanto $m \mid c$. ∎

3.7.11. Proposición. *En todo dominio A tenemos*

1) *si $(a_1, \ldots, a_n) = (d)$, entonces $d = \operatorname{mcd}(a_1, \ldots, a_n)$;*

2) *si $(a_1) \cap \cdots \cap (a_n) = (m)$, entonces $m = \operatorname{mcm}(a_1, \ldots, a_n)$.*

Además, si A es un dominio de ideales principales, entonces mcd y mcm siempre existen. En este caso se tiene

1) *$(a_1, \ldots, a_n) = (d)$, donde $d = \operatorname{mcd}(a_1, \ldots, a_n)$;*

2) *$(a_1) \cap \cdots \cap (a_n) = (m)$, donde $m = \operatorname{mcm}(a_1, \ldots, a_n)$.*

Demostración. Vamos a ver el caso del mcd; el caso del mcm es parecido. Si $(a_1, \ldots, a_n) = (d)$, entonces $a_i \in (d)$ para todo $i = 1, \ldots, n$, lo que significa que $d \mid a_i$. Supongamos que $d' \mid a_i$ para todo i. Se tiene

$$c_1 a_1 + \cdots + c_n a_n = d$$

para algunos $c_1, \ldots, c_n \in A$, y luego $d' \mid d$.

Ahora si A es un dominio de ideales principales, entonces para cualesquiera $a_1, \ldots, a_n \in A$ existe $c \in A$ tal que $(a_1, \ldots, a_n) = (c)$. Pero acabamos de ver que $c = \operatorname{mcd}(a_1, \ldots, a_n)$. ∎

3.7.12. Comentario (♣). En general, en cualquier dominio donde existen los mcm, se tiene

$$(a_1) \cap \cdots \cap (a_n) = (m), \quad \text{donde } m = \operatorname{mcm}(a_1, \ldots, a_n).$$

Sin embargo, en general, la intersección de ideales principales no tiene por qué ser un ideal principal.

3.7.13. Corolario (Relación de Bézout). *Si A es un dominio de ideales principales, entonces para cualesquiera $a_1, \ldots, a_n \in A$ existen $c_1, \ldots, c_n \in A$ tales que*

$$c_1 a_1 + \cdots + c_n a_n = \operatorname{mcd}(a_1, \ldots, a_n).$$

Demostración. Se sigue de la igualdad $(a_1,\ldots,a_n) = (d)$, donde $d = \operatorname{mcd}(a_1,\ldots,a_n)$. ■

3.7.14. Corolario (Elementos coprimos). *En un dominio de ideales principales,* $\operatorname{mcd}(a_1,\ldots,a_n) = 1$ *si y solamente si* $(a_1,\ldots,a_n) = A$.

3.7.15. Ejemplo. Tenemos

1) $\operatorname{mcd}(2, 1+\sqrt{-3}) = 1$ en $\mathbb{Z}[\sqrt{-3}]$, pero $(2, 1+\sqrt{-3}) \neq \mathbb{Z}[\sqrt{-3}]$;

2) $\operatorname{mcd}(p, X) = 1$ en $\mathbb{Z}[X]$, pero $(p, X) \neq \mathbb{Z}[X]$;

3) $\operatorname{mcd}(X, Y) = 1$ en $k[X, Y]$, pero $(X, Y) \neq k[X, Y]$.

Esto sucede porque $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[X]$, $k[X, Y]$ no son dominios de ideales principales—véase los ejemplos 3.4.11, 3.4.12, 3.4.13. ▲

3.8 Dominios de factorización única

Todo número compuesto es medido por algún número primo.
Todo número o bien es número primo o es medido por algún número primo.

Euclides, “Elementos”, Libro VII

Cualquier número compuesto puede resolverse en factores primos de una manera única.

Gauss, “Disquisitiones Arithmeticae”, §16

3.8.1. Definición. Se dice que un dominio A es un **dominio de factorización única**[*] si

1) todo elemento no nulo $a \in A$ puede ser descompuesto como

$$a = u\, p_1 \cdots p_s,$$

donde $u \in A^\times$ es invertible y $p_1,\ldots,p_s \in A$ son irreducibles;

2) tales descomposiciones son únicas salvo el orden de los múltiplos y la relación de equivalencia $\sim$: si

$$a = u\, p_1 \cdots p_s = v\, q_1 \cdots q_t$$

donde $u, v \in A^\times$ y p_i, q_j son irreducibles, se tiene necesariamente $s = t$, y después de una permutación de los múltiplos, se cumple $p_i \sim q_i$ para todo $1 \le i \le s$.

3.8.2. Comentario. En la factorización $a = up_1 \cdots p_s$ *no se supone* que entre los p_i no hay repeticiones. Diferentes p_i y p_j pueden ser asociados.

3.8.3. Ejemplo. Todo cuerpo es trivialmente un dominio de factorización única: todo elemento no nulo es invertible y las condiciones de la definición de arriba son vacías. ▲

[*] También se usa el término “anillo factorial”.

3.8.4. Ejemplo. El anillo de los enteros $\mathbb{Z}$ es un dominio de factorización única. Por ejemplo, según la definición de arriba, las expresiones

$$-12 = -1\cdot 2\cdot 2\cdot 3 = 2\cdot (-3)\cdot 2$$

se consideran como la misma factorización de -12. En el anillo de los enteros de Gauss $\mathbb{Z}[i]$ podemos factorizar

$$-12 = (1+i)\,(1+i)\,(1+i)\,(1+i)\cdot 3 = (-1)\cdot (1+i)\,(1+i)\,(1-i)\,(1-i)\cdot 3.$$

De nuevo, estas dos factorizaciones se identifican: los elementos irreducibles $1+i$ e $1-i$ son asociados en $\mathbb{Z}[i]$. Más adelante veremos que $\mathbb{Z}[i]$ es también un dominio de factorización única.

En el anillo $\mathbb{Z}[\sqrt{-3}]$ tenemos

$$-12 = \sqrt{-3}\cdot\sqrt{-3}\cdot 2\cdot 2 = \sqrt{-3}\cdot\sqrt{-3}\cdot (1+\sqrt{-3})\,(1-\sqrt{-3}).$$

Estas dos factorizaciones son *diferentes*: los elementos irreducibles 2 y $1\pm\sqrt{-3}$ no son asociados entre sí. El anillo $\mathbb{Z}[\sqrt{-3}]$ no es un dominio de factorización única. ▲

La factorización única en $\mathbb{Z}$ se conoce como el **teorema fundamental de la aritmética** y a partir de los tiempos de Euclides se aceptaba como algo obvio, pero fue demostrado rigurosamente por primera vez por Gauss. Lo vamos a probar en esta sección mediante las implicaciones

$$\text{dom. euclidiano} \Longrightarrow \text{dom. de ideales principales} \Longrightarrow \text{dom. de factorización única}$$

La primera implicación es el contenido de 3.6.4, y nuestro objetivo será establecer la segunda.

3.8.5. Ejemplo (♣). Definamos un **polinomio trigonométrico real** como una suma formal finita

$$f(x) = a_0 + \sum_{1\le k\le n} (a_k \cos kx + b_k \operatorname{sen} kx),$$

donde $a_k, b_k \in \mathbb{R}$. Los productos se calculan mediante la distributividad y las fórmulas

$$\begin{aligned}
\cos(kx)\operatorname{sen}(\ell x) &= \frac{1}{2}\operatorname{sen}((k+\ell)\,x) - \frac{1}{2}\operatorname{sen}((k-\ell)\,x),\\
\cos(kx)\cos(\ell x) &= \frac{1}{2}\cos((k+\ell)\,x) + \frac{1}{2}\cos((k-\ell)\,x),\\
\operatorname{sen}(kx)\operatorname{sen}(\ell x) &= \frac{1}{2}\cos((k-\ell)\,x) - \frac{1}{2}\cos((k+\ell)\,x).
\end{aligned}$$

Digamos que el **grado** de f es el mayor k tal que $a_k \ne 0$ o $b_k \ne 0$.

1) Se puede comprobar que $\deg(fg) = \deg f + \deg g$.

2) Como consecuencia, si $f, g \ne 0$, tenemos $fg \ne 0$. Entonces, los polinomios trigonométricos forman un dominio. Denotémoslo por $Trig_{\mathbb{R}}$.

3) De la misma manera, la fórmula para el grado qemuestra que los elementos invertibles en $Trig_{\mathbb{R}}$ son los polinomios trigonométricos no nulos de grado 0.

4) Además, todo polinomio trigonométrico de grado 1 es irreducible en $Trig_{\mathbb{R}}$: si $\deg f = 1$, entonces $g \mid f$ implica que $\deg g = 1$ y $g \sim f$, o bien $\deg g = c \ne 0$ y $g \sim 1$.

Por lo que acabamos de decir, la identidad

$$(\operatorname{sen} x)^2 = (1+\cos x)\,(1-\cos x)$$

representa dos diferentes factorizaciones en elementos irreducibles, así que $Trig_{\mathbb{R}}$ no es un dominio de factorización única[*]. ▲

[*] Este curioso ejemplo viene del artículo [Tro1988].

Caracterización de dominios de factorización única

3.8.6. Lema. *En un dominio de factorización única todo elemento irreducible es primo.*

Demostración. Sea p un elemento irreducible. Ahora si $p \mid ab$, entonces tenemos $ab = pc$ para algún c. Consideremos las descomposiciones de a y b en elementos irreducibles:

$$a = u\,p_1 \cdots p_r, \quad b = v\,q_1 \cdots q_t.$$

De la identidad

$$u v\, p_1 \cdots p_r\, q_1 \cdots q_t = pc$$

podemos concluir que $p \sim p_i$ o $p \sim q_j$ para algún i, j. En particular, $p \mid a$ o $p \mid b$. ■

3.8.7. Ejemplo. Sea n un entero libre de cuadrados. En general, se sabe lo siguiente.

1) Los anillos $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{-2}]$ son dominios de factorización única; esto será probado más adelante.

2) Para todo $n < -3$ el anillo $\mathbb{Z}[\sqrt{n}]$ no es un dominio de factorización única: usando el mismo argumento de 3.2.6 es fácil ver que 2 es un elemento irreducible, pero no es primo.

3) Si $n < 0$ y $n \equiv 1 \pmod 4$, entonces entre los anillos $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ los únicos dominios de factorización única corresponden a

$$n = -3, -7, -11, -19, -43, -67, -163.$$

Este resultado está lejos de ser elemental y se conoce como el **teorema de Heegner–Stark** (no es tan difícil probar que para estos n se tiene factorización única, lo difícil es probar que para ningún otro $n < 0$, $n \equiv 1 \pmod 4$ en el anillo $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ hay factorización única).

4) Si $n > 1$ y $n \equiv 1 \pmod 4$, entonces $\mathbb{Z}[\sqrt{n}]$ no es un dominio de factorización única: de nuevo, 2 es irreducible, pero no es primo, como vimos en 3.6.9. En este caso el anillo más grande $\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$ puede o no puede ser un dominio de factorización única.

5) Si $n > 1$ y $n \equiv 2, 3 \pmod 4$, tampoco se sabe cuándo en general $\mathbb{Z}[\sqrt{n}]$ tiene factorización única.

La situación completa para $n > 1$ no se conoce, aunque para cada n fijo se puede hacer un cálculo[*] que dirá si el anillo correspondiente tiene factorización única (y en este caso esto equivale a ser un dominio de ideales principales[**]). He aquí una pequeña tabla donde están subrayados los anillos que no son dominios de factorización única.

$\mathbb{Z}[\sqrt{2}]$	$\mathbb{Z}[\sqrt{3}]$	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$\mathbb{Z}[\sqrt{6}]$	$\mathbb{Z}[\sqrt{7}]$	$\mathbb{Z}[\sqrt{10}]$	$\mathbb{Z}[\sqrt{11}]$
$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	$\mathbb{Z}[\sqrt{14}]$	$\mathbb{Z}[\sqrt{15}]$	$\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$	$\mathbb{Z}[\sqrt{19}]$	$\mathbb{Z}[\frac{1+\sqrt{21}}{2}]$	$\mathbb{Z}[\sqrt{22}]$
$\mathbb{Z}[\sqrt{23}]$	$\mathbb{Z}[\sqrt{26}]$	$\mathbb{Z}[\frac{1+\sqrt{29}}{2}]$	$\mathbb{Z}[\sqrt{30}]$	$\mathbb{Z}[\sqrt{31}]$	$\mathbb{Z}[\frac{1+\sqrt{33}}{2}]$	$\mathbb{Z}[\sqrt{34}]$
$\mathbb{Z}[\sqrt{35}]$	$\mathbb{Z}[\frac{1+\sqrt{37}}{2}]$	$\mathbb{Z}[\sqrt{38}]$	$\mathbb{Z}[\sqrt{39}]$	$\mathbb{Z}[\frac{1+\sqrt{41}}{2}]$	$\mathbb{Z}[\sqrt{42}]$	$\mathbb{Z}[\sqrt{43}]$
$\mathbb{Z}[\sqrt{46}]$	$\mathbb{Z}[\sqrt{47}]$	$\mathbb{Z}[\sqrt{51}]$	$\mathbb{Z}[\frac{1+\sqrt{53}}{2}]$	$\mathbb{Z}[\sqrt{55}]$	$\mathbb{Z}[\frac{1+\sqrt{57}}{2}]$	$\mathbb{Z}[\sqrt{58}]$
$\mathbb{Z}[\sqrt{59}]$	$\mathbb{Z}[\frac{1+\sqrt{61}}{2}]$	$\mathbb{Z}[\sqrt{62}]$	$\mathbb{Z}[\frac{1+\sqrt{65}}{2}]$	$\mathbb{Z}[\sqrt{66}]$	$\mathbb{Z}[\sqrt{67}]$	$\mathbb{Z}[\frac{1+\sqrt{69}}{2}]$
$\mathbb{Z}[\sqrt{70}]$	$\mathbb{Z}[\sqrt{71}]$	$\mathbb{Z}[\frac{1+\sqrt{73}}{2}]$	$\mathbb{Z}[\sqrt{74}]$	$\mathbb{Z}[\frac{1+\sqrt{77}}{2}]$	$\mathbb{Z}[\sqrt{78}]$	$\mathbb{Z}[\sqrt{79}]$
$\mathbb{Z}[\sqrt{82}]$	$\mathbb{Z}[\sqrt{83}]$	$\mathbb{Z}[\frac{1+\sqrt{85}}{2}]$	$\mathbb{Z}[\sqrt{86}]$	$\mathbb{Z}[\sqrt{87}]$	$\mathbb{Z}[\frac{1+\sqrt{89}}{2}]$	$\mathbb{Z}[\sqrt{91}]$
$\mathbb{Z}[\frac{1+\sqrt{93}}{2}]$	$\mathbb{Z}[\sqrt{94}]$	$\mathbb{Z}[\sqrt{95}]$	$\mathbb{Z}[\frac{1+\sqrt{97}}{2}]$	$\mathbb{Z}[\frac{1+\sqrt{101}}{2}]$	$\mathbb{Z}[\sqrt{102}]$	$\mathbb{Z}[\sqrt{103}]$

Por ejemplo, en el anillo $\mathbb{Z}[\sqrt{10}]$ el elemento 2 es irreducible: si $\alpha \mid 2$, entonces hay tres casos:

[*] Cálculo del grupo de clases. Por ejemplo, el el programa PARI/GP el comando `bnfinit(x^2-n).no` devuelve 1 si hay factorización única y un número > 1 si no hay (en algún sentido este número mide qué tan lejos estamos de tener factorización única).

[**] Esta es una propiedad general del **anillo de enteros** de un **cuerpo de números**.

- $N(\alpha) = \pm 1$, y luego $\alpha \in \mathbb{Z}[\sqrt{10}]^\times$;
- $N(\alpha) = \pm 4$, y luego $\alpha \sim 2$;
- $N(\alpha) = \pm 2$. Este caso en realidad no ocurre: si $a^2 - 10\,b^2 = \pm 2$, entonces $a^2 \equiv \pm 2 \pmod 5$, pero los cuadrados módulo 5 son 0, 1, y 4.

Sin embargo, 2 no es primo en $\mathbb{Z}[\sqrt{10}]$: se tiene $2 \mid 2\cdot 5 = (\sqrt{10})^2$, pero, $2 \nmid \sqrt{10}$. Esto demuestra que $\mathbb{Z}[\sqrt{10}]$ no es un dominio de factorización única.

Según una famosa conjetura de Gauss, hay un número infinito de $n > 0$ tales que el anillo correspondiente

$$\begin{cases} \mathbb{Z}[\sqrt{n}], & \text{si } n \equiv 2,3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right], & \text{si } n \equiv 1 \pmod 4 \end{cases}$$

es un dominio de factorización única. Para más información sobre el tema, consulte el libro [Mak2013]. ▲

El descubrimiento de anillos que no son dominios de factorización única fue uno de los sucesos más importantes en la matemática del siglo XIX.

3.8.8. Definición. Sea A un anillo conmutativo. Se dice que una **cadena ascendente de ideales**

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots \subseteq A$$

se estabiliza si existe n tal que $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$.

3.8.9. Lema. *Sean A es un dominio de factorización única y $a, b \in A$ dos elementos no nulos. Consideremos las factorizaciones en elementos irreducibles*

$$a = u p_1 \cdots p_r, \quad b = v q_1 \cdots q_s.$$

Si $b \mid a$, pero $a \nmid b$, entonces $r > s$.

Demostración. Escribamos

$$a = bc$$

y sea

$$c = w\, q_{s+1} \cdots q_t$$

la factorización de c. Luego,

$$u p_1 \cdots p_r = v w\, q_1 \cdots q_s\, q_{s+1} \cdots q_t.$$

Tenemos entonces $r = t \ge s$. Pero el caso de $t = s$ está excluido: esto implicaría que $a \sim b$. ■

3.8.10. Lema. *Si A es un dominio de factorización única, entonces toda cadena acendente de ideales principales en A se estabiliza.*

Demostración. Por el lema anterior, si tenemos

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots,$$

y a tiene n factores irreducibles, entonces a_1 tiene $\le n-1$ factores irreducibles, a_2 tiene $\le n-2$ factores irreducibles, etcétera. Si continuamos esta cadena, llegaremos a un elemento que no tiene factores irreducibles y por ende es invertible y el ideal correspondiente coincide con todo A. ■

3.8.11. Lema. *Sea A un dominio donde toda cadena acendente de ideales principales se estabiliza. Entonces,*

1) *todo elemento no nulo y no invertible $a \in A$ es divisible por un elemento irreducible;*

2) *todo elemento $a \ne 0$ posee una factorización en irreducibles; es decir, puede ser escrito como*

$$a = u\, p_1 \cdots p_n$$

donde $u \in A^\times$ y $p_1, \ldots, p_n \in A$ son elementos irreducibles.

Demostración. En la parte 1), se $a \in A$ un elemento tal que $a \ne 0$ y $a \notin A^\times$. Si a es irreducible, no hay nada que probar. Si a es reducible, entonces podemos escribir $a = a_1\, b_1$ donde a_1 es un divisor no trivial: $a_1 \notin A^\times$ y $a_1 \not\sim a$. Si a_1 es irreducible, la prueba está terminada. En el caso contrario, podemos escribir $a_1 = a_2\, b_2$ donde $a_2 \notin A^\times$ y $a_2 \not\sim a_1$. Continuando de esta manera, se obtienen elementos $a_1, a_2, a_3, \ldots$ tales que

$$a_1 \mid a, \quad a_2 \mid a_1, \quad a_3 \mid a_2, \quad a_4 \mid a_3, \quad \ldots,$$

lo que nos da una cadena ascendente de ideales principales

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq (a_3) \subseteq (a_4) \subseteq \cdots \subset A.$$

Pero por nuestra hipótesis sobre A, en algún momento la cadena se estabiliza, lo que significa que $(a_n) = (a_{n+1})$ para n suficientemente grande; es decir, $a_n \sim a_{n+1}$. Podemos concluir que el proceso siempre termina y nos da un factor irreducible de a.

La parte 2) se demuestra de manera similar. Si para $a \ne 0$ se tiene $a \in A^\times$ o a es irreducible, no hay que probar nada. En el caso contrario, podemos escribir $a = p_1\, a_1$ donde p_1 es un factor irreducible cuya existencia fue probada en la parte 1). Luego, si $a_1 \in A^\times$ o a_1 es irreducible, la prueba está terminada. En el caso contrario, escribamos $a_1 = p_2\, a_2$, donde p_2 es irreducible, etcétera. Notamos que

$$a_1 \mid a, \quad a_2 \mid a_1, \quad a_3 \mid a_2, \quad \ldots$$

lo que corresponde a una cadena de ideales principales

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq (a_4) \subsetneq \cdots$$

En esta cadena $a_n \not\sim a_{n+1}$: se tiene $a_n = p_n\, a_{n+1}$, así que $a_n \mid a_{n+1}$ implicaría $p_n \sim 1$ que no es el caso. Pero toda cadena de ideales principales en A se estabiliza por nuestra hipótesis, así que la construcción debe terminar por algún $a_n \in A^\times$ o a_n irreducible. Esto nos da una descomposición

$$a = p_1 a_1 = p_1 p_2 a_2 = \cdots = p_1 \cdots p_n a_n. \qquad \blacksquare$$

Para probar que algo es un dominio de factorización única nos servirá la siguiente caracterización.

3.8.12. Teorema. *Sea A un dominio. Las siguientes condiciones son equivalentes.*

1) *A es un dominio de factorización única;*

2) *En A se cumple*

   a) *toda cadena ascendente de ideales principales se estabiliza*[*],

   b) *todo elemento irreducible es primo.*

Demostración. La implicación 1) ⇒ 2) fue probada en 3.8.6 y 3.8.10.

Para la implicación 2) ⇒ 1), notamos que hemos probado en 3.8.11 que la condición a) implica existencia de factorizaciones, y falta solo probar su unicidad. Consideremos entonces dos factorizaciones

$$a = u\, p_1 \cdots p_s = v\, q_1 \cdots q_t$$

[*] Para los especialistas: esta condición es menos fuerte que estabilización de cualquier cadena de ideales. Por ejemplo, en el anillo $k[X_1, X_2, X_3, \ldots]$ de polinomios en un número infinito de variables la cadena $(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \cdots$ no se estabiliza, pero toda cadena de ideales *principales* $(f_1) \subseteq (f_2) \subseteq (f_3) \subseteq \cdots$ sí se estabiliza. Este anillo es un dominio de factorización única.

Sin pérdida de generalidad, asumamos que $s \le t$ y procedamos por inducción sobre s.

Si $s = 0$, no hay que probar nada: $u = v\,q_1 \cdots q_t$ para $t > 0$ implica que $q_1 \cdots q_t = uv^{-1}$ es invertible, pero luego todo q_i es invertible, lo que no es el caso, puesto que los q_i son primos. Entonces, $t = 0$.

Asumamos que el resultado es cierto para $s-1$ factores. Consideremos la igualdad

$$u\,p_1 \cdots p_s = v\,q_1 \cdots q_t.$$

Dado que p_s es primo y $p_s \mid v\,q_1 \cdots q_t$, tenemos $p_s \mid q_i$ para algún $1 \le i \le t$ (notamos que p_s, siendo primo, no puede dividir al elemento invertible v). Después de una renumeración de los múltiplos, podemos asumir que $p_s \mid q_t$. Pero q_t es también primo, así que $p_s \sim q_t$; es decir, $p_s = w\,q_t$ para algún $w \in A^\times$. Ahora en la identidad

$$u\,p_1 \cdots p_{s-1}\,(w\,q_t) = v\,q_1 \cdots q_{t-1}\,q_t$$

podemos cancelar q_t y obtener

$$uw\,p_1 \cdots p_{s-1} = v\,q_1 \cdots q_{t-1}.$$

Por la hipótesis de inducción, se tiene $s-1 = t-1$ y $p_i \sim q_i$ para todo $1 \le i \le s-1$, después de una permutación de los múltiplos. ■

Note que en nuestros ejemplos de anillos que no son dominios de factorización única, la condición que falla es b).

Factorización única en dominios de ideales principales

3.8.13. Lema. *Si A es un dominio de ideales principales, entonces toda cadena ascendente de ideales en A se estabiliza.*

Demostración. Para una cadena de ideales

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots \subseteq A$$

la unión

$$\mathfrak{a} := \bigcup_{n\ge 1} \mathfrak{a}_n$$

es también un ideal, pero por la hipótesis sobre A es principal: se tiene $\mathfrak{a} = (x)$ para algún $x \in A$. Luego, $x \in \mathfrak{a}_n$ para algún n y

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots = \mathfrak{a}.$$ ■

3.8.14. Corolario. *Todo dominio de ideales principales es un dominio de factorización única.*

Demostración. Las condiciones a) y b) del teorema fueron comprobadas para dominios de ideales principales en 3.8.13 y 3.6.6. ■

3.8.15. Corolario. *Todo dominio euclidiano es un dominio de factorización única.*

3.8.16. Corolario. *Para todo cuerpo k el anillo de polinomios $k[X]$ es un dominio de factorización única.*

3.8.17. Comentario. Para algoritmos de factorización en los anillos de polinomios $\mathbb{F}_p[X]$ y $\mathbb{Q}[X]$, véase por ejemplo el libro [Coh1993].

3.8.18. Comentario. Hay muchos ejemplos de dominios de factorización única que no son dominios de ideales principales, como el anillo de polinomios con coeficientes enteros $\mathbb{Z}[X]$ (donde el ideal $(2, X)$ no es principal) o el anillo de polinomios en n variables $k[X_1, \ldots, X_n]$ (donde el ideal $(X_1, \ldots, X_n)$ no es principal). Vamos a probar la factorización única en estos anillos más adelante en el capítulo 5.

3.9 Primos de Gauss

Ya sabemos que los enteros de Gauss $\mathbb{Z}[i]$ forman un dominio euclidiano, y entonces un dominio de factorización única. Ahora vamos a describir los elementos primos (irreducibles) en $\mathbb{Z}[i]$. Para encontrarlos, hay que factorizar los enteros primos $p = 2, 3, 5, 7, 11, \ldots$ en $\mathbb{Z}[i]$.

3.9.1. Observación. *Si para un elemento $\pi = a + bi \in \mathbb{Z}[i]$ la norma $N(\pi) = a^2 + b^2 = p$ es un número entero primo, entonces π es un elemento primo en $\mathbb{Z}[i]$.*

Demostración. Supongamos que $\pi = xy$. Luego, $N(\pi) = N(x)\,N(y)$. Pero ya que $N(\pi)$ es primo, tenemos necesariamente $N(x) = 1$ o $N(y) = 1$. En el primer caso $\pi \sim y$, mientras que en el segundo caso $\pi \sim x$. ■

3.9.2. Ejemplo. Los números $1 \pm i$, $1 \pm 2i$, $2 \pm 3i$ son primos en $\mathbb{Z}[i]$. ▲

3.9.3. Observación. *Sea π un primo en $\mathbb{Z}[i]$. Entonces, $\pi \mid p$ donde p es un número entero primo.*

Demostración. Tenemos $\pi \mid N(\pi) := \pi\overline{\pi}$. Luego, $N(\pi) > 1$, ya que π no es nulo y no invertible, y $N(\pi) = p_1 \cdots p_n$, así que $\pi \mid p_j$ para algún j. ■

Entonces, para obtener los primos en $\mathbb{Z}[i]$, hay que factorizar los primos enteros $2, 3, 5, 7, 11, \ldots$

3.9.4. Ejemplo. Tenemos las siguientes factorizaciones en $\mathbb{Z}[i]$:

$$\begin{aligned} 2 &= -i \cdot (1+i)^2, \\ 3 &= 3, \\ 5 &= (1+2i)\,(1-2i), \\ 7 &= 7, \\ 11 &= 11, \\ 13 &= (2+3i)\,(2-3i), \\ &\cdots \end{aligned}$$

▲

3.9.5. Comentario (♣). Notamos que los primos enteros como $p = 5$ y 13 se vuelven productos de dos diferentes primos en $\mathbb{Z}[i]$. Se dice que estos p **se escinden** en $\mathbb{Z}[i]$. Por otro lado, los primos enteros como $p = 3, 7, 11$ permanecen primos en $\mathbb{Z}[i]$, y se dice que estos p son **inertes**. El primo 2 es excepcional: en su factorización en $\mathbb{Z}[i]$ aparece el cuadrado $(1+i)^2$, y por esto se dice que 2 **se ramifica**.

3.9.6. Teorema (≈ Teorema de los dos cuadrados de Fermat). *Para un primo $p \in \mathbb{Z}$ las siguientes condiciones son equivalentes:*

1) *p es compuesto en $\mathbb{Z}[i]$,*

2) *p puede ser escrito como una suma de dos cuadrados $a^2 + b^2$,*

3) *$p = 2$ o $p \equiv 1 \pmod 4$.*

En este caso p es un producto de dos primos conjugados en $\mathbb{Z}[i]$.

Antes de probar el teorema, necesitamos un lema.

3.9.7. Lema (Lagrange). *Si p es un primo entero y $p \equiv 1 \pmod 4$, entonces $p \mid (a^2+1)$ para algún $a \in \mathbb{Z}$.*

Demostración. La primera ley suplementaria de reciprocidad cuadrática* nos dice que -1 es un cuadrado módulo un primo impar p si y solo si $p \equiv 1 \pmod 4$:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{4}}.$$

Para -1 ser un cuadrado módulo p significa que $a^2 + 1 \equiv 0 \pmod p$ para algún a. ■

*Véanse por ejemplo mis apuntes http://cadadr.org/san-salvador/2018-cp-tne/reciprocidad-cuadratica.pdf

3.9.8. Ejemplo. Tenemos

$$\begin{aligned} 5 &= 2^2+1, \\ 13 \mid 26 &= 5^2+1, \\ 17 &= 4^2+1, \\ 29 \mid 145 &= 12^2+1, \\ 37 &= 6^2+1, \\ 41 \mid 82 &= 9^2+1. \end{aligned}$$

▲

Demostración del teorema. Para ver que 1) implica 2), notamos que si $p = xy$, donde x e y no son invertibles, entonces $p^2 = N(x)\,N(y)$, así que $N(x) = N(y) = p$ y en particular x e y son primos. Si $x = a + bi$, entonces

$$p = N(x) = x\overline{x} = a^2 + b^2.$$

Para ver que 2) implica 3), notamos que si $p = a^2 + b^2$, entonces, puesto que los cuadrados módulo 4 son 0 y 1, tenemos necesariamente $p = 2$ o $p \equiv 1 \pmod 4$.

En fin, para la implicación entre 3) y 1), notamos que si $p \equiv 1 \pmod 4$, entonces por el lema de Lagrange, $p \mid (a^2+1)$ para algún $a \in \mathbb{Z}$. Luego,

$$p \mid (a-i)\,(a+i),$$

aunque $p \nmid (a \pm i)$, así que p es compuesto en $\mathbb{Z}[i]$. El caso de $p = 2$ es excepcional:

$$2 = (1+i)\,(1-i).$$

■

3.9.9. Comentario (♣). Para otra prueba del teorema de arriba y también el teorema de los *cuatro* cuadrados, véanse mis apuntes

http://cadadr.org/san-salvador/2018-03-cuadrados/cuadrados.pdf

Podemos concluir que los primos en $\mathbb{Z}[i]$ son de dos tipos:

1) primos enteros p tales que $p \equiv 3 \pmod 4$;

2) elementos $\pi \in \mathbb{Z}[i]$ tales que la norma $N(\pi)$ es un primo entero p y $p = 2$ o $p \equiv 1 \pmod 4$.

Tenemos la siguiente lista de los primos en $\mathbb{Z}[i]$, excluyendo los primos asociados:

$$1+i, \quad 3, \quad 2 \pm i, \quad 7, \quad 11, \quad 2 \pm 3i, \quad 1 \pm 4i, \quad 19, \quad \ldots$$

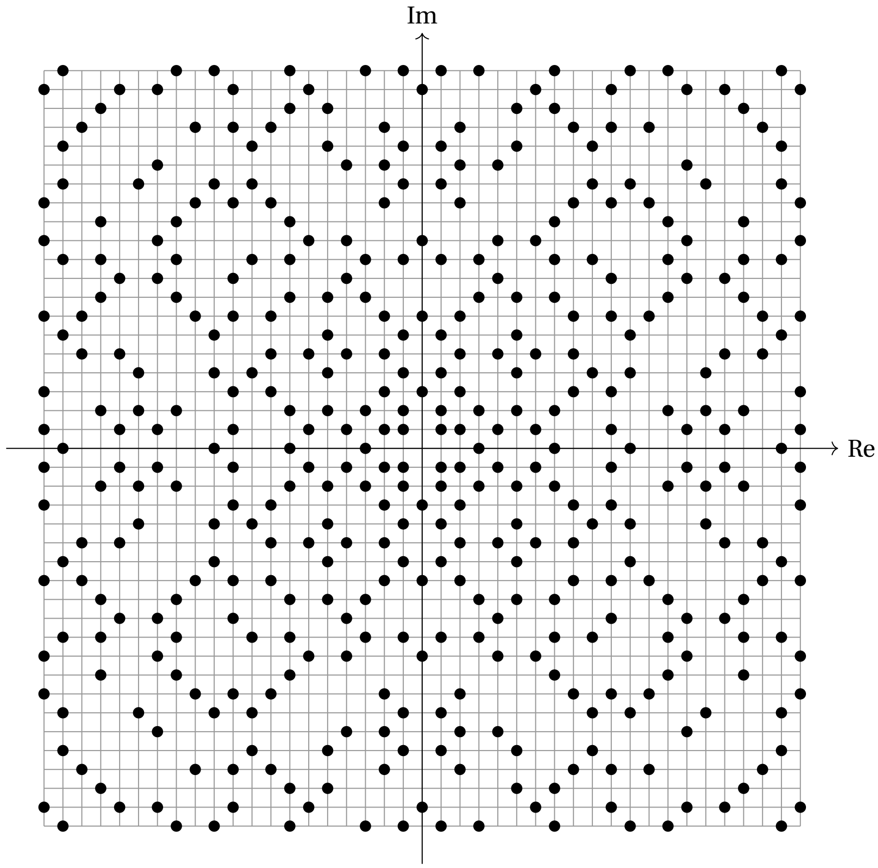

Figura 3.7: Los primos de Gauss en el plano complejo

3.10 Valuaciones p-ádicas

Sea A un dominio de factorización única. Todo elemento no nulo $a \in A$ está definido, salvo un múltiplo invertible, por sus factores primos. Es conveniente juntar factores repetidos y escribir a como $u\,p_1^{k_1} \cdots p_n^{k_n}$ donde los p_i son primos no asociados entre sí (es decir, $p_i \nsim p_j$ para $i \ne j$). El exponente k de un factor primo p se llama la **valuación p-ádica** de a.

3.10.1. Definición. Sea $p \in A$ un elemento primo. Para un elemento $a \in A$, $a \ne 0$ definamos

$$v_p(a) := \text{máx}\{k \mid p^k \mid a\}$$

y para el elemento nulo pongamos

$$v_p(0) := \infty.$$

El número $v_p(a)$ se llama la **valuación p-ádica** de a.

En otras palabras, para un elemento no nulo se tiene $v_p(a) = n$ precisamente cuando se puede escribir $a = p^n\,a'$, donde $p \nmid a'$. La factorización única en A significa que para todo $a \ne 0$ se cumple

$$a \sim \prod_p p^{v_p(a)},$$

donde el producto es sobre las clases de equivalencia de los elementos primos módulo la relación $\sim$. Notamos que en realidad este producto es finito, puesto que $v_p(a) = 0$ para todo p, salvo un número finito.

3.10.2. Ejemplo. Tenemos

$$v_2(60) = 2, \quad v_3(60) = 1, \quad v_5(60) = 1$$

y $v_p(60) = 0$ para $p \ne 2, 3, 5$. ▲

3.10.3. Ejemplo. En el anillo $\mathbb{Z}[i]$ tenemos

$$60 = 2^2 \cdot 3 \cdot 5 = -(1+i)^4 \cdot 3 \cdot (1+2i) \cdot (1-2i),$$

así que

$$v_{1+i}(60) = 4, \quad v_3(60) = 1, \quad v_{1+2i}(60) = 1, \quad v_{1-2i}(60) = 1$$

y $v_\pi(60) = 0$ para otros primos. ▲

3.10.4. Proposición. *La valuación p-ádica satisface las siguientes propiedades.*

V1) $v_p(a) = \infty$ *si y solamente si* $a = 0$.

V2) $v_p(ab) = v_p(a) + v_p(b)$.

V3) $v_p(a+b) \ge \text{mín}\{v_p(a), v_p(b)\}$.

Demostración. La parte V1) hace parte de la definición. Para la parte V2), si $a = 0$ o $b = 0$, la igualdad es evidente. Ahora si a y b no son nulos y $v_p(a) = m$ y $v_p(b) = n$, esto significa que

$$a = p^m\,a', \quad b = p^n\,b',$$

donde $p \nmid a'$ y $p \nmid b'$. Luego,

$$ab = p^{m+n}\,a'b',$$

donde $p \nmid a'b'$, así que $v_p(ab) = m+n$. De la misma manera, la parte V3) es evidente cuando $a = 0$ o $b = 0$. Para a e b no nulos, de nuevo podemos asumir que $v_p(a) = m$ y $v_p(b) = n$, donde sin pérdida de generalidad $m \le n$. Luego,

$$a + b = p^m\,a' + p^n\,b' = p^m\,(a' + p^{n-m}\,b'),$$

entonces $p^m \mid (a+b)$ y por ende $v_p(a+b) \ge m$. ■

3.10.5. Observación. *Si $u \in A^\times$, entonces $v_p(u) = 0$ y $v_p(ua) = a$ para todo $a \in A$. En particular, $v_p(-a) = v_p(a)$ para todo $a \in A$.*

Demostración. Estas propiedades se siguen de la definición de v_p, pero podemos deducirlas de las propiedades V1), V2), V3). Primero, tenemos

$$v_p(1) = v_p(1 \cdot 1) = v_p(1) + v_p(1),$$

así que $v_p(1) = 0$. Luego, si $u \in A^\times$, entonces

$$v_p(u) + v_p(u^{-1}) = v_p(uu^{-1}) = v_p(1) = 0,$$

de donde $v_p(u) = 0$, puesto que $v_p(u), v_p(u) \ge 0$. En fin,

$$v_p(ua) = v_p(u) + v_p(a) = 0 + v_p(a) = v_p(a).$$ ■

Nos conviene extender las valuaciones p-ádicas al cuerpo de fracciones de A.

3.10.6. Definición. Sean A un dominio de factorización única, $p \in A$ un elemento primo y $\operatorname{Frac} A$ el cuerpo de fracciones de A (véase el capítulo 1). Para $\frac{a}{b} \in \operatorname{Frac} A$ definamos la valuación p-ádica sobre $\operatorname{Frac} A$ mediante

$$v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b).$$

Hay que verificar que esta definición tiene sentido: si $\frac{a}{b} = \frac{a'}{b'}$, entonces $ab' = a'b$. Luego,

$$v_p(a) + v_p(b') = v_p(a') + v_p(b);$$

es decir,

$$v_p(a) - v_p(b) = v_p(a') - v_p(b').$$

Esto significa que

$$v_p\left(\frac{a}{b}\right) = v_p\left(\frac{a'}{b'}\right).$$

Notamos que para toda fracción no nula se tiene

$$\frac{a}{b} = \prod_p p^{v_p(a/b)},$$

donde el producto se toma sobre todos los primos en A salvo la relación $\sim$, y la igualdad se entiende salvo un múltiplo $u \in A^\times$.

3.10.7. Ejemplo. Para $a = \frac{12}{34} = \frac{2^2 \cdot 3}{2 \cdot 17}$ se tiene

$$v_2(a) = 1, \quad v_3(a) = 1, \quad v_{17}(a) = -1,$$

y $v_p(a) = 0$ para otros p. ▲

3.10.8. Observación. *La valuación p-ádica sobre* $\operatorname{Frac} A$ *satisface las mismas propiedades:*

V1) $v_p\left(\frac{a}{b}\right) = \infty$ *si y solamente si* $\frac{a}{b} = \frac{0}{1}$.

V2) $v_p\left(\frac{a}{b}\frac{c}{d}\right) = v_p\left(\frac{a}{b}\right) + v_p\left(\frac{c}{d}\right)$.

V3) $v_p\left(\frac{a}{b} + \frac{c}{d}\right) \ge \min\left\{v_p\left(\frac{a}{b}\right), v_p\left(\frac{c}{d}\right)\right\}$. □

La desigualdad $v_p(a+b) \ge \min\{v_p(a), v_p(b)\}$ puede ser mejorada de la siguiente manera.

3.10.9. Observación. *Para cualesquiera $a, b \in A$, si $v_p(a) \ne v_p(b)$, entonces*

$$v_p(a+b) = \text{mín}\{v_p(a), v_p(b)\}.$$

De la misma manera, para cualesquiera $\frac{a}{b}, \frac{c}{d} \in \operatorname{Frac} A$, si $v_p\left(\frac{a}{b}\right) \ne v_p\left(\frac{c}{d}\right)$, entonces

$$v_p\left(\frac{a}{b} + \frac{c}{d}\right) = \text{mín}\left\{v_p\left(\frac{a}{b}\right), v_p\left(\frac{c}{d}\right)\right\}.$$

Demostración. La propiedad en cuestión sigue formalmente de las propiedades V1), V2), V3). Asumamos que se cumple la desigualdad estricta

$$v_p(a+b) > \text{mín}\{v_p(a), v_p(b)\}.$$

Entonces, tenemos

$$v_p(a) = v_p(a+b-b) \ge \text{mín}\{v_p(a+b), v_p(b)\} = v_p(b)$$

y de la misma manera

$$v_p(b) = v_p(a+b-a) \ge \text{mín}\{v_p(a+b), v_p(a)\} = v_p(a).$$

■

3.10.10. Comentario. Por inducción, de la última observación se sigue que si $a = a_1 + \cdots + a_n$ y existe $i = 1, \ldots, n$ tal que $v_p(a_i) < v_p(a_j)$ para $i \ne j$, entonces $v_p(a) = v_p(a_i)$.

3.10.11. Observación. *Recordemos que A se identifica con el subanillo de $\operatorname{Frac} A$ formado por las fracciones $\frac{a}{1}$, donde $a \in A$. Se tiene*

$$A = \left\{\frac{a}{b} \in \operatorname{Frac} A \;\middle|\; v_p\left(\frac{a}{b}\right) \ge 0 \textit{ para todo primo } p\right\},$$

donde se consideran todos los primos en A salvo la relación $\sim$ y

$$A^\times = \left\{\frac{a}{b} \in \operatorname{Frac} A \;\middle|\; v_p\left(\frac{a}{b}\right) = 0 \textit{ para todo primo } p\right\}.$$

Demostración. Tenemos $\frac{a}{b} = \prod_p p^{v_p(a/b)}$ salvo un múltiplo $u \in A^\times$, así que si $v_p\left(\frac{a}{b}\right) \ge 0$ para todo p, se tiene $\frac{a}{b} \in A$ (es decir, $\frac{a}{b} = \frac{a'}{1}$ para algún $a' \in A$). ■

3.10.12. Observación. *En todo dominio de factorización única existen los mcm y mcd y estos pueden ser calculados como*

$$\operatorname{mcd}(a,b) = \prod_p p^{\text{mín}\{v_p(a), v_p(b)\}}, \quad \operatorname{mcm}(a,b) = \prod_p p^{\text{máx}\{v_p(a), v_p(b)\}}.$$

□

3.10.13. Comentario. Las fórmulas de la última proposición no se usan en cálculos prácticos: normalmente es mucho más fácil calcular el $\operatorname{mcd}(a,b)$ y $\operatorname{mcm}(a,b)$ que obtener las factorizaciones de a y b (es decir, calcular todas las valuaciones $v_p(a)$ y $v_p(b)$).

3.11 Ejercicios

Ejercicio 3.1. Sea p un número primo. Para el anillo $\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ p \nmid b \right\}$ definamos

$$v_p\left(\frac{a}{b}\right) := \text{máx}\{k \mid p^k \mid a\}, \quad v_p(0) := +\infty.$$

1) Demuestre que para cualesquiera $x, y \in \mathbb{Z}_{(p)}$ se cumple

$$v_p(xy) = v_p(x) + v_p(y).$$

2) Demuestre que todo elemento no nulo $x \in \mathbb{Z}_{(p)}$ puede ser escrito como up^n donde $u \in \mathbb{Z}_{(p)}^\times$ y $n = v_p(x)$.

3) Demuestre que todo elemento irreducible en $\mathbb{Z}_{(p)}$ está asociado con p.

Ejercicio 3.2. Sea k un cuerpo. Consideremos el anillo de las series de potencias $k[[X]]$. Definamos para $f = \sum_{i\ge 0} a_i X^i \in k[[X]]$

$$v(f) := \text{mín}\{i \mid a_i \ne 0\}, \quad v(0) := +\infty$$

(recuerde el primer ejercicio de la hoja 4).

1) Demuestre que toda serie no nula $f \in k[[X]]$ puede ser escrita como $g X^n$ donde $g \in k[[X]]^\times$ y $n = v(f)$.

2) Demuestre que todo elemento irreducible en $k[[X]]$ está asociado con X.

Ejercicio 3.3. Sea $n \le -3$ un entero negativo libre de cuadrados. Usando la norma, demuestre que los números 2 y $1 \pm \sqrt{n}$ son irreducibles en el anillo $\mathbb{Z}[\sqrt{n}]$

Ejercicio 3.4. Sea $n \le -3$ un entero negativo libre de cuadrados. Demuestre que 2 no es primo en $\mathbb{Z}[\sqrt{n}]$. *Sugerencia: note que si n es par, entonces $2 \mid (\sqrt{n})^2$, y si n es impar, entonces $2 \mid (1+\sqrt{n})(1-\sqrt{n})$.*

Ejercicio 3.5. Sea $n \ne 1$ un entero libre de cuadrados. Consideremos el anillo $\mathbb{Z}[\sqrt{n}]$ con la norma

$$N(a + b\sqrt{n}) := a^2 - nb^2 \in \mathbb{Z}.$$

Demuestre que si $N(\alpha) = \pm 2, \pm 3, \pm 5, \pm 7, \ldots$ es un número primo, entonces α es irreducible en $\mathbb{Z}[\sqrt{n}]$.

Ejercicio 3.6. Determine cuáles de los números

$$3 + 2\sqrt{5}, \quad 4 + 2\sqrt{5}, \quad 2 - \sqrt{5}, \quad 7 + 3\sqrt{5}$$

son irreducibles en el anillo $\mathbb{Z}[\sqrt{5}]$.

Ejercicio 3.7. Demuestre que en el anillo $\mathbb{Z}[\sqrt{3}]$ no existe un elemento invertible α tal que $1 < \alpha < 2 + \sqrt{3}$. Encuentre los elementos invertibles en $\mathbb{Z}[\sqrt{3}]$.

Ejercicio 3.8. Sea k un cuerpo. Demuestre que un polinomio f es irreducible en el anillo $k[X]$ si y solo si f no es constante y f no se puede escribir como $f = gh$ con $\deg g, \deg h < \deg f$.

Ejercicio 3.9. Encuentre los polinomios irreducibles en el anillo $\mathbb{C}[X]$.

Ejercicio 3.10. Sean k un cuerpo y $f \in k[X]$ un polinomio de grado 2 o 3. Demuestre que f es irreducible si y solo si f no tiene raíces en k.

Ejercicio 3.11. Consideremos el polinomio

$$f := X^3 + X + 1 \in k[X].$$

Determine para cuáles cuerpos k entre $\mathbb{R}, \mathbb{C}, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$ este polinomio es irreducible.

Ejercicio 3.12. Demuestre que el polinomio

$$f := X^2 - 2X - 2 \in \mathbb{F}_p[X]$$

es irreducible si y solo si $p \equiv \pm 5 \pmod{12}$.

Ejercicio 3.13. Encuentre todos los polinomios mónicos irreducibles de grado 2 y 3 en el anillo $\mathbb{F}_p[X]$ para $p = 2, 3$.

Ejercicio 3.14 (Hendrik Lenstra). Sean $f, g \in \mathbb{F}_5[X]$ dos polinomios tales que $\deg f = 3$, $\deg g = 2$ y

$$fg = u \cdot \prod_{a \in \mathbb{F}_5} (X - a)$$

para algún $u \in \mathbb{F}_5^\times$. Demuestre que el polinomio cúbico $f + g$ es irreducible en $\mathbb{F}_5[X]$. ¿Cuántos pares de polinomios (f, g) tienen la propiedad de arriba? ¿Cuántos polinomios cúbicos irreducibles hay en $\mathbb{F}_3[X]$?

Ejercicio 3.15. Para algún cuerpo k encuentre un polinomio de grado 4 en $k[X]$ que no tiene raíces en k pero es reducible.

Ejercicio 3.16. Demuestre que $\mathbb{Z}[\sqrt{-2}]$ es un dominio euclidiano respecto a la norma habitual

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

Ejercicio 3.17. Demuestre que $\mathbb{Z}[\sqrt{2}]$ es un dominio euclidiano respecto a la norma

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

Ejercicio 3.18. Consideremos el anillo de los enteros de Gauss $\mathbb{Z}[i]$.

1) Encuentre algunos $\alpha, \beta \in \mathbb{Z}[i]$ tales que $\mathfrak{a} := (1 + i) = \{m\alpha + n\beta \mid m, n \in \mathbb{Z}\}$, donde $(1 + i)$ denota el ideal principal en $\mathbb{Z}[i]$ generado por $1 + i$.

2) La misma pregunta para el ideal principal $\mathfrak{b} = (1 + 2i)$.

3) Dibuje los elementos de $\mathfrak{a}$ y $\mathfrak{b}$ en el plano complejo.

Ejercicio 3.19. Calcule $\operatorname{mcd}(\alpha, \beta)$ y $\operatorname{mcm}(\alpha, \beta)$

1) para $\alpha = 9 + 13i$, $\beta = 8 + 6i$ en $\mathbb{Z}[i]$,

2) para $\alpha = 8 + 5\sqrt{2}$, $\beta = 6 + 5\sqrt{2}$ en $\mathbb{Z}[\sqrt{2}]$.

Ejercicio 3.20. Calcule $\operatorname{mcm}(4 + \sqrt{2}, 2 + 3\sqrt{2})$ en el anillo $\mathbb{Z}[\sqrt{2}]$.

Ejercicio 3.21. Calcule el $\operatorname{mcd}(X^5 + X^4 + X^3 + 2X + 2,\ X^5 + X^2 + 2X + 1)$ en $\mathbb{Q}[X]$ y en $\mathbb{F}_3[X]$.

Ejercicio 3.22. Demuestre que el ideal $\mathfrak{a} = (3, 2 + \sqrt{-5})$ no es principal en el anillo $\mathbb{Z}[\sqrt{-5}]$.
Sugerencia: supongamos que $\mathfrak{a} = (\alpha)$ para algún $\alpha \in \mathbb{Z}[\sqrt{-5}]$. En particular, existen $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$ tales que $3 = \alpha\beta$ y $2 + \sqrt{-5} = \alpha\gamma$. Analice las normas $N(a + b\sqrt{-5}) = a^2 + 5\,b^2$ y obtenga una contradicción.

Ejercicio 3.23. Para $n = 1, 2, 3, 4, \ldots$ consideremos el anillo

$$\mathbb{Z}\Big[\frac{1}{n}\Big] := \Big\{\frac{a}{n^k} \;\Big|\; a \in \mathbb{Z},\ k = 0, 1, 2, 3, \ldots\Big\}.$$

Demuestre que todo ideal en $\mathbb{Z}\big[\frac{1}{n}\big]$ es principal, generado por $\frac{a}{1}$ para algún $a \in \mathbb{Z}$.

Ejercicio 3.24 (Norma de Dedekind). Sea A un dominio. Asumamos que existe una función $\delta\colon A\setminus\{0\}\to\mathbb{N}$ que satisface la siguiente propiedad: para cualesquiera $x,y\in A\setminus\{0\}$, si $x\nmid y$, entonces existen $a,b\in A$ tales que

$$ax+by\neq 0,\quad \delta(ax+by)<\delta(x).$$

Demuestre que A es un dominio de ideales principales.

Ejercicio 3.25. Sea A un anillo conmutativo.

1) Demuestre que si $\mathfrak{a}_i\subseteq A$ es una familia de ideales en A, entonces $\bigcap_{i\in I}\mathfrak{a}_i$ es un ideal en A.

2) Demuestre que si $\mathfrak{a}_1\subseteq\mathfrak{a}_2\subseteq\mathfrak{a}_3\subseteq\cdots\subseteq A$ es una cadena de ideales en A, entonces $\bigcup_{i\in I}\mathfrak{a}_i$ es un ideal en A.

Ejercicio 3.26. Sean X un conjunto y A un anillo conmutativo. Recordamos que las aplicaciones $f\colon X\to A$ forman un anillo conmutativo $\operatorname{Fun}(X,A)$ respecto a las operaciones punto por punto. Para un subconjunto $Z\subseteq X$ sea $I(Z)$ el conjunto de las aplicaciones que se anulan en Z:

$$I(Z):=\{f\colon X\to A\mid f(x)=0 \text{ para todo } x\in Z\}.$$

Demuestre que este es un ideal en $\operatorname{Fun}(X,A)$.

Ejercicio 3.27 (Euclides). Sea A un dominio de factorización única que no es un cuerpo y que tiene un número finito de elementos invertibles $A^\times$. En este ejercicio vamos a probar que en A hay un número infinito de elementos primos no asociados entre sí.

0) Asumamos que $p_1,\ldots,p_s$ son todos los primos no asociados entre sí en A.

1) Demuestre que para algún $n=1,2,3,\ldots$ se tiene

$$(p_1\cdots p_s)^n+1\notin A^\times.$$

2) Demuestre que $(p_1\cdots p_s)^n+1$ no es divisible por ningún primo entre $p_1,\ldots,p_s$. Esto nos da una contradicción: un elemento no nulo y no invertible que no es divisible por ningún primo.

Ejercicio 3.28. Demuestre que si k es un cuerpo finito, entonces hay un número infinito de polinomios irreducibles $f\in k[X]$.
Sugerencia: use el ejercicio anterior.

Ejercicio 3.29. Exprese el número 420 como un producto $up_1^{k_1}\cdots p_s^{k_s}$ en $\mathbb{Z}[i]$, donde $u\in\mathbb{Z}[i]^\times$ y $p_1,\ldots,p_s$ son primos de Gauss no asociados entre sí.

Ejercicio 3.30. Demuestre que en un dominio de factorización única A, si $\operatorname{mcd}(a,b)=1$ y $ab=c^k$ para algún $c\in A$ y $k=1,2,3,\ldots$, entonces existen $a',b'\in A$ tales que $a\sim a'^k$ y $b\sim b'^k$.

Ejercicio 3.31. En el anillo $\mathbb{Z}[\sqrt{-7}]$ consideremos los números $\alpha=1+\sqrt{-7}$ y $\beta=1-\sqrt{-7}$.

1) Demuestre que $\operatorname{mcd}(\alpha,\beta)=1$.

2) Demuestre que $\alpha\beta$ es un cubo, pero α y β no son asociados con cubos en $\mathbb{Z}[\sqrt{-7}]$.

Ejercicio 3.32. Asumamos que a,b,c son números enteros positivos tales que

$$a^2+b^2=c^2$$

y $\operatorname{mcd}(a,b)=1$. En este caso se dice que (a,b,c) es una **terna pitagórica primitiva**.

1) Demuestre que uno de los números a y b debe ser impar y el otro debe ser par.

   Asumamos que a es impar y b es par.

2) Usando el ejercicio 3.30, demuestre que existen números enteros u, v tales que

$$a + bi = (u + vi)^2 \quad \text{en } \mathbb{Z}[i],$$

y entonces

$$a = u^2 - v^2, \quad b = 2uv.$$

Ejercicio 3.33. Sea $p = 2, 3, 5, 7, \ldots$ un número primo y $k = 1, 2, 3, 4, \ldots$ Demuestre que

$$v_p\left(\binom{p^k}{n}\right) = k - v_p(n) \quad \text{para todo } n = 1, 2, \ldots, p^k.$$

Sugerencia: calcule las valuaciones p-ádicas de ambos lados de la identidad

$$n!\binom{p^k}{n} = p^k\,(p^k - 1)\,(p^k - 2)\cdots(p^k - n + 1).$$

Note que $v_p(p^k - a) = v_p(a)$ para todo $a = 1, 2, \ldots, p^k - 1$.

Ejercicio 3.34 (Fórmula de Legendre). Demuestre que para todo primo p y todo número natural n se tiene

$$v_p(n!) = \sum_{i\ge 1} \lfloor n/p^i \rfloor.$$

En particular, calcule $v_2(100!)$.

Ejercicio 3.35 (Normas p-ádicas). Sea R un dominio de factorización única y $p \in R$ un elemento primo. Fijemos un número real $0 < \rho < 1$ y pongamos para todo $x \in R$

$$|x|_p := \rho^{v_p(x)}.$$

Demuestre que $|\cdot|_p$ cumple las siguientes propiedades.

N1) $|x|_p = 0$ si y solo si $x = 0$.

N2) $|xy|_p = |x|_p \cdot |y|_p$.

N3) $|x + y|_p \le \text{máx}\{|x|_p, |y|_p\}$, y se cumple la igualdad si $|x|_p \ne |y|_p$.

Bibliografía

[AW2004] Şaban Alaca and Kenneth S. Williams, *Introductory algebraic number theory*, Cambridge University Press, Cambridge, 2004.

[Coh1993] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag Berlin Heidelberg, 1993.
https://doi.org/10.1007/978-3-662-02945-9

[DF2004] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[Mak2013] Trifković Mak, *Algebraic theory of quadratic numbers*, Universitext, 2013.
http://doi.org/10.1007/978-1-4614-7717-4

[Tro1988] Hale F. Trotter, *An overlooked example of nonunique factorization*, The American Mathematical Monthly **95** (1988), no. 4, 339–342.
http://www.jstor.org/stable/2323570