Capítulo 4
Grupos de unidades

Después del capítulo precedente, podemos dar algunos ejemplos de grupos que no hemos visto antes. Los siguientes ejemplos son banales en el sentido de que ciertas estructuras algebraicas ya tienen axiomas de grupos como una parte de su definición.

4.0.1. Ejemplo. Todo anillo (y en particular todo cuerpo) es un grupo abeliano respecto a la adición. Por ejemplo, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos abelianos respecto a la adición habitual de números. ▲

4.0.2. Ejemplo. Los restos módulo n forman un anillo y en particular un grupo abeliano respecto a la adición. ▲

4.0.3. Ejemplo. Tenemos una cadena de subgrupos aditivos

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

▲

4.0.4. Ejemplo. Los números enteros divisibles por n forman un subgrupo de $\mathbb{Z}$:

$$n\mathbb{Z} := \{n\,x \mid x \in \mathbb{Z}\}.$$

▲

4.0.5. Ejemplo. Todo espacio vectorial es un grupo abeliano respecto a la adición de vectores. Por ejemplo, para todo cuerpo k, el espacio vectorial k^n es un grupo abeliano. ▲

4.1 El grupo de unidades de un anillo

En general, salvo 1 (identidad) en un anillo R no hay elementos inversos respecto a la multiplicación. Los elementos que tienen inversos forman un grupo.

4.1.1. Definición. Si para $u \in R$ existe u^{-1} tal que

$$u\,u^{-1} = u^{-1}\,u = 1, \tag{4.1}$$

se dice que u es una **unidad**[*] o un **elemento invertible**.

[*]No confundir con *la identidad* $1 \in R$, que es nada más un ejemplo muy particular de unidades.

Como siempre, el elemento u^{-1} está definido de modo único por (4.1); esto se demuestra de la misma manera que la unicidad de los elementos inversos en un grupo.

4.1.2. Comentario. Supongamos que para $u \in R$ existen dos elementos $a, b \in R$ tales que $au = 1$ y $ub = 1$. En este caso necesariamente $a = b$:

$$a = a \cdot 1 = a\,(ub) = (au)\,b = 1 \cdot b = b.$$

Las unidades forman un grupo respecto a la multiplicación que se denota por $R^\times$. De hecho, $1 \in R^\times$ es el elemento neutro y si $u, v \in R^\times$, entonces $uv \in R^\times$:

$$(uv) \cdot (v^{-1}\,u^{-1}) = (v^{-1}\,u^{-1}) \cdot (uv) = 1.$$

4.1.3. Ejemplo. En un cuerpo todo elemento no nulo $x \in k$ tiene su inverso x^{-1}, así que el grupo de unidades viene dado por

$$k^\times = k \setminus \{0\}.$$

Es abeliano (por nuestra definición, la multiplicación en cuerpo es conmutativa). ▲

4.1.4. Ejemplo. Para $\mathbb{Z}$ obviamente tenemos

$$\mathbb{Z}^\times = \{\pm 1\}.$$

▲

4.1.5. Ejemplo. Tenemos una cadena de subgrupos multiplicativos

$$\{\pm 1\} \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times.$$

▲

4.1.6. Ejemplo. El grupo $\mathbb{Q}^\times$ tiene como su subgrupo el conjunto $\mathbb{Q}_{>0}$ formado por los números racionales positivos. De la misma manera, los números reales positivos $\mathbb{R}_{>0}$ forman un subgrupo de $\mathbb{R}^\times$. ▲

4.2 El círculo y las raíces de la unidad

El grupo $\mathbb{C}^\times$ contiene varios subgrupos interesantes.

4.2.1. Ejemplo. Recordemos que para un número complejo $z = x + y\sqrt{-1} \in \mathbb{C}$ su **valor absoluto** es dado por

$$|z| := \sqrt{z\,\overline{z}} = \sqrt{(x + y\sqrt{-1}) \cdot (x - y\sqrt{-1})} = \sqrt{x^2 + y^2}.$$

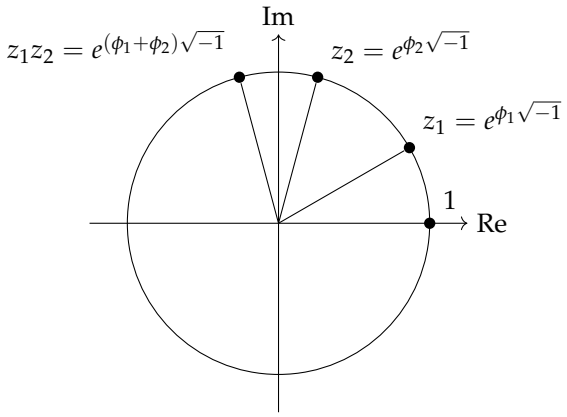
Notamos que para cualesquiera $z_1, z_2 \in \mathbb{C}$ se cumple

$$|z_1 z_2| = |z_1| \cdot |z_2|.$$

Se ve que el conjunto de los números complejos de valor absoluto 1

$$\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{\phi\sqrt{-1}} \mid 0 \leq \phi < 2\pi\}$$

es un subgrupo de $\mathbb{C}^\times$ respecto a la multiplicación. Este grupo se llama el **grupo del círculo**, ya que sus elementos son los puntos del círculo unitario en el plano complejo.



▲

4.2.2. Ejemplo. Para un número $n = 1, 2, 3, 4, \ldots$, una **raíz n-ésima de la unidad** es un número complejo z tal que

$$z^n = 1.$$

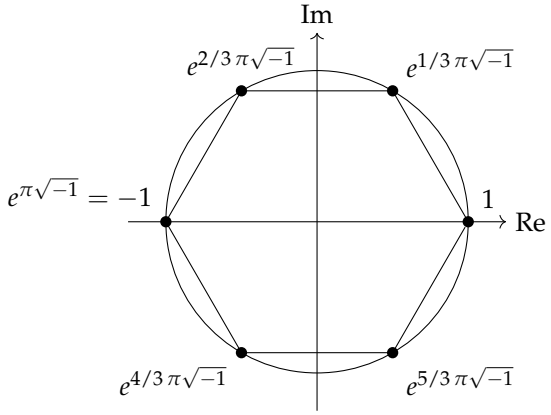
Como sabemos, esta ecuación tiene precisamente n soluciones diferentes

$$e^{2\pi k\sqrt{-1}/n}, \quad k = 0, 1, \ldots, n-1.$$

Estas forman un grupo abeliano respecto a la multiplicación compleja. Este grupo se denota por $\mu_n(\mathbb{C})$ y se llama el **grupo de las raíces n-ésimas de la unidad**:

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1\}.$$

Como el ejemplo más sencillo tenemos $\mu_2(\mathbb{C}) = \{\pm 1\}$. El dibujo de abajo representa el grupo $\mu_6(\mathbb{C})$ en el plano complejo.



Si $m \mid n$, entonces $z^m = 1$ implica $z^n = 1$ y se ve que $\mu_m(\mathbb{C})$ es un subgrupo de $\mu_n(\mathbb{C})$. Por ejemplo, en el dibujo de arriba se ve que $\mu_2(\mathbb{C}) \subset \mu_6(\mathbb{C})$ y $\mu_3(\mathbb{C}) \subset \mu_6(\mathbb{C})$. Todas las raíces de la unidad forman un grupo

$$\mu_\infty(\mathbb{C}) = \{z \in \mathbb{C}^\times \mid z^n = 1 \text{ para algún } n = 1, 2, 3, \ldots\} = \bigcup_{n \geq 1} \mu_n(\mathbb{C}).$$

Tenemos una cadena de subgrupos

$$\mu_m(\mathbb{C}) \overset{\text{si } m|n}{\subset} \mu_n(\mathbb{C}) \subset \mu_\infty(\mathbb{C}) \subset \mathbb{T} \subset \mathbb{C}^\times.$$

▲

4.3 Los restos módulo n invertibles

4.3.1. Ejemplo. Un número $a \in \mathbb{Z}$ es invertible módulo $n = 1, 2, 3, \ldots$ si y solamente si $\mathrm{mcd}(a, n) = 1$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \mathrm{mcd}(a, n) = 1\}.$$

Por ejemplo,

$$\begin{aligned}
(\mathbb{Z}/2\mathbb{Z})^\times &= \{[1]_1\},\\
(\mathbb{Z}/3\mathbb{Z})^\times &= \{[1]_3, [2]_3\},\\
(\mathbb{Z}/4\mathbb{Z})^\times &= \{[1]_4, [3]_4\},\\
(\mathbb{Z}/5\mathbb{Z})^\times &= \{[1]_5, [2]_5, [3]_5, [4]_5\},\\
(\mathbb{Z}/6\mathbb{Z})^\times &= \{[1]_6, [5]_6\},\\
(\mathbb{Z}/7\mathbb{Z})^\times &= \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\},\\
(\mathbb{Z}/8\mathbb{Z})^\times &= \{[1]_8, [3]_8, [5]_8, [7]_8\},\\
(\mathbb{Z}/9\mathbb{Z})^\times &= \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\},\\
(\mathbb{Z}/10\mathbb{Z})^\times &= \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\},\\
&\ldots
\end{aligned}$$

La función

$$\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times| = \text{número de enteros entre 0 y } n-1 \text{ coprimos con } n$$

se llama la **función ϕ de Euler**. He aquí algunos de sus valores[*]:

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$:	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8
n:	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\phi(n)$:	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

La función ϕ de Euler cumple las siguientes propiedades.

1) si $p = 2, 3, 5, 7, 11, \ldots$ es primo y $k = 1, 2, 3, 4, \ldots$, tenemos

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

2) si m y n son coprimos, entonces

$$\phi(mn) = \phi(m) \cdot \phi(n)$$

(se dice que ϕ es una **función multiplicativa**).

[*] Tenemos $\phi(1) = 1$. De hecho, $\mathbb{Z}/1\mathbb{Z}$ es el anillo nulo, y su único elemento es invertible.

Para demostrar 1), consideramos los números

$$a = 0, 1, 2, \ldots, p^k - 2, p^k - 1.$$

En esta lista hay p^k elementos. Luego, $\mathrm{mcd}(a, p^k) = 1$ si y solamente si $p \nmid a$. Los números en la esta tales que $p \mid a$ son los múltiplos de p: $0, p, 2p, 3p, \ldots$—cada p-ésimo número, en total p^k/p de ellos. Entonces,

$$\phi(p^k) = p^k - p^k/p = p^k \left(1 - \frac{1}{p}\right).$$

En particular, para $k = 1$ tenemos $\phi(p) = p - 1$. Es otro modo de decir que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo (tiene todos sus elementos invertibles, salvo el cero).

En general, las mismas consideraciones pueden ser aplicadas a un número arbitario $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$. De los números

$$0, 1, 2, \ldots, n - 1$$

para cada p_i se puede quitar los n/p_i múltiplos de p_i. Pero algunos de estos múltiplos son divisibles al mismo tiempo por p_i y p_j para $i \neq j$, o por tres diferentes primos, etc. El conteo requiere una especie del principio de inclusión-exclusión y nos lleva a la fórmula

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right). \tag{4.2}$$

De esta expresión está clara la propiedad 2). Sin embargo, sería más convincente primero demostrar 2) de otra manera y luego deducir (4.2). Es lo que vamos a hacer más adelante. ▲

4.4 Unidades en anillos aritméticos

4.4.1. Ejemplo. Para los enteros de Gauss el grupo de unidades es de orden 4:

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

Para verlo, definamos la aplicación

$$\begin{aligned} N\colon \mathbb{Z}[\sqrt{-1}] &\to \mathbb{Z}, \\ a + b\sqrt{-1} &\mapsto (a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2, \end{aligned}$$

llamada la **norma**. Note que $N(x) \geq 0$ para todo $x \in \mathbb{Z}[\sqrt{-1}]$. La norma es multiplicativa:

$$N(xy) = N(x)\, N(y).$$

Esto implica que para todo $u \in \mathbb{Z}[\sqrt{-1}]^\times$ se tiene

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

y por lo tanto $N(u) = 1$. Viceversa, para $a + b\sqrt{-1}$ podemos calcular su inverso en el cuerpo de números complejos:

$$(a + b\sqrt{-1})^{-1} = \frac{a - b\sqrt{-1}}{(a + b\sqrt{-1})(a - b\sqrt{-1})} = \frac{a - b\sqrt{-1}}{a^2 + b^2}.$$

Si $N(a+b\sqrt{-1}) = a^2+b^2 = 1$, entonces $(a+b\sqrt{-1})^{-1} \in \mathbb{Z}[\sqrt{-1}]$. Esto demuestra que

$$a+b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]^\times \quad \text{si y solamente si} \quad N(a+b\sqrt{-1}) = a^2+b^2 = 1.$$

La ecuación $a^2+b^2=1$ tiene 4 soluciones enteras $(\pm 1, 0), (0, \pm 1)$ que corresponden a $\pm 1, \pm\sqrt{-1}$. Estos elementos son invertibles.

$\cdot$	$+1$	-1	$+\sqrt{-1}$	$-\sqrt{-1}$
$+1$	$+1$	-1	$+\sqrt{-1}$	$-\sqrt{-1}$
-1	-1	$+1$	$-\sqrt{-1}$	$+\sqrt{-1}$
$+\sqrt{-1}$	$+\sqrt{-1}$	$-\sqrt{-1}$	-1	$+1$
$-\sqrt{-1}$	$-\sqrt{-1}$	$+\sqrt{-1}$	$+1$	-1

El mismo argumento demuestra que para un entero $n = 2, 3, 4, \ldots$ y el anillo conmutativo

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

se tiene $\mathbb{Z}[\sqrt{-n}]^\times = \{\pm 1\}$ para todo $n \geq 2$ —para verlo, considere la norma

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

▲

4.4.2. Ejemplo. Para el anillo $\mathbb{Z}[\sqrt{2}]$ podemos considerar la norma

$$\begin{aligned} N\colon \mathbb{Z}[\sqrt{2}] &\to \mathbb{Z}, \\ a+b\sqrt{2} &\mapsto (a+b\sqrt{2})\,(a-b\sqrt{2}) = a^2-2b^2. \end{aligned}$$

Esta aplicación es también multiplicativa y por lo tanto $N(u) = \pm 1$ para todo $u \in R^\times$. Luego, tenemos

$$(a+b\sqrt{2})^{-1} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})\,(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2},$$

así que

$$a+b\sqrt{2} \quad \text{si y solamente si} \quad N(a+b\sqrt{2}) = a^2-2b^2 = 1.$$

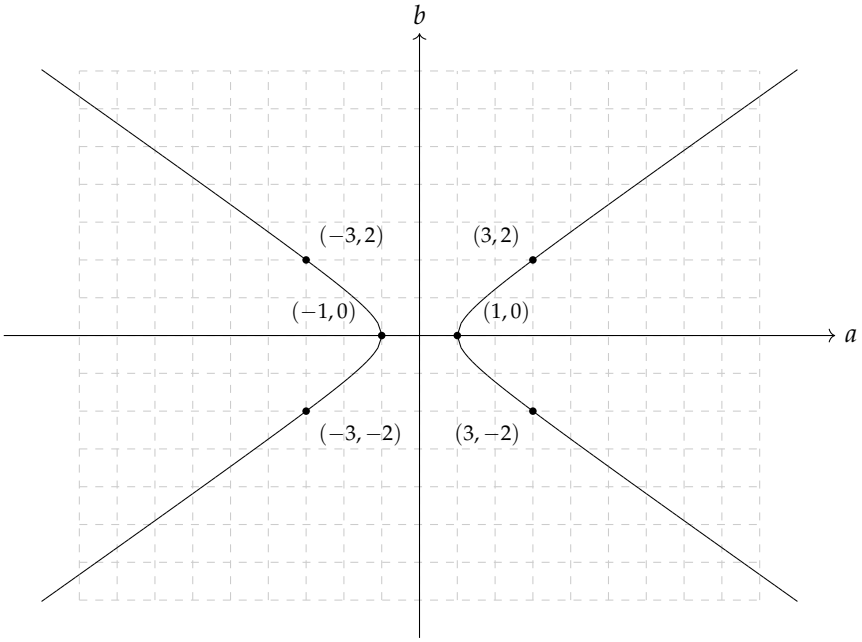
Entonces, para calcular el grupo $\mathbb{Z}[\sqrt{2}]$, hay que encontrar las soluciones enteras de la ecuación

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

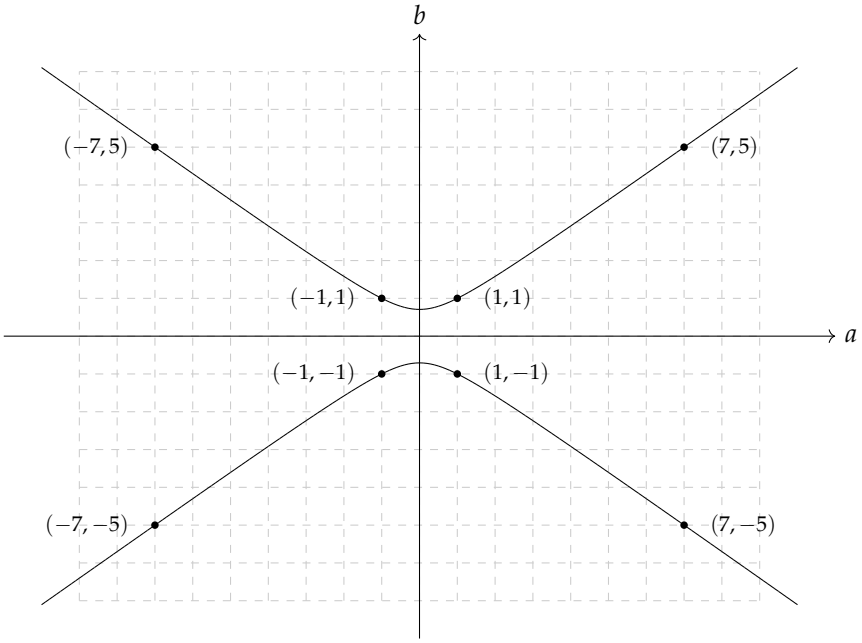
Esta se conoce como la **ecuación de Pell**[*]. No vamos a entrar en los detalles, pero hay un número infinito de soluciones $(a, b) \in \mathbb{Z}^2$. Por ejemplo,

$$(a,b) = (\pm 1, 0),\ (\pm 1, \pm 1),\ (\pm 3, \pm 2),\ (\pm 7, \pm 5),\ \ldots \tag{4.3}$$

[*] 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.



$a^2 - 2b^2 = 1$



$a^2 - 2b^2 = -1$

Las soluciones (4.3) corresponden a las unidades

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

Note que todas las soluciones de arriba son de la forma $\pm(1+\sqrt{2})^n$ para algún $n \in \mathbb{Z}$. Evidentemente, son unidades y estas forman un subgrupo de $\mathbb{Z}[\sqrt{2}]^\times$. De hecho, no hay otras unidades:

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}.$$

Vamos a omitir la demostración ya que esta requiere un análisis más atento de la ecuación de Pell. ▲

La diferencia entre $\mathbb{Z}[\sqrt{-1}]^\times$ por un lado y $\mathbb{Z}[\sqrt{2}]$ por el otro lado es que en el primer anillo el elemento que hemos añadido a $\mathbb{Z}$ es complejo (es decir, $\operatorname{Im}\sqrt{-1} \neq 0$), mientras que $\sqrt{2}$ es real. Esto se estudia en la teoría de números algebraica. Para otro ejemplo similar, véase el ejercicio 4.1.

4.5 Polinomios invertibles

En el capítulo anterior hemos introducido el anillo de polinomios $R[X]$, y sería interesante calcular su grupo de unidades.

4.5.1. Observación. *Si un polinomio $f = \sum_{i\geq 0} a_i X^i \in R[X]$ es invertible, entonces su coeficiente constante es invertible en R; es decir, $a_0 \in R^\times$.*

Demostración. Si existe otro polinomio $g = \sum_{i\geq 0} b_i X^i \in R[X]$ tal que $fg = 1$, esto significa que los coeficientes del producto de f y g están dados por

$$c_k := \sum_{i+j=k} a_i b_j = \begin{cases} 1, & \text{si } k = 0,\\ 0, & \text{si } k > 0.\end{cases}.$$

En particular, $a_0\, b_0 = 1$, lo que significa que $b_0 = a_0^{-1}$. ■

Entonces, la condición $a_0 \in R^\times$ es necesaria para que $f = \sum_{i\geq 0} a_i X^i \in R[X]$ sea invertible, pero no es suficiente. Para simplificar la vida, supongamos que R es un dominio de integridad: $ab = 0$ implica $a = 0$ o $b = 0$. En este caso nos puede servir la noción del grado de un polinomio.

4.5.2. Proposición. *Si R es un dominio de integridad, entonces un polinomio $f = \sum_{i\geq 0} a_i X^i \in R[X]$ es invertible en $R[X]$ si y solamente si $a_0 \in R^\times$ y $a_i = 0$ para $i > 0$. En otras palabras, se tiene una identificación*

$$R[X]^\times = R^\times.$$

Demostración. Apenas hemos visto que la condición $a_0 \in R^\times$ es necesaria. Ahora si f es invertible, tenemos $fg = 1$ para algún polinomio g y luego la identidad

$$0 = \deg(fg) = \deg f + \deg g$$

implica que $\deg f = \deg g = 0$. ■

4.5.3. Comentario. Si en R hay divisores de cero, por ejemplo si $R = \mathbb{Z}/4\mathbb{Z}$, entonces tenemos solamente la desigualdad $\deg(fg) \leq \deg f + \deg g$ en lugar de $\deg(fg) = \deg f + \deg g$ y nuestro argumento no funcióna. En este caso existen polinomios invertibles de grados superiores. Por ejemplo, en el anillo $\mathbb{Z}/4\mathbb{Z}[X]$ se cumple

$$(2X+1)\cdot(2X+1) = 4X^2 + 4X + 1 \equiv 1 \pmod 4.$$

4.6 El grupo lineal general

En los cursos básicos de álgebra lineal mucho tiempo se dedica a multiplicación e inversión de matrices. De hecho, detrás de todo esto hay un grupo.

4.6.1. Definición. Sea V un espacio vectorial sobre un cuerpo. Consideremos todas las aplicaciones lineales *invertibles* $f\colon V \to V$ (isomorfismos entre V y sí mismo); es decir, las que poseen un aplicación lineal inversa $f^{-1}\colon V \to V$ tal que

$$f \circ f^{-1} = \mathrm{id}_V = f^{-1} \circ f.$$

Estas forman un grupo respecto a la composición habitual de aplicaciones. El elemento neutro es la aplicación identidad y los elementos inversos son las aplicaciones inversas. Este grupo se denota por $\mathrm{GL}(V)$ y se llama el **grupo lineal general** de V.

Note que este es un análogo lineal del grupo simétrico S_X. De hecho, $\mathrm{GL}(V)$ es un subconjunto de S_V, pero no tiene sentido considerar todas las biyecciones de conjuntos $V \to V$—son muchas—y por esto restringimos nuestra atención a las biyecciones lineales; es decir, las biyecciones que preservan la estructura algebraica de V.

En general, todas las aplicaciones lineales $f\colon V \to V$ forman un anillo $\mathrm{End}(V)$ que se llama el **anillo de endomorfismos** de V. La adición en este anillo viene dada por

$$(f+g)(v) := f(v) + g(v)$$

y la multiplicación de f por g es la composición $f \circ g$. Este anillo no es conmutativo si $\dim V > 1$. El grupo lineal general es el grupo de unidades correspondiente:

$$\mathrm{GL}(V) = \mathrm{End}(V)^\times.$$

El procedimiento habitual para hacer cálculos con aplicaciones lineales es fijar una base y usar matrices. En el capitulo anterior hemos encontrado el anillo de matrices $M_n(R)$. Es un anillo no conmutativo, pero también tiene sentido considerar su grupo de unidades.

4.6.2. Observación. *Los elementos invertibles en el anillo de matrices $M_n(R)$ son precisamente las matrices con determinante invertible en R:*

$$M_n(R)^\times = \{A \in M_n(R) \mid \det A \in R^\times\}.$$

Demostración. El determinante satisface

$$\det(AB) = \det(A)\cdot\det(B)$$

para cualesquiera $A, B \in M_n(R)$. Luego, si para $A \in M_n(R)$ existe su matriz inversa $A^{-1} \in M_n(R)$, entonces

$$1 = \det(I) = \det(A\,A^{-1}) = \det(A)\cdot\det(A^{-1}) = \det(A^{-1})\cdot\det(A),$$

lo que demuestra que para toda matriz invertible en $M_n(R)$ se tiene necesariamente $\det(A) \in R^\times$. En la otra dirección, si $\det(A) \in R^\times$, podemos usar la fórmula (también conocida como la "regla de Cramer")

$$A^{-1} = \det(A)^{-1} \operatorname{adj}(A),$$

donde $\operatorname{adj}(A)$ es la **matriz adjunta**. ■

4.6.3. Definición. El grupo

$$\mathrm{GL}_n(R) := M_n(R)^\times = \{A \in M_n(R) \mid \det A \in R^\times\}$$

se llama el **grupo lineal general** sobre R.

4.6.4. Ejemplo. Si $R = k$ es un cuerpo, entonces

$$\mathrm{GL}_n(k) = \{A \in M_n(k) \mid \det A \neq 0\}.$$

▲

4.6.5. Ejemplo. Para las matrices con elementos enteros, tenemos

$$\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}.$$

▲

4.6.6. Ejemplo. Para $n = 1$ tenemos

$$\mathrm{GL}_1(R) = R^\times.$$

Para $n \geq 2$ y $R \neq 0$ el grupo $\mathrm{GL}_n(R)$ no es abeliano (en los ejercicios de abajo vamos a calcular su centro). ▲

4.6.7. Ejemplo. Las matrices de $n \times n$ con determinante 1 forman un grupo

$$\mathrm{SL}_n(R) := \{A \in \mathrm{GL}_n(R) \mid \det A = 1\}.$$

Es un subgrupo de $\mathrm{GL}_n(R)$ conocido como el **grupo lineal especial**. En particular, el grupo

$$\mathrm{SL}_2(\mathbb{Z}) := \{A \in M_2(\mathbb{Z}) \mid \det A = 1\}$$

tiene mucha importancia en aritmética; es conocido como el **grupo modular** y vamos a verlo más adelante. ▲

4.6.8. Ejemplo. Hemos visto que para todo primo p los restos módulo p forman un cuerpo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Entonces, el anillo de matrices $M_n(\mathbb{F}_p)$ es finito, de orden p^{n^2}, y en particular los grupos $\mathrm{GL}_n(\mathbb{F}_p)$ y $\mathrm{SL}_n(\mathbb{F}_p)$ son también finitos. ¿Cuál es su orden?

El grupo $\mathrm{GL}_n(\mathbb{F}_p)$ consiste de matrices invertibles de $n \times n$. Para contarlas, podemos escribirlas fila por fila (o columna por columna), recordando que entre estas no podemos tener dependencias lineales. En la primera fila podemos escribir cualquier vector $(x_{11}, x_{12}, \ldots, x_{1n})$, salvo el vector nulo $(0, 0, \ldots, 0)$. Tenemos $|\mathbb{F}_p|^n = p^n - 1$ posibilidades. Luego, en la segunda fila podemos poner cualquier vector $(x_{21}, x_{22}, \ldots, x_{2n})$, salvo los $p = |\mathbb{F}_p|$ vectores linealmente dependientes con $(x_{11}, x_{12}, \ldots, x_{1n})$. Continuando de este modo notamos que para la i-ésima fila hay $p^n - p^i$ posibilidades. Entonces, el número de matrices invertibles de $n \times n$ con elementos en un cuerpo finito $\mathbb{F}_p$ es[*]

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1) \cdot (p^n - p) \cdots (p^n - p^{n-1}).$$

[*]En general existen cuerpos finitos $\mathbb{F}_q$ de orden $q = p^k$ donde p es primo. Para $k = 1$ tenemos $\mathbb{F}_q = \mathbb{Z}/p\mathbb{Z}$ y para $k > 1$ omití la construcción por falta de tiempo. Para $\mathbb{F}_q$ la fórmula y su prueba sería idéntica, solo hay que reemplazar "p" por "q".

Para el grupo $\mathrm{SL}_n(\mathbb{F}_p)$ es suficiente notar que si hay una matriz $A \in \mathrm{SL}_n(\mathbb{F}_p)$, es decir, $\det A = 1$, entonces multiplicando A por un escalar $a \in \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$, se obtiene una matriz $A' := a\,A$ con $\det A' = a$. Además, todas las matrices con determinante a se producen de este modo. Esto demuestra que

$$|\,\mathrm{GL}_n(\mathbb{F}_p)| = |\mathbb{F}_p^\times| \cdot |\,\mathrm{SL}_n(\mathbb{F}_p)|;$$

es decir,

$$|\,\mathrm{SL}_n(\mathbb{F}_p)| = \frac{1}{p-1} \cdot |\,\mathrm{GL}_n(\mathbb{F}_p)|.$$

Notamos que para $p = 2$ se tiene

$$\mathrm{GL}_n(\mathbb{F}_2) = \mathrm{SL}_n(\mathbb{F}_2)$$

(de hecho, en $\mathbb{F}_2$ el único elemento no nulo es 1).

Por ejemplo, el grupo $\mathrm{GL}_2(\mathbb{F}_2)$ tiene 6 elementos:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ C := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ D := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\ E := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

He aquí su tabla de multiplicación[*].

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	D	E	B	C
B	B	E	I	D	C	A
C	C	D	E	I	A	B
D	D	C	A	B	E	I
E	E	B	C	A	I	D

El siguiente caso no trivial sería de $\mathrm{GL}_2(\mathbb{F}_3)$, y este grupo ya tiene $(3^2-1)\cdot(3^2-3) = 48$ elementos y no es muy instructivo enumerarlos todos...

Sería interesante comparar la tabla de multiplicación de arriba con la tabla de multiplicación en el grupo simétrico S_3.

[*]La compilé con ayuda de computadora para no equivocarme. Favor de no hacer estos cálculos otra vez; verifique alguna fila para ver cómo se multiplican las matrices sobre $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Por ejemplo,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad (\text{mód } 2).$$

$\circ$	id	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(2 3)	(1 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 2 3)	(1 3 2)	(2 3)	(1 3)
(2 3)	(2 3)	(1 3 2)	id	(1 2 3)	(1 3)	(1 2)
(1 3)	(1 3)	(1 2 3)	(1 3 2)	id	(1 2)	(2 3)
(1 2 3)	(1 2 3)	(1 3)	(1 2)	(2 3)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 3)	(1 2)	id	(1 2 3)

▲

4.7 Ejercicios

Ejercicio 4.1. *Para el anillo de los enteros de Eisenstein $\mathbb{Z}[\zeta_3]$, calcule el grupo de unidades $\mathbb{Z}[\zeta_3]^\times$ y escriba la tabla de multiplicación correspondiente.*
Indicación: considere la norma

$$N(a+b\,\zeta_3) := (a+b\,\zeta_3)\,\overline{(a+b\,\zeta_3)} = a^2 - ab + b^2.$$

Ejercicio 4.2. *Sea R un anillo conmutativo. Se dice que un elemento $u \in R$ es una **unidad** si existe un elemento $u^{-1} \in R$ tal que $uu^{-1} = u^{-1}u = 1$. Se dice que $x \in R$ es un **nilpotente** si existe un número $n = 1, 2, 3, \ldots$ tal que $x^n = 0$.*

Encuentre las unidades y nilpotentes en los anillos $\mathbb{Z}/4\mathbb{Z}$ y $\mathbb{Z}/9\mathbb{Z}$.

Ejercicio 4.3. *Continuemos con las nociones introducidas en el ejercicio precedente. Sea R un anillo conmutativo.*

1) *Demuestre que si $x \in R$ es un nilpotente y $a \in R$ es cualquier elemento del anillo, entonces ax es un nilpotente.*
2) *Demuestre que si $x, y \in R$ son nilpotentes, entonces $x + y$ es también un nilpotente.*
3) *Demuestre que si $x \in R$ es un nilpotente, entonces $1 + x$ es una unidad.*
   Indicación: recuerde la identidad

$$(1+X)\cdot(1 - X + X^2 - X^3 + X^4 - X^5 + \cdots) = 1$$

   en $R[\![X]\!]$.
4) *Demuestre que si $u \in R$ es una unidad y $x \in R$ es un nilpotente, entonces $u + x$ es una unidad.*

Ejercicio 4.4. *Calcule la matriz inversa para las siguientes matrices:*

$$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} \in M_3(\mathbb{F}_3), \quad \begin{pmatrix} 1 & X & 0 \\ 0 & 1 & X \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z}[X]).$$

Ejercicio 4.5. *Consideremos las matrices de $n \times n$ que tienen 1 en las entradas diagonales, ceros debajo de la diagonal y números arbitrarios arriba de la diagonal.*

$$\{(x_{ij}) \mid x_{ii} = 1 \text{ para todo } i,\ x_{ij} = 0 \text{ para } i > j\}.$$

Por ejemplo, para $n = 3$ son de la forma

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

Demuestre que estas matrices forman un subgrupo de $\mathrm{GL}_n(R)$.

Ejercicio 4.6. *Consideremos el conjunto de matrices*

$$O_n(k) = \{A \in \mathrm{GL}_n(k) \mid A^t\,A = A\,A^t = I\},$$

donde A^t denota la matriz transpuesta.

1) *Demuestre que $O_n(k)$ es un subgrupo de $\mathrm{GL}_n(k)$. Este se llama el **grupo ortogonal** sobre k.*
2) *Para $n = 2$ y $k = \mathbb{R}$ demuestre que los elementos de $O_2(\mathbb{R})$ son de la forma*

$$\begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix} \quad o \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}.$$

3) *Demuestre que el grupo diédrico D_n es un subgrupo de $O_2(\mathbb{R})$. Escriba las matrices[*] que corresponden a los*

[*] En este ejercicio hay que identificar las aplicaciones lineales $\mathbb{R}^2 \to \mathbb{R}^2$ con matrices de 2×2.

elementos r y f.

Ejercicio 4.7. *Demuestre que el grupo $\mathrm{SL}_2(\mathbb{Z})$ es infinito.*

Ejercicio 4.8. *Demuestre que las únicas matrices invertibles que conmutan con todas las matrices son las* ***matrices escalares***

$$aI = \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} \quad \text{para } a \in R^\times.$$

Es decir,

$$Z(\mathrm{GL}_n(R)) = \{aI \mid a \in R^\times\}.$$

1) *Fijemos algunos índices $1 \leq i, j \leq n$, $i \neq j$. Denotemos por e_{ij} la matriz de $n \times n$ cuyos coeficientes son nulos, excepto el coeficiente (i, j) que es igual a 1. Consideremos las matrices $I + e_{ij}$. Estas tienen ceros en todas las entradas, excepto 1 en la posición (i, j) y en la diagonal. Demuestre que*

$$\det(I + e_{ij}) = 1$$

En particular, $I + e_{ij} \in \mathrm{GL}_n(R)$.

2) *Supongamos que $A \in Z(\mathrm{GL}_n(R))$. En particular, debe cumplirse*

$$(I + e_{ij})\, A = A\, (I + e_{ij}),$$

que es equivalente a la identidad

$$e_{ij}\, A = A\, e_{ij}$$

en el anillo de matrices $M_n(R)$. Recuerde la tarea anterior donde hemos visto que esto implica que A es una matriz escalar.

3) *Note que el centro de $Z(\mathrm{SL}_n(R))$ también consiste en las matrices escalares (de determinante 1).*

Ejercicio 4.9. *Demuestre que una serie formal de potencias $f = \sum_{i \geq 0} a_i\, X^i \in R[\![X]\!]$ es invertible (pertenece a $R[\![X]\!]^\times$) si y solamente si su coeficiente constante es invertible ($a_0 \in R^\times$).*

Ejercicio 4.10. *Calcule las series $(1 - X)^{-1}$, $(1 - X^2)^{-1}$, $(1 - (X + X^2))^{-1}$ en el anillo $\mathbb{Z}[\![X]\!]$.*