Grupos y Anillos

Bibliografía:

- Apuntes de clase, Ángel del Río Mateos.

Capítulo 1

Anillos

1.1. Operaciones binarias

Una **operación** (**binaria**) en un conjunto X es una aplicación $* : X \times X \to X$, escribimos $a * b := *(a, b)$, y decimos que $*$ es:

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

Un $x \in X$ es:

- **Neutro por la izquierda** de X con respecto a $*$ si $\forall y \in X, x * y = y$, **por la derecha** si $\forall y \in X, y * x = x$ y **neutro** si es neutro por la izquierda y por la derecha.
- **Cancelativo por la izquierda** en X respecto a $*$ si $\forall a, b \in X, (x*a = x*b \implies a = b)$, **por la derecha** si $\forall a, b \in X, (a * x = b * x \implies a = b)$ y **cancelativo** si es cancelativo por la izquierda y por la derecha.
- **Simétrico** de $y \in X$ **por la izquierda** si existe un neutro e tal que $x * y = e$, **por la derecha** si $y * x = e$ y **simétrico** de y e **invertible** si es simétrico por la izquierda y por la derecha.

Dado un conjunto X y una operación $*$ en X, $(X, *)$ es:

1. Un **semigrupo** si $*$ es asociativa.
2. Un **monoide** si además X tiene un elemento neutro respecto a $*$.
3. Un **grupo** si además todo elemento de X es invertible.
4. Un **grupo abeliano** si además $*$ es conmutativa.

Ejemplos:

1. $(\mathbb{N}, +)$ es un monoide conmutativo, y $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son grupos abelianos.
2. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son monoides conmutativos con el producto.
3. Llamamos Y^X al conjunto de funciones de X a Y. Dado un conjunto X, $(X^X, \circ)$ es un monoide, pero no es conmutativo si $|X| \geq 2$.

Dada una operación $*$ en un conjunto X:

1. Si $*$ es conmutativa, todo neutro por un lado es neutro, todo elemento cancelativo por un lado es cancelativo y todo elemento con simétrico por un lado es invertible.
2. Si e es neutro por la izquierda y f lo es por la derecha, $e = f$. En particular, X tiene a lo sumo un neutro.

Dado un monoide $(X, *)$ y $a \in X$:

1. Si x es simétrico por la izquierda de a e y es simétrico por la derecha de a, entonces $x = y$. En particular, a tiene a lo sumo un simétrico.
2. Si a tiene simétrico por un lado, es cancelable por dicho lado. En particular, todo invertible es cancelable.

1.2. Anillos

Un **anillo** es una terna $(A, +, \cdot)$ formada por un conjunto A y dos operaciones sobre A llamadas **suma** y **producto** tales que $(A, +)$ es un grupo abeliano, $(A, \cdot)$ es un monoide y el producto es **distributivo** respecto de la suma, es decir, $\forall a, b, c \in A, (a \cdot (b + c) = (a \cdot b) + (a \cdot c) \wedge (a + b) \cdot c = (a \cdot c) + (b \cdot c))$. Si además $\cdot$ es conmutativo, $(A, +, \cdot)$ es un **anillo conmutativo**.

Asumimos que el producto tiene más prioridad que la suma, y escribimos $ab \coloneqq a \cdot b$. Llamamos **opuesto** de $a \in A$, $-a$, al simétrico de a respecto de la suma, y escribimos $a - b \coloneqq a + (-b)$. Si además a es invertible, llamamos **inverso** de a, a^{-1}, al simétrico de A respecto del producto. Si b es invertible en A y A es conmutativo, escribimos $a/b \coloneqq \frac{a}{b} \coloneqq ab^{-1}$. Decimos que $a \in A$ es **regular** si es cancelable respecto del producto o **singular** en caso contrario. Una **unidad** de A es un elemento invertible, y llamamos A^* al conjunto de unidades de A.

Ejemplos:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos conmutativos con la suma y el producto usuales.
2. Dada una familia de anillos $(A_i)_{i \in I}$, el producto $\prod_{i \in I} A_i$ es un anillo con las operaciones definidas componente a componente, esto es, dados $a, b \in \prod_{i \in I} A_i$, $a + b \coloneqq (a_i + b_i)_{i \in I}$ y $ab \coloneqq (a_i b_i)_{i \in I}$. En particular, si A es un anillo y X es un conjunto, $A^X = \prod_{x \in X} A$ es un anillo con la suma y el producto dados por $(f+g)(x) \coloneqq f(x)+g(x)$ y $(fg)(x) \coloneqq f(x)g(x)$.
3. Si A es un anillo y n es un entero positivo, el conjunto $\mathcal{M}_n(A)$ de matrices cuadradas en A de tamaño n es un anillo con la suma y el producto habituales.

Sean A un anillo y $a, b, c \in A$:

1. Todo elemento es cancelable respecto de la suma.
2. Todo elemento invertible es regular.
3. $b + a = a \implies b = 0$, $\forall a \in A, ba = a \implies b = 1$. En particular, el 0 y el 1 son únicos.
4. El opuesto de a es único, y si a es invertible, el inverso es único.
5. $0a = a0 = 0$.
6. $a(-b) = (-a)b = -(ab)$.
7. $a(b - c) = ab - ac$.
8. a y b son invertibles si y sólo si lo son ab y ba, en cuyo caso $(ab)^{-1} = b^{-1}a^{-1}$.
9. Si $0 = 1$, $A = \{0\}$.

Dado un anillo A, llamamos 0_A al cero de A y 1_A al uno de A. Si $a \in A$, definimos $0_{\mathbb{Z}}a \coloneqq 0$, y para $n \in \mathbb{Z}^+$, $na \coloneqq (n-1)a + a$ y $(-n)a \coloneqq -(na)$. Definimos $a^{0_{\mathbb{Z}}} \coloneqq 1_A$, para $n \in \mathbb{Z}^+$, $a^n \coloneqq a^{n-1}a$, y si a es invertible, $a^{-n} \coloneqq (a^{-1})^n$.

Dados un anillo A, $a, b \in A$ y $m, n \in \mathbb{Z}$:

1. $n(a + b) = na + nb$.
2. $(n + m)a = na + ma$.
3. $n(ma) = (nm)a$.
4. Si $n, m \geq 0$, $a^{n+m} = a^n a^m$, y si a es invertible, esto se cumple para n y m enteros arbitrarios.
5. Si A es conmutativo y $n \geq 0$, $(ab)^n = a^n b^n$, y si además a y b son invertibles, esto se cumple para todo entero n.

1.3. Subanillos

Sean $*$ una operación sobre un conjunto A y $B \subseteq A$, B es **cerrado** respecto a $*$ si $\forall a, b \in B, a * b \in B$, en cuyo caso $\hat{*} : B \times B \to B$ dada por $x \hat{*} y \coloneqq x * y$ es la operación **inducida** en B por $*$, que identificamos con $*$. Sea B cerrado respecto a $*$, si $(A, *)$ y $(B, *)$ son semigrupos, B es un **subsemigrupo** de A; si son monoides con el mismo neutro, es un **submonoide**, y si son grupos con el mismo neutro, es un **subgrupo**. Si B es cerrado respecto a las operaciones $+$ y $\cdot$ en A y $(A, +, \cdot)$ y $(B, +, \cdot)$ son anillos con el mismo uno, B es un **subanillo** de A.

Para que $B \subseteq A$ sea un subsemigrupo del semigrupo $(A, *)$, basta con que B sea cerrado respecto a $*$; para que sea un submonoide del monoide $(A, *)$, también debe contener al neutro, y para que sea un subgrupo del grupo $(A, *)$, debe además ser cerrado respecto a inversos.

$B \subseteq A$ es un subanillo de A si y sólo si contiene al 1 y es cerrado para sumas productos y opuestos, si y sólo si contiene al 1 y es cerrado para restas y productos, y en tal caso el cero de A es el de B.

Algunos subanillos:

1. Todo anillo A es un subanillo de sí mismo, el **subanillo impropio**, y el resto de subanillos son **propios**.
2. Cada uno de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es un subanillo de los posteriores.
3. $\{0\}$ es subanillo de A si y sólo si $A = \{0\}$.
4. Llamamos **subanillo primo** de A a $\mathbb{Z}1 \coloneqq \{n1_A\}_{n\in\mathbb{Z}}$, el menor subanillo de A.
5. Si A y B son anillos y $B \neq 0$, $A \times \{0_B\}$ es cerrado para sumas y productos pero no es un subanillo de $A \times B$.
6. Dado $z \in \mathbb{C}$, llamamos $\mathbb{Z}[z] \coloneqq \{a + bz\}_{a,b\in\mathbb{Z}}$ y $\mathbb{Q}[z] \coloneqq \{a + bz\}_{a,b\in\mathbb{Q}}$. Dado $m \in \mathbb{Z}$, $\mathbb{Z}[\sqrt{m}]$ y $\mathbb{Q}[\sqrt{m}]$ son subanillos de $\mathbb{C}$, y si además $m \geq 0$, lo son también de $\mathbb{R}$. Si m es el cuadrado de un entero, $\mathbb{Z}[\sqrt{m}] = \mathbb{Z}$ y $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}$, y de lo contrario $a + b\sqrt{m} = c + d\sqrt{m} \implies a = c \wedge b = d$. Podemos ver $\mathbb{Z}[\sqrt{m}]$ con $m < 0$ como el conjunto de vértices de un enlosado del plano complejo por losas rectangulares con base 1 y altura $\sqrt{|m|}$.
7. Dado un espacio topológico X, $\{f \in \mathbb{R}^X \mid f \text{ continua}\}$ es un subanillo de $\mathbb{R}^X$ con la suma y el producto por elementos.
8. Dado un espacio vectorial V, $\{f \in V^V \mid f \text{ lineal}\}$ es un subanillo de $(V^V, +, \circ)$.
9. Dado un anillo A y un conjunto X, $\{f \in A^X \mid f \text{ constante}\}$ es un subanillo de A^X.

1.4. Homomorfismos

Un **homomorfismo** entre dos anillos A y B es una aplicación $f : A \to B$ tal que para $x, y \in A$:

1. $f(x) + f(y) = f(x + y)$.
2. $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

Un **isomorfismo** es un homomorfismo biyectivo, y un **automorfismo** de A es un isomorfismo de A en A. Dos anillos A y B son **isomorfos** si existe un isomorfismo entre ellos.

Sean $f : A \to B$ un homomorfismo de anillos y $a, b, a_1, \ldots, a_n \in A$:

1. $f(0) = 0$.
2. $f(-a) = -f(a)$.
3. $f(a - b) = f(a) - f(b)$.
4. $f(a_1 + \cdots + a_n) = f(a_1) + \cdots + f(a_n)$.
5. $f(na) = nf(a)$.
6. Si a es invertible, $f(a)$ también lo es y $f(a)^{-1} = f(a^{-1})$.

7. $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$.
8. Si A' es un subanillo de A, $f(A')$ es un subanillo de B.
9. Si B' es un subanillo de B, $f^{-1}(B')$ es un subanillo de A.
10. Si f es un isomorfismo de anillos, f^{-1} también.

Ejemplos:

1. Dados anillos A y B, $f : A \to B$ dada por $f(a) = 0$ es un homomorfismo si y sólo si $B = 0$.
2. Sea B un subanillo de A, la inclusión $i : B \to A$ es un homomorfismo.
3. Dado un anillo A, $\mu : \mathbb{Z} \to A$ dada por $\mu(n) \coloneqq n1$ es el único homomorfismo de anillos de $\mathbb{Z}$ en A.
4. Dada una familia de anillos $(A_i)_{i\in I}$ y $j \in I$, la **proyección** $p_j : \prod_{i\in I} A_i \to A_j$ dada por $p_j(a) \coloneqq a_j$ es un homomorfismo.
5. La **conjugación** de complejos, dada por $\overline{a + bi} \coloneqq a - bi$ para $a, b \in \mathbb{R}$, es un automorfismo en $\mathbb{C}$. Del mismo modo, si d es un entero que no es un cuadrado, definiendo el conjugado de $a+b\sqrt{d}$ como $a-b\sqrt{d}$ en $\mathbb{Z}[\sqrt{d}]$ o en $\mathbb{Q}[\sqrt{d}]$ tenemos un automorfismo. Entonces llamamos **norma** a la aplicación $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ o $N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}$ dada por $N(a + b\sqrt{d}) \coloneqq (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$.

1.5. Ideales

Un **ideal** de un anillo conmutativo A es un subconjunto $I \subseteq A$ no vacío tal que $\forall x, y \in I, x + y \in I$ y $\forall x \in I, \forall a \in A, ax \in I$. Todo ideal contiene al 0.

1. Dado un anillo A, $0 \coloneqq \{0\}$ es un ideal de A llamado **ideal cero**, y A es un ideal llamado **ideal impropio**, en oposición al resto que son **ideales propios**.
2. Dado un anillo A y $T \subseteq A$, llamamos **ideal generado** por T a

$$TA \coloneqq (T) \coloneqq \left\{ \sum_{k=1}^{n} a_k t_k \right\}_{n\in\mathbb{N}, a_k \in A, t_k \in T}.$$

   En particular, dado $b \in A$, llamamos **ideal principal** generado por b a $(b) \coloneqq bA \coloneqq \{b\}A$. Todos los ideales de $\mathbb{Z}$ son de esta forma.
3. Sean I un ideal de A y J un ideal de B, $I \times J$ es un ideal de $A \times B$.

Dado un ideal I de A, $a, b \in A$ son **congruentes módulo** I, $a \equiv b$ mód I, si $b - a \in I$, y esta es una relación de equivalencia en A con clases de equivalencia de la forma $[a] \coloneqq a + I \coloneqq \{a + x\}_{x\in I}$ y conjunto cociente $A/I = \{[a]\}_{a\in A}$. Además, $a \equiv b$ mód $(0) \iff a = b$.

Las operaciones $[a] + [b] \coloneqq [a + b]$ y $[a][b] \coloneqq [ab]$ están bien definidas y dotan a A/I de una estructura de anillo conmutativo con cero $[0]$ y uno $[1]$, que llamamos **anillo cociente de** A **módulo** I.

$A/0 \cong A$ y $A/A \cong 0$. Dado $n \in \mathbb{Z}^+$, llamamos $\mathbb{Z}_n \coloneqq \frac{\mathbb{Z}}{n\mathbb{Z}} = \{0 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$.
Dado un anillo conmutativo A:

1. $b \in A$ es invertible si y sólo si $(b) = A$.

2. Un ideal I de A es impropio si y sólo si $1 \in I$, si y sólo si I contiene una unidad de A.

Sea $f : A \to B$ un homomorfismo de anillos, llamamos **núcleo** de f a $\ker f \coloneqq f^{-1}(0)$. Entonces $\mathrm{Im} f$ es un subanillo de B y $\ker f$ es un ideal de A.

Un homomorfismo de anillos $f : A \to B$ es inyectivo si y sólo si $\ker f = 0$.

Teorema de la correspondencia: Si I es un ideal de A, $J \overset{\pi}{\mapsto} J/I \coloneqq \{[a]\}_{a \in J}$ es una biyección entre el conjunto de los ideales de A que contienen a I y el de los ideales de A/I, y tanto π como π^{-1} preservan la inclusión.

Demostración: Empezamos viendo que, si $J \supseteq I$ es ideal de A, J/I es un ideal de A/I. Como $0 \in J$, $[0] \in J/I \neq \emptyset$; para $[x], [y] \in J/I$, $[x] + [y] = [x + y] \in J/I$, y para $[x] \in J/I$ y $[a] \in A/I$, $[a][x] = [ax] \in J/I$. Además, $\pi^{-1}(J/I) = J$, pues $\pi^{-1}(J/I) = \{x \mid \pi(x) = [x] \in J/I\}$, pero si $x \in J$, $[x] \in J/I$, y si $[x] \in J/I$, existe $a \in I \subseteq J$ con $x + a \in J$ y por tanto $-a \in J$ y $(x + a) - a = x \in J$.

Ahora vemos que, dado un ideal X de A/I, $\pi^{-1}(X)$ es un ideal de A que contiene a I. En efecto, como $[0] = I \in X$, $\pi^{-1}(X) = \{x \mid [x] \in X\} \ni 0$; para $x, y \in \pi^{-1}(X)$, $[x], [y] \in X$, luego $[x + y] = [x] + [y] \in X$ y $x + y \in \pi^{-1}(X)$; para $x \in \pi^{-1}(X)$ y $a \in A$, $[ax] = [a][x] \in X$ y $ax \in \pi^{-1}(X)$, y para $x \in I$, $[x] \in I/I = 0$, luego $x \in \pi^{-1}(0) \subseteq \pi^{-1}(X)$ e $I \subseteq \pi^{-1}(X)$. Además, $\pi^{-1}(X)/I = \{x \mid [x] \in X\}/I = \{[x] \mid [x] \in X\} = X$.

Para ver que π preserva la inclusión, sean $I \subseteq J \subseteq K$ ideales de A, queremos ver que $J/I \subseteq K/I$. Para $[x] \in J/I$, existe $a \in I \subseteq J$ con $x + a \in J$, luego $x = (x + a) - a \in J \subseteq K$ y por tanto $[x] \in K/I$. Queda ver que π^{-1} también preserva la inclusión. Sean $X \subseteq Y$ ideales de A/I, queremos ver que $\pi^{-1}(X) \subseteq \pi^{-1}(Y)$. Sea $x \in \pi^{-1}(X)$, entonces $[x] \in X \subseteq Y$, luego existe $a \in I \subseteq \pi^{-1}(Y)$ con $x + a \in \pi^{-1}(Y)$, y como $\pi^{-1}(Y)$ es un ideal, $x = (x + a) - a \in \pi^{-1}(Y)$.

1.6. Operaciones con ideales

La intersección de una familia de ideales de A es un ideal de A, con lo que (X) es la intersección de todos los ideales de A que contienen a X. Por otro lado, si $\{I_x\}_{x \in X}$ es una familia de ideales de A, definimos los ideales

$$\begin{aligned} \sum_{x \in X} I_x &\coloneqq \left\{ \sum_{x \in S} a_x \;\middle|\; S \subseteq X \text{ finito}, a_x \in I_x \right\}, \\ \prod_{x \in X} I_x &\coloneqq \left\{ \sum_{k=1}^{n} \prod_{x \in S} a_{kx} \;\middle|\; n \in \mathbb{N}, S \subseteq X \text{ finito}, a_{kx} \in I_x \right\}. \end{aligned}$$

Entonces:

1. Si $\{I_x\}_{x \in X}$ es una familia de ideales de A, $\sum_{x \in X} I_x = \left(\bigcup_{x \in X} I_x\right)$.

2. Si $I_1, \ldots, I_n$ son ideales de A, $I_1 \cdots I_n = \left(\{x_1 \cdots x_n\}_{x_k \in I_k}\right)$.

Sean $n, m \in \mathbb{Z}$ coprimos, $(n)(m) = (nm)$, $(n) \cap (m) = (\mathrm{mcm}(n, m))$ y $(n) + (m) = (\mathrm{mcd}(n, m))$.

1.7. Teoremas de isomorfía

Primer teorema de isomorfía: Dado un homomorfismo de anillos conmutativos $f : A \to B$, existe un único isomorfismo de anillos $\tilde{f} : A/\ker f \to \mathrm{Im}f$ tal que $i \circ \tilde{f} \circ p = f$, donde $i : \mathrm{Im}f \to B$ es la inclusión y $p : A \to A/\ker f$ es la proyección. En particular,

$$A/\ker f \cong \mathrm{Im}f.$$

Demostración: Sean $K \coloneqq \ker f$ e $I \coloneqq \mathrm{Im}f$. La función $\tilde{f} : A/K \to I$ dada por $\tilde{f}(x+K) \coloneqq f(x)$ está bien definida, pues si $x+K = y+K$, $x-y \in K$ y por tanto $f(x)-f(y) = f(x-y) = 0$ y $f(x) = f(y)$. Es claro que $\tilde{f}$ es un homomorfismo de anillos suprayectivo. Para ver que es inyectivo, sea $x+K \in \ker \tilde{f}$, entonces $0 = \tilde{f}(x+K) = f(x)$ y por tanto $x \in K$ y $x+K = 0+K = 0$. Para ver que $i \circ \tilde{f} \circ p = f$, $(i \circ \tilde{f} \circ p)(x) = \tilde{f}(x+K) = f(x)$ para todo $x \in A$. Para la unicidad, sea $\hat{f} : A/K \to I$ otro isomorfismo con $i \circ \hat{f} \circ p = f$, para $x \in A$, $\hat{f}(x+K) = i(\hat{f}(p(x)) = f(x) = \tilde{f}(x+K)$.

Así, si A y B son anillos conmutativos, $\frac{A\times B}{0\times B} \cong A$.

Segundo teorema de isomorfía: Dados dos ideales $I \subseteq J$ de A,

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

Demostración: J/I es ideal de A/I por el teorema de la correspondencia. Sea $f : A/I \to A/J$ dada por $f(a+I) \coloneqq a+J$, es fácil ver que f es un homomorfismo de anillos suprayectivo y que $\ker f = J/I$, y entonces basta aplicar el primer teorema de isomorfía.

Tercer teorema de isomorfía: Sea A un anillo con un subanillo B y un ideal I:

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

   Sean $x, y \in B \cap I$, $x+y \in B$ y $x+y \in I$, y sean $x \in B \cap I$ y $a \in B$, $ax \in I$ y $ax \in B$.

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

   Sean $a, b \in B$ y $x, y \in I$, $(a+x)-(b+y) = (a-b)+(x-y) \in B+I$ y $(a+x)(b+y) = ab+ay+xb+xy = ab+(ay+bx+xy) \in B+I$, y como $1 \in B \subseteq B+I$, $B+I$ es un subanillo. Además, para $x, y \in I$, $x+y \in I \subseteq B+I$, y para $a \in B$ y $x, y \in I$, $(a+x)y \overset{a+x\in A}{\in} I \subseteq B+I$.

3. $$\frac{B}{B\cap I} \cong \frac{B+I}{I}.$$

   Sea $f : B \to A/I$ dada por $f(x) \coloneqq x+I$, es claro que $\ker f = B \cap I$ e $\mathrm{Im}f = (B+I)/I$, y basta aplicar el primer teorema de isomorfía.

Un anillo A tiene **característica** $n \in \mathbb{Z}^{\geq 0}$ si n es el menor entero positivo con $n1_A = 0_A$, o 0 si no existe tal n. Sean A un anillo conmutativo, $f : \mathbb{Z} \to A$ el único homomorfismo de anillos ($f(n) = n1$) y $n \geq 0$, A tiene característica n si y sólo si $\ker f = n\mathbb{Z}$, si y sólo si el subanillo primo de A es isomorfo a $\mathbb{Z}_n$, si y sólo si A contiene un subanillo isomorfo a $\mathbb{Z}_n$.

Teorema chino de los restos: Sean A un anillo conmutativo, $n \geq 1$ e $I_1, \ldots, I_n$ ideales de A con $I_i + I_j = A$ para $i \neq j$, entonces $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ y

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

Demostración: Supongamos primero $n = 2$. Como $I_1 + I_2 = A$, sean $x_1 \in I_1$ y $x_2 \in I_2$ con $x_1 + x_2 = 1$, para $a \in I_1 \cap I_2$, $a = x_1 a + a x_2 \in I_1 I_2$, luego $I_1 \cap I_2 \subseteq I_1 I_2$, y la otra inclusión es clara. Por otro lado, $f : A \to \frac{A}{I_1} \times \frac{A}{I_2}$ dada por $f(a) \coloneqq (a + I_1, a + I_2)$ es un homomorfismo de anillos con núcleo $I_1 \cap I_2$, y es suprayectiva porque para $(a_1 + I_1, a_2 + I_2) \in \frac{A}{I_1} \times \frac{A}{I_2}$,

$$f(a_1 x_2 + a_2 x_1) = (a_1 x_2 + a_2 x_1 + I_1, a_1 x_2 + a_2 x_1 + I_2) =$$
$$= (a_1 x_2 + I_1, a_2 x_1 + I_2) \overset{\substack{x_2 \equiv 1 \text{ mód } I_1 \\ x_1 \equiv 1 \text{ mód } I_2}}{=} (a_1 + I_1, a_2 + I_2).$$

El resultado se obtiene por el primer teorema de isomorfía.

Para $n > 2$, supongamos que esto se cumple para $n - 1$. Entonces, por la hipótesis de inducción, $I_1 \cap \cdots \cap I_{n-1} \cap I_n = (I_1 \cap \cdots \cap I_{n-1}) I_n = I_1 \cdots I_{n-1} I_n$. Para $k \leq n - 1$, existen $a_k \in I_k$ y $b_k \in I_n$ con $a_k + b_k = 1$ y, multiplicando,

$$1 = \prod_{k=1}^{n-1} (a_k + b_k) =: a_1 \cdots a_{n-1} + b,$$

con $b \in I_n$ porque en cada sumando que incluye hay al menos un factor en I_n, y como $a_1 \cdots a_{n-1} \in I_1 \cap \cdots \cap I_{n-1}$, $1 \in (I_1 \cap \cdots \cap I_{n-1}) + I_n$ y por tanto $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$. Así,

$$\frac{A}{I_1 \cap \cdots \cap I_n} \cong \frac{A}{I_1 \cap \cdots \cap I_{n-1}} \times \frac{A}{I_n} \cong \frac{A}{I_1} \times \cdots \times \frac{A}{I_{n-1}} \times \frac{A}{I_n}.$$

Capítulo 2

Divisibilidad en dominios

Un **dominio** (**de integridad**) es un anillo conmutativo en que todos los elementos no nulos son regulares, y un **cuerpo** es uno en que todos los elementos no nulos son invertibles. Un **subdominio** es un subanillo de un dominio que es dominio, y un **subcuerpo** es un subanillo de un cuerpo que es cuerpo. Todo cuerpo es un dominio. Si A es un anillo conmutativo:

1. A es un cuerpo si y sólo si los únicos ideales de A son 0 y A, si y sólo si todo homomorfismo de anillos $A \to B$ con $B \neq 0$ es inyectivo.
2. Un $a \in A$ es regular si y sólo si $\forall b \in A, (ab = 0 \implies b = 0)$.
3. A es un dominio si y sólo si $\forall a, b \in A \setminus \{0\}, ab \neq 0$.
4. Todo subanillo de un dominio es un dominio.
5. La característica de un dominio no trivial es 0 o un número primo.

Algunos dominios:

1. $\mathbb{Z}$ es un dominio no cuerpo, y $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.
2. Para $n \geq 2$, $\mathbb{Z}_n$ es un dominio si y sólo si es un cuerpo, si y sólo si n es primo.
3. Si $m \in \mathbb{Z}$ no es cuadrado de entero, $\mathbb{Z}[\sqrt{m}]$ es un dominio no cuerpo y $\mathbb{Q}[\sqrt{m}]$ es cuerpo.
4. Un producto de anillos no triviales nunca es un dominio.

2.1. Ideales maximales y primos

Un ideal I del anillo A es **maximal** si no está contenido estrictamente en ningún ideal propio de A, y es **primo** si $\forall a, b \in A, (ab \in I \implies a \in I \vee b \in I)$. Sea I un ideal propio de A:

1. I es maximal si y sólo si A/I es un cuerpo.
2. I es primo si y sólo si A/I es un dominio.
3. Si I es maximal, es primo.

4. A es cuerpo si y sólo si 0 es maximal.

5. A es dominio si y sólo si 0 es primo.

Dado un conjunto S con un orden parcial, una **cadena** de S es un subconjunto totalmente ordenado. S es **inductivo** si toda cadena suya tiene supremo. Del axioma de elección se deduce el **lema de Zorn:** Todo conjunto inductivo tiene un elemento maximal.

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

2.2. Divisibilidad

Dados un anillo conmutativo A y $a, b \in A$, a **divide** a b, es un **divisor** de b o b es un **múltiplo** de a en A, $a \mid b$, si existe $c \in A$ tal que $b = ac$. Propiedades:

1. Reflexiva.

2. Transitiva.

3. $1 \mid a \mid 0$.

4. $0 \mid a \iff a = 0$.

5. $a \mid 1$ si y sólo si a es unidad, en cuyo caso $\forall x \in A, a \mid x$.

6. Si a divide a ciertos elementos, divide a cualquier combinación lineal de estos con coeficientes en A.

7. Si c es regular y $ac \mid bc$, $a \mid b$.

Dos elementos $a, b \in A$ son **asociados** en A si $a \mid b \mid a$ en A, si y sólo si tienen los mismos divisores, si y sólo si tienen los mismos múltiplos. Esta relación es de equivalencia.

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

Sean A un anillo conmutativo y $a \in A \setminus (A^* \cup \{0\})$, a es **irreducible** en A si $\forall b, c \in A, (a = bc \implies b \in A^* \vee c \in A^*)$, y es **primo** en A si $\forall b, c \in A, (a \mid bc \implies a \mid b \vee a \mid c)$.

Si A es un dominio, todo primo es irreducible.

Irreducible en un dominio no implica primo.

Sean A un anillo conmutativo y $a, b \in A$:

1. $a = 0 \iff (a) = 0$.

2. $a \in A^* \iff (a) = A$.

3. $a \mid b \iff (b) \subseteq (a) \iff b \in (a)$.

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

5. a es primo si y sólo si (a) es un ideal primo no nulo de A.

6. Si A es un dominio, a es irreducible si y sólo si (a) es maximal entre los ideales principales no nulos de A, es decir, si $(a) \neq 0, A$ y $\forall b \in A, ((a) \subseteq (b) \neq A \implies (a) = (b))$.

Dados un anillo conmutativo A y $S \subseteq A$, $a \in A$ es un **máximo común divisor** de S en A, $a = \text{mcd}S$, si divide a cada elemento de S y es múltiplo de cada elemento que cumple esto, y es un **mínimo común múltiplo** de S en A, $a = \text{mcm}S$, si es múltiplo de cada elemento de S y divide a cada elemento que cumple esto. Para $a, b \in A$:

1. $a = \text{mcd}S$ si y solo si (a) es el menor ideal principal de A que contiene a S. En particular, si $(a) = (S)$, $a = \text{mcd}S$.

2. $a = \text{mcm}S$ si y sólo si (a) es el mayor ideal principal de A contenido en $\bigcap_{s \in S}(s)$. En particular, si $(a) = \bigcap_{s \in S}(s)$, $a = \text{mcm}S$.

3. Si $a = \text{mcd}S$, $b = \text{mcd}S$ si y sólo si a y b son asociados en A.

4. Si $a = \text{mcm}S$, $b = \text{mcm}S$ si y sólo si a y b son asociados en A.

5. Si a divide a todo elemento de S y $a \in (S)$, entonces $a = \text{mcd}S$. En tal caso llamamos **identidad de Bézout** a una expresión de la forma $a = a_1 s_1 + \cdots + a_n s_n$ con $a_1, \ldots, a_n \in A$ y $s_1, \ldots, s_n \in S$, que existe porque $a \in (S)$.

6. $\text{mcd}S = 1$ si y sólo si los únicos divisores comunes de los elementos de S son las unidades de A.

7. Si $1 \in (S)$, $\text{mcd}S = 1$.

2.3. Dominios de factorización única

Dado un dominio D, una **factorización en producto de irreducibles** de $a \in D$ es una expresión de la forma $a = up_1 \cdots p_n$, donde u es una unidad de D y $p_1, \ldots, p_n$ son irreducibles en D. Dos factorizaciones en producto de irreducibles de $a \in D$, $a = up_1 \cdots p_m$ y $a = vq_1 \cdots q_n$, son **equivalentes** si $m = n$ y existe una permutación σ de $\mathbb{N}_n := \{1, \ldots, n\}$ tal que para $k \in \mathbb{N}_n$, p_k y $q_{\sigma(k)}$ son asociados, en cuyo caso u y v también lo son.

D es un **dominio de factorización** (**DF**) si todo elemento no nulo de D admite una factorización en producto de irreducibles, y es un **dominio de factorización única** (**DFU** o **UFD**) si, además, todas las factorizaciones de un mismo elemento son equivalentes.

1. **Teorema Fundamental de la Aritmética:** $\mathbb{Z}$ es un DFU.

2. Dado $m \in \mathbb{Z}^+$, $\mathbb{Z}[\sqrt{m}]$ es un DF.

Un dominio D es un DFU si y sólo si todo elemento no nulo de D es producto de una unidad por primos, si y sólo si D es un dominio de factorización en el que todo elemento irreducible es primo.

$1 \implies 2]$ Todo elemento no nulo de D puede expresarse como producto de una unidad por irreducibles. Sea entonces $p \in D$ irreducible, queremos ver que p es primo, esto es, que para $a, b \in D$ con $p \mid ab$, $p \mid a$ o $p \mid b$. Para $a = 0$ o $b = 0$ esto es claro, por lo que suponemos $a, b \neq 0$. Sea $t \in D$ con $pt = ab$, si $t = up_1 \cdots p_n$, $a = vq_1 \cdots q_m$ y $b = wr_1 \cdots r_k$ son las factorizaciones en irreducibles de t, a y b, entonces $upp_1 \cdots p_n = (vw)q_1 \cdots q_m r_1 \cdots r_k$, y por la unicidad de la factorización, p es asociado de algún q_i, y entonces $p \mid a$, o de algún r_i, y entonces $p \mid b$.

$2 \implies 3$] Como los primos en un dominio son irreducibles, D es un DF. Sean $p \in D$ irreducible, $u \in D^*$ y $q_1, \dots, q_k \in D$ primos con $p = uq_1 \cdots q_k$. Entonces o q_1 es unidad o lo es $uq_2 \cdots q_k$, pero como q_1 no lo es, debe ser $k = 1$. De aquí, p y q_1 son asociados, y como q_1 es primo, p también.

$3 \implies 1$] Sean $d = up_1 \cdots p_n = vq_1 \cdots q_m$ factorizaciones en producto de irreducibles de un cierto $d \neq 0$ y podemos suponer $n \leq m$. Si $n = 0$, entonces d es unidad y, como los divisores de unidades son unidades, $m = 0$ y las factorizaciones son equivalentes. Si $n > 0$, supuesto esto probado para $n - 1$, como p_n es primo, divide a algún q_i y, como q_i es irreducible, existe $w \in D^*$ con $p_n w = q_i$ y ambos son asociados. Podemos suponer $i = m$, y entonces $up_1 \cdots p_n = vq_1 \cdots q_{m-1} w p_n$ y $up_1 \cdots p_{n-1} = (vw)q_1 \cdots q_{m-1}$. Por la hipótesis de inducción, $n - 1 = m - 1$, con lo que $n = m$, y existe una permutación τ en $\mathbb{N}_{n-1}$ tal que p_i y $q_{\tau(i)}$ son asociados para cada i, y obviamente τ se extiende a una permutación σ de $\mathbb{N}_n$ con esta propiedad. Por tanto las factorizaciones iniciales son equivalentes.

2.4. Dominios de ideales principales

Un **dominio de ideales principales** (**DIP** o **PID**) es un dominio en que todos los ideales son principales. Si D es un DIP y $a \in D \setminus (D^* \cup \{0\})$, a es irreducible si y solo si (a) es un ideal maximal, si y solo si $\frac{D}{(a)}$ es un cuerpo, si y solo si a es primo, si y solo si (a) es un ideal primo, si y solo si $\frac{D}{(a)}$ es un dominio.

$1 \iff 2$] Sabemos que a es irreducible si y solo si (a) es maximal entre los ideales principales no nulos de D, pero en un DIP estos son todos los ideales no nulos de D, y como $a \neq 0$, $(a) \neq 0$.

$2 \iff 3 \implies 6$] Visto.

$1 \impliedby 4 \iff 5 \iff 6$] Visto.

Todo DIP es un DFU. **Demostración:** Supongamos que existe $a \in D \setminus \{0\}$ que no admite factorización en irreducibles. Entonces, como a no es irreducible ni unidad, existen $x, y \in D \setminus (D^* \cup \{0\})$ con $a = xy$, y al menos x o y (por ejemplo x) no admite factorización, con lo que $(a) \subsetneq (x)$. Por inducción existe una sucesión $(a_n)_{n\in\mathbb{N}}$ en D de elementos que no admiten factorización con $(a_0) \subsetneq (a_1) \subsetneq \dots$. Sea $I \coloneqq (a_1, a_2, \dots) = \bigcup_{n\in\mathbb{N}}(a_n)$, como D es un DIP, existe $x \in D$ con $I = (x)$, luego $x \in \bigcup_{n\in\mathbb{N}}(a_n)$ y existe n con $x \in (a_n)$. Como además $a_n \in I = (x)$, $(a_n) = (x) = I$ y por tanto $(a_n) = (a_{n+1})\#$.

2.5. Dominios euclídeos

Dado un dominio $D \neq 0$, una función $\delta : D \setminus \{0\} \to \mathbb{N}$ es **euclídea** si cumple:

1. $\forall a, b \in D \setminus \{0\}, (a \mid b \implies \delta(a) \leq \delta(b))$.
2. $\forall a \in D, b \in D \setminus \{0\}, \exists q, r \in D : (a = bq + r \wedge (r = 0 \vee \delta(r) < \delta(b)))$.

Un **dominio euclídeo** es uno que admite una función euclídea.

1. El valor absoluto es una función euclídea en $\mathbb{Z}$.
2. El cuadrado del módulo complejo es una función euclídea en $\mathbb{Z}[i]$.

Sean δ una función euclídea en D, I un ideal de D y $a \in I \setminus \{0\}$, entonces

$$I = (a) \iff \forall x \in I \setminus \{0\}, \delta(a) \leq \delta(x).$$

Como **teorema**, todo dominio euclídeo es DIP.

Si δ es una función euclídea en D, un elemento $a \in D$ es una unidad si y sólo si $\delta(a) = \delta(1)$, si y sólo si $\forall x \in D \setminus \{0\}, \delta(a) \leq \delta(x)$.

2.6. Cuerpos de fracciones

Sean $D \neq 0$ un dominio y $X \coloneqq D \times (D \setminus \{0\})$, definimos la relación binaria

$$(a_1, s_1) \sim (a_2, s_2) : \iff a_1 s_2 = a_2 s_1.$$

Esta relación es de equivalencia.

Llamamos $a/s \coloneqq \frac{a}{s} \coloneqq [(a, s)] \in Q(D) \coloneqq X/\sim$, y las operaciones

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \qquad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2},$$

están bien definidas.

Para $a, b \in D$ y $s, t \in D \setminus \{0\}$:

1. $\frac{a}{s} = \frac{0}{1} \iff a = 0$.
2. $\frac{a}{s} = \frac{1}{1} \iff a = s$.
3. $\frac{at}{st} = \frac{a}{s}$.
4. $\frac{a}{s} = \frac{b}{s} \iff a = b$.
5. $\frac{a}{s} + \frac{b}{s} = \frac{a+b}{s}$.

De aquí, $(Q(D), +, \cdot)$ es un cuerpo llamado **cuerpo de fracciones** o **de cocientes** de D cuyo cero es $\frac{0}{1}$ y cuyo uno es $\frac{1}{1}$.

$\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$. Es fácil ver que la función $u : D \to Q(D)$ dada por $u(a) \coloneqq a/1$ es un homomorfismo inyectivo, por lo que podemos ver a D como un subdominio de $Q(D)$ identificando a cada $a \in D$ con $a/1 \in Q(D)$.

Propiedad universal del cuerpo de fracciones: Dados un dominio D y $u : D \to Q(D)$ dada por $u(a) \coloneqq a/1$:

1. Sean K un cuerpo y $f : D \to K$ un homomorfismo inyectivo, el único homomorfismo de cuerpos $\tilde{f} : Q(D) \to K$ con $\tilde{f} \circ u = f$ viene dado por $\tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$.
2. Sean K un cuerpo no trivial y $g, h : Q(D) \to K$ homomorfismos que coinciden en D, entonces $g = h$.

3. Sean F un cuerpo no trivial y $v : D \to F$ un homomorfismo inyectivo tal que para todo cuerpo K y homomorfismo inyectivo $f : D \to K$ existe un único homomorfismo $\tilde{f} : F \to K$ con $\tilde{f} \circ v = f$, entonces existe un isomorfismo $\phi : F \to Q(D)$ con $\phi \circ v = u$.

Sean D un dominio, K un cuerpo no trivial y $f : D \to K$ un homomorfismo inyectivo, K contiene un subcuerpo isomorfo a $Q(D)$.

De aquí, para $m \in \mathbb{Z}$, $Q(\mathbb{Z}[\sqrt{m}]) \cong \mathbb{Q}[\sqrt{m}]$, lo que nos permite identificar los elementos de $Q(\mathbb{Z}[\sqrt{m}])$ con los de $\mathbb{Q}[\sqrt{m}]$.

Sea K un cuerpo no trivial, existe un subcuerpo K' de K llamado **subcuerpo primo** de K contenido en cualquier subcuerpo de K, y este es isomorfo a $\mathbb{Z}_p$ si la característica de K es un entero primo p o a $\mathbb{Q}$ en caso contrario.

Capítulo 3

Polinomios

Dado un anillo conmutativo A, llamamos $A[[X]]$ al anillo conmutativo de las sucesiones de elementos de A entendidas como **series de potencias** en una **indeterminada** X, $(a_n)_n = \sum_{n=0}^{\infty} a_n X^n$, con las operaciones

$$(a_n)_n + (b_n)_n := (a_n + b_n)_n; \qquad (a_n)_n (b_n)_n := \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_n .$$

Llamamos $A[X]$ al subanillo de $A[[X]]$ formado por las sucesiones con un número finito de elementos no nulos, a las que llamamos **polinomios** en X. A es un subanillo de $A[X]$ identificando los elementos de A con los **polinomios constantes**, de la forma $P(X) = a_0$. Dado un ideal I de A, $\{a_0 + a_1 X + \cdots + a_n X^n \in A[X] \mid a_0 \in I\}$ e $I[X] := \{a_0 + a_1 X + \cdots + a_n X^n \in A[X] \mid a_0, \ldots, a_n \in I\}$ son ideales de $A[X]$.

Dado $p := \sum_{k \in \mathbb{N}} p_k X^k \in A[X] \setminus \{0\}$, llamamos **grado** de p a $\operatorname{gr}(p) := \operatorname{máx}\{k \in \mathbb{N} \mid p_k \neq 0\}$, **coeficiente** de **grado** k de p a p_k, **coeficiente independiente** al de grado 0 y **coeficiente principal** al de grado $\operatorname{gr}(p)$. Un polinomio es **mónico** si su coeficiente princial es 1. El polinomio 0 tiene grado $-\infty$ por convención.

Un **monomio** es un polinomio de la forma aX^n con $a \in A$ y $n \in \mathbb{N}$. Todo polinomio en $A[X]$ se escribe como suma finita de monomios de distinto grado de forma única salvo orden.

Si $P, Q \in A[X] \setminus \{0\}$ tienen coeficientes principales respectivos p y q:

1. $\operatorname{gr}(P + Q) \leq \operatorname{máx}\{\operatorname{gr}(P), \operatorname{gr}(Q)\}$, con desigualdad estricta si y sólo si $\operatorname{gr}(P) = \operatorname{gr}(Q)$ y $p + q = 0$.

2. $\operatorname{gr}(PQ) \leq \operatorname{gr}(P) + \operatorname{gr}(Q)$, con igualdad si y sólo si $pq \neq 0$.

$A[X]$ no es un cuerpo. Es un dominio si y sólo si lo es A, en cuyo caso llamamos **cuerpo de las funciones racionales** sobre A al cuerpo de fracciones de $A[X]$.

3.1. Propiedad universal

Propiedad universal del anillo de polinomios (PUAP): Sean A un anillo y $u : A \to A[X]$ el homomorfismo inclusión:

1. Para cada homomorfismo de anillos conmutativos $f : A \to B$ y $b \in B$, el único homomorfismo $\tilde{f} : A[X] \to B$ tal que $\tilde{f}(X) = b$ y $\tilde{f} \circ u = f$ es

$$\tilde{f}\left(\sum_n p_n X^n\right) := \sum_n f(p_n) b^n.$$

2. $A[X]$ y u están determinados salvo isomorfismos por la propiedad universal: dados un homomorfismo de anillos $v : A \to P$ y $t \in P$ tales que, para cada homomorfismo de anillos $f : A \to B$ y $b \in B$, existe un único $\tilde{f} : P \to B$ tal que $\tilde{f} \circ v = f$ y $\tilde{f}(t) = b$, existe un isomorfismo $\phi : A[X] \to P$ tal que $\phi \circ u = v$ y $\phi(X) = t$.

Así:

1. Si A es un subanillo de B y $b \in B$, el **homomorfismo de sustitución** o **de evaluación** en b es $S_b : A[X] \to B$ dado por

$$S_b(p) := p(b) := \sum_n p_n b^n,$$

y su imagen es el subanillo generado por $A \cup \{b\}$, llamado $A[b]$. Todo $p \in A[X]$ induce una **función polinómica** $\hat{p} : B \to B$ dada por $\hat{p}(b) := S_b(p)$.

2. Dado $a \in A$, el homomorfismo de sustitución S_{X+a} es un automorfismo de $A[X]$ con inverso S_{X-a}.

3. Si A es un anillo conmutativo, $\frac{A[X]}{(X)} \cong A$.

4. Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo $\hat{f} : A[X] \to B[X]$ dado por

$$\hat{f}(p) = \sum_n f(p_n) X^n,$$

que es inyectivo o suprayectivo si lo es f.

5. Si A es un subanillo de B, $A[X]$ lo es de $B[X]$.

6. Si I es un ideal de A, el **homomorfismo de reducción de coeficientes módulo** I es $\tilde{\pi} : A[X] \to (A/I)[X]$ dado por

$$\tilde{\pi}(p) := \sum_n (p_n + I) X^n.$$

Su núcleo es $I[X]$, por lo que $(A/I)[X] \cong \frac{A[X]}{I[X]}$.

3.2. Raíces de polinomios

Sean $f, g \in A[X]$, si el coeficiente principal de g es invertible en A, existen dos únicos polinomios $q, r \in A[X]$, llamados respectivamente **cociente** y **resto** de la **división** de f entre g, tales que $f = gq + r$ y $\operatorname{gr}(r) < \operatorname{gr}(g)$, y se obtienen con el algoritmo 1. En particular, el grado es una función euclídea.

Entrada: Polinomios f y $g \neq 0$ con coeficiente principal de g invertible.
Salida: Cociente q y resto r de f entre g.
$m := \operatorname{gr}(g)$;
función `dividir(`f, acc`)` // acc acumula términos de q.
  $n := \operatorname{gr}(f)$;
  si $n < m$ **entonces** (acc, f);
  sinó `dividir(`$f - \frac{f_n}{g_m} X^{n-m} g, acc + \frac{f_n}{g_m} X^{n-m}$`)`;
fin
$q, r \leftarrow$ `dividir(`$f, 0$`)`;

Algoritmo 1: División de polinomios.

Teorema del resto: Dados $f \in A[X]$ y $a \in A$, el resto de f entre $X - a$ es $f(a)$. De aquí se obtiene el **teorema de Ruffini**, que dice que f es divisible por $X - a$ si y sólo si $f(a) = 0$, en cuyo caso a es una **raíz** de f.

Para $f \in A[X] \setminus \{0\}$ y $a \in A$, existe $m := \max\{k \in \mathbb{N} \mid (X-a)^k \mid f\}$. Llamamos a m **multiplicidad** de a en f, y a es raíz de f si y sólo si $m \geq 1$. Decimos que a es una **raíz simple** de f si $m = 1$ y que es una **raíz compuesta** si $m > 1$.

La multiplicidad de a en f es el único natural m tal que $f = (X-a)^m g$ para algún $g \in A[X]$ del que a no es raíz.

Si D es un dominio, $f \in D[X] \setminus \{0\}$, $a_1, \ldots, a_n$ son n elementos de D y $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}^{>0}$ con $(X - a_k)^{\alpha_k} \mid f$ para cada k, entonces $(X-a_1)^{\alpha_1} \cdots (X-a_n)^{\alpha_n} \mid f$, por lo que $\sum_{k=1}^{n} \alpha_k \leq \operatorname{gr}(f)$ y, en particular, la suma de las multiplicidades de las raíces de f, y el número de raíces, no son superiores a $\operatorname{gr}(f)$.

Principio de las identidades polinómicas: Sea D un dominio:

1. Para $f, g \in D[X]$, si las funciones polinómicas $f, g : D \to D$ coinciden en m elementos de D con $m > \operatorname{gr}(f), \operatorname{gr}(g)$, los polinomios f y g son iguales.

2. D es infinito si y sólo si cualquier par de polinomios distintos en $D[X]$ define dos funciones polinómicas distintas en D.

Como ejemplo de lo anterior, por el teorema pequeño de Fermat, dado un primo p, todos los elementos de $\mathbb{Z}_p$ son raíces de 0 y $X^p - X$.

Dado un anillo conmutativo A, definimos la **derivada** de $P := \sum_k a_k X^k \in A[X]$ como $P' := D(P) := \sum_{k \geq 1} k a_k X^{k-1}$, y escribimos $P^{(0)} := P$ y $P^{(n+1)} := P^{(n)\prime}$. Dados $a, b \in A$ y $P, Q \in A[X]$:

1. $(aP + bQ)' = aP' + bQ'$.

2. $(PQ)' = P'Q + PQ'$.

3. $(P^n)' = nP^{n-1}P'$.

Dados un dominio D de característica 0, $P \in D[X] \setminus \{0\}$ y $a \in D$, la multiplicidad de a en P es el menor $m \in \mathbb{N}_0$ con $P^{(m)}(a) \neq 0$.

3.3. Divisibilidad en anillos de polinomios

Dado un anillo A, $A[X]$ es un dominio euclídeo si y sólo si es un DIP, si y sólo si A es un cuerpo.

Sean D un dominio y $p \in D$:

1. p es irreducible en D si y sólo si lo es en $D[X]$.

   $\Longrightarrow$] Si hubiera $Q \in D[X]$ con $pQ = 1$ sería $\mathrm{gr}Q = 0$ y $Q \in D$, pero sabemos que p no es unidad en $D\#$. Entonces si $p = PQ$ con $P, Q \in D[X]$, como $P, Q \neq 0$, $\mathrm{gr}P = \mathrm{gr}Q = 0$, luego $P, Q \in D$ y uno de P o Q es unidad.

   $\Longleftarrow$] Se obtiene de que $D \subseteq D[X]$.

2. Si p es primo en $D[X]$, lo es en D.

   Sean $a, b \in D$ con $p \mid ab$, $p \mid a$ o $p \mid b$ en $D[X]$, pero si, por ejemplo, $pt = a$ para un $t \in D[X]$, entonces $\mathrm{gr}t = 0$ y $p \mid a$ en D, y para b es análogo.

3. Si D es un DFU, p es irreducible en D si y sólo si lo es en $D[X]$, si y sólo si es primo en D, si y sólo si lo es en $D[X]$.

   $3 \implies 1, 4 \implies 2]$ Por ser D y $D[X]$ dominios.

   $1 \implies 3]$ Por ser D un DFU.

   $1 \iff 2, 4 \implies 3]$ Son los puntos anteriores.

   $3 \implies 4]$ Si p es primo en D, sean $a := a_0 + \cdots + a_n X^n$, $b := b_0 + \cdots + b_m X^m \in D[X]$ tales que $p \nmid a, b$, i el menor índice con $p \nmid a_i$ y j el menor índice con $p \nmid b_j$, el coeficiente de grado $i + j$ de ab es $a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0$, y p divide a todos los sumandos de esta fórmula salvo a $a_i b_j$ por ser p primo en D, de donde $p \nmid ab$ y por tanto p es primo en $D[X]$.

Sea D un DFU, definimos $\varphi : D \setminus 0 \to \mathbb{N}$ tal que $\varphi(a)$ es el número de factores irreducibles en la factorización por irreducibles de a en D, contando repetidos, y para $a, b \in D \setminus \{0\}$, $\varphi(ab) = \varphi(a) + \varphi(b)$ y $\varphi(a) = 0 \iff a \in D^*$.

Si D es un DFU, K es su cuerpo de fracciones y $f \in D[X]$ es irreducible en $D[X]$, es irreducible en $K[X]$. **Demostración:** Si no lo fuera, existirían $G, H \in K[X]$ con $f = GH$ y $\mathrm{gr}(G), \mathrm{gr}(H) > 0$, pues los elementos de grado 0 son nulos o unidades. Si tomamos representantes de los coeficientes de G y $b \in D \setminus 0$ múltiplo común de los denominadores en estos representantes, $g := bG \in D[X]$, y si hacemos lo mismo con H obtenemos un $c \in D \setminus \{0\}$ con $h := cH \in D[X]$. Entonces $bcf = gh$, y basta ver que existen $g', h' \in D[X]$ con $f = g'h'$, $\mathrm{gr}(g') = \mathrm{gr}(g)$ y $\mathrm{gr}(h') = \mathrm{gr}(h)$, pues entonces f no es irreducible en $D[X]\#$. Para $\varphi(bc) = 0$, podemos tomar $g' := (bc)^{-1} g$ y $h' := h$. Si $n := \varphi(bc) > 0$, probado esto para $\varphi(bc) = n - 1$, existen $p, d \in D$ con $bc = pd$ y p primo, luego $p \mid bcf = gh$ en $D[X]$ y, por estar en un DFU, $p \mid g$. Sea entonces $\tilde{g} \in D[X]$ con $g = p\tilde{g}$, y por tanto $\mathrm{gr}(g) = \mathrm{gr}(\tilde{g})$, es $pdf = bcf = gh = p\tilde{g}h$ y $df = \tilde{g}h$, y como $\varphi(d) = \varphi(bc) - 1 = n - 1$, existen $g', h' \in D[X]$ con $f = g'h'$, $\mathrm{gr}(g') = \mathrm{gr}(\tilde{g}) = \mathrm{gr}(g)$ y $\mathrm{gr}(h') = \mathrm{gr}(h)$.

Como **teorema**, D es un DFU si y sólo si lo es $D[X]$.

$\Longrightarrow$] Primero vemos que todo $a \coloneqq a_0+\cdots+a_nX^n \in D[X]$ con $a_n \neq 0$ no invertible es producto de irreducibles. Si $n+\varphi(a_n)=0$, a es unidad. Para $n+\varphi(a_n)=1$, tanto si $n=0$ y $\varphi(a_n)=1$ como si $n=1$ y $\varphi(a_n)=0$, a sería irreducible. Supongamos que $n+\varphi(a_n)>1$ y que esto se cumple para valores de $n+\varphi(a_n)$ menores. Si a es irreducible o si $n=0$ es obvio. De lo contrario existen $b \coloneqq b_0+\cdots+b_mX^m, c \coloneqq c_0+\cdots+c_kX^k \in D[X]$ no invertibles ni unidades con $b_m, c_k \neq 0$, luego $0 < m+\varphi(b_m), k+\varphi(c_k) < m+k+\varphi(b_m)+\varphi(c_k) = n+\varphi(a_n)$, y aplicando la hipótesis de inducción a b y c y «pegando» las factorizaciones se obtiene el resultado.

Queda ver que todo irreducible f de $D[X]$ es primo. Para $\operatorname{gr}(f)=0$ ya lo tenemos. De lo contrario, sean $g,h \in D[X]$ con $f \mid gh$, entonces $f \mid gh$ en $K[X]$, y f es irreducible y por tanto primo en $K[X]$. Si, por ejemplo, $f \mid g$ en $K[X]$, existe $G \in K[X]$ con $g=fG$, y queda ver que $G \in D[X]$, para lo cual, si $a \in D$ cumple $aG \in D[X]$ con $\varphi(a)$ mínimo, basta ver que $\varphi(a)=0$. Supongamos $\varphi(a)>0$ y sean $p, b \in D$ con $a=pb$ y p primo, con lo que $p \mid ag = afG$ en $D[X]$. Si fuera $p \mid f$, sería $p \mid f_k$ para cada k y, como $\operatorname{gr}(f) \geq 1$, f no sería irreducible#, luego $p \mid aG$ en $D[X]$. Sea $h \in D[X]$ con $aG=ph$, entonces $pbG=ph$ y $bG=h \in D[X]$, pero $\varphi(b)<\varphi(a)$, luego $\varphi(a)$ no es mínimo.#

$\Longleftarrow$] D es un dominio y cada $a \in D \setminus (D^* \cup \{0\})$ es producto de irreducibles de $D[X]$, que tendrán grado 0 por tenerlo a y serán primos por ser $D[X]$ un DFU, por lo que serán también primos en D. Por tanto D es un DFU.

Si D es un DFU y K es su cuerpo de fracciones, definimos la relación de equivalencia en K $x \sim y :\iff \exists u \in D^* : y = ux$, con lo que $[x] = xD^*$ y, en particular, si $x \in D$, $[x]$ es el conjunto de los asociados de x en D. Definimos $\cdot : K \times (K/\sim) \to K/\sim$ como $a(bD^*) = (ab)D^*$. Esto está bien definido. Además, $a(b(cD^*)) = (ab)(cD^*)$.

Definimos $c : K[X] \to K/\sim$ tal que, para $p \coloneqq \sum_{k\geq 0} p_kX^k \in D[X]$, $c(p) \coloneqq \{x \mid x = \operatorname{mcd}_{k\geq 0} p_k\}$, y para $p \in K[X]$, si $a \in D \setminus \{0\}$ cumple $ap \in D[X]$, $c(p) \coloneqq a^{-1}c(ap)$. Esto está bien definido. Si $c(p)=aD^*$, a es el **contenido** de p ($a=c(p)$).

Para $a \in K$ y $p \in K[X]$:

1. Si $a \in D$ y $p \in D[X]$, $a \mid p$ en $D[X]$ si y sólo si $a \mid c(p)$ en D.
2. $c(ap) = ac(p)$.
3. $p \in D[X] \iff c(p) \in D$.

Un polinomio p es **primitivo** si $c(p)=1$, esto es, si $p \in D[X]$ y $\operatorname{mcd}_k p_k = 1$.

Lema de Gauss: Para $f,g \in D[X]$, $c(fg)=c(f)c(g)$, y en particular fg es primitivo si y sólo si f y g lo son. **Demostración:** $f' \coloneqq f/c(f)$ es primitivo, pues $c(f') = c(c(f)^{-1}f) = c(f)^{-1}c(f) = 1$, y análogamente $g' \coloneqq g/c(g)$ es primitivo, luego $fg = c(f)c(g)f'g'$ y basta ver que $f'g' \in D[X]$ es primitivo. Si no lo fuera, $c(f'g')$ tendría un divisor irreducible, y por tanto primo, p en D, luego $p \mid f'g'$ y entonces $p \mid f'$ o $p \mid g'$, con lo que $p \mid c(f') = 1$ o $p \mid c(g') = 1$#.

Dado $f \in D[X] \setminus D$ primitivo, f es irreducible en $D[X]$ si y sólo si lo es en $K[X]$, si y sólo si $\forall G,H \in K[X], (f = GH \implies \operatorname{gr}(G)=0 \vee \operatorname{gr}(H)=0)$, si y sólo si $\forall g,h \in D[X], (f=gh \implies \operatorname{gr}(g)=0 \vee \operatorname{gr}(h)=0)$.

$1 \implies 2 \implies 3$] Visto.

$3 \implies 4]$ Obvio.

$4 \implies 1]$ Como f es primitivo, sus únicos divisores de grado 0 son unidades, por lo que para $g, h \in D[X]$ con $f = gh$, g o h es unidad.

De aquí que si D es un DFU con cuerpo de fracciones K, los irreducibles de $D[X]$ son precisamente los de D y los polinomios primitivos de $D[X] \setminus D$ irreducibles en $K[X]$.

3.4. Factorización en el anillo de polinomios de un DFU

Sean K un cuerpo y $f \in K[X]$:

1. Si $\mathrm{gr}(f) = 1$, f es irreducible en $K[X]$.
2. Si $\mathrm{gr}(f) > 1$ y f tiene una raíz en K, f no es irreducible en $K[X]$.
3. Si $\mathrm{gr}(f) \in \{2, 3\}$, f es irreducible en $K[X]$ si y sólo si no tiene raíces en K.

Si D es un DFU con cuerpo de fracciones K, $f \coloneqq \sum_k a_k X^k \in D[X]$ y $n \coloneqq \mathrm{gr}(f)$, todas las raíces de f en K son de la forma $\frac{r}{s}$ con $r \mid a_0$ y $s \mid a_n$.

Criterio de reducción: Sean $\phi : D \to K$ un homomorfismo de anillos donde D es un DFU y K es un cuerpo, $\hat{\phi} : D[X] \to K[X]$ el homomorfismo inducido por ϕ y f un polinomio primitivo de $D[X] \setminus D$, si $\hat{\phi}(f)$ es irreducible en $K[X]$ y $\mathrm{gr}(\hat{\phi}(f)) = \mathrm{gr}(f)$, entonces f es irreducible en $D[X]$.

En particular, si $p \in \mathbb{Z}$ es primo, $f \coloneqq \sum_k a_k X^k \in \mathbb{Z}[X]$ es primitivo, $n \coloneqq \mathrm{gr}(f)$, $p \nmid a_n$ y f es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Z}[X]$.

Criterio de Eisenstein: Sean D un DFU, $f \coloneqq \sum_k a_k X^k \in D[X]$ primitivo y $n \coloneqq \mathrm{gr} f$, si existe un irreducible $p \in D$ tal que $\forall k \in \{0, \ldots, n-1\}, p \mid a_k$ y $p^2 \nmid a_0$, entonces f es irreducible en $D[X]$.

Así:

1. Si $a \in \mathbb{Z}$ y existe $p \in \mathbb{Z}$ cuya multiplicidad en a es 1, $X^n - a$ es irreducible.
2. Para $n \geq 3$, llamamos **raíces n-ésimas de la unidad** o **de 1** a las raíces de $X^n - 1$ en $\mathbb{C}$, que son los n vértices del n-ágono regular inscrito en el círculo unidad de $\mathbb{C}$ con un vértice en el 1. $X^n - 1 = (X-1)\Phi_n(X)$, donde $\Phi_n(X) \coloneqq X^{n-1} + X^{n-2} + \cdots + X + 1$ es el **n-ésimo polinomio ciclotómico** y sus raíces en $\mathbb{C}$ son las raíces n-ésimas de 1 distintas de 1. En $\mathbb{Q}$, $X + 1 \mid \Phi_4(X)$, pero si n es primo, $\Phi_n(X)$ es irreducible.

3.5. Polinomios en varias indeterminadas

Dados un anillo conmutativo A y $n \geq 2$, definimos el **anillo de polinomios** en n indeterminadas con coeficientes en A como $A[X_1, \ldots, X_n] \coloneqq A[X_1, \ldots, X_{n-1}][X_n]$. Llamamos **indeterminadas** a los símbolos $X_1, \ldots, X_n$ y **polinomios en n indeterminadas** a los elementos de $A[X_1, \ldots, X_n]$. Dados un anillo conmutativo A y $n \in \mathbb{N}^*$:

1. $A[X_1, \ldots, X_n]$ no es un cuerpo.
2. $A[X_1, \ldots, X_n]$ es un dominio si y sólo si lo es A.

3. Si A es un dominio, $A[X_1,\dots,X_n]^* = A^*$.

4. $A[X_1,\dots,X_n]$ es un DFU si y sólo si lo es A.

5. $A[X_1,\dots,X_n]$ es un DIP si y sólo si $n=1$ y A es un cuerpo.

Dados $a \in A$ e $i := (i_1,\dots,i_n) \in \mathbb{N}^n$, llamamos a $aX_1^{i_1}\cdots X_n^{i_n} \in A[X_1,\dots,X_n]$ **monomio** de **tipo** i y coeficiente a. Todo $p \in A[X_1,\dots,X_n]$ se escribe de forma única como suma de monomios de distinto tipo,

$$p := \sum_{i\in\mathbb{N}^n} p_i X_1^{i_1}\cdots X_n^{i_n},$$

con $p_i = 0$ para casi todo $i \in \mathbb{N}^n$.

PUAP en n indeterminadas: Sean A un anillo conmutativo, $n \in \mathbb{N}^*$ y $u : A \to A[X_1,\dots,X_n]$ la inclusión:

1. Dados un homomorfismo de anillos $f : A \to B$ y $b_1,\dots,b_n \in B$, existe un único homomorfismo de anillos $\tilde{f} : A[X_1,\dots,X_n] \to B$ tal que $\tilde{f}\circ u = f$ y $\tilde{f}(X_k) = b_k$ para $k \in \{1,\dots,n\}$.

2. Dados un anillo conmutativo P, $T_1,\dots,T_n \in P$ y un homomorfismo $v : A \to P$ tales que, dados un homomorfismo de anillos $f : A \to B$ y $b_1,\dots,b_n \in B$, existe un único homomorfismo $\tilde{f} : P \to B$ tal que $\tilde{f}\circ v = f$ y $\tilde{f}(T_k) = b_k$ para $k \in \{1,\dots,n\}$, existe un isomorfismo $\phi : A[X_1,\dots,X_n] \to P$ tal que $\phi\circ u = v$ y $\phi(X_k) = T_k$ para cada $k \in \{1,\dots,n\}$.

Así:

1. Dados dos anillos conmutativos $A \subseteq B$ y $b_1,\dots,b_n \in B$, el **homomorfismo de sustitución** $S : A[X_1,\dots,X_n] \to B$ viene dado por $p(b_1,\dots,b_n) := S(p) := \sum_{i\in\mathbb{N}^n} p_i b_1^{i_1}\cdots b_n^{i_n}$. Su imagen es el subanillo de B generado por $A\cup\{b_1,\dots,b_n\}$, $A[b_1,\dots,b_n]$, y dados dos homomorfismos de anillos $f,g : A[b_1,\dots,b_n] \to C$, $f = g$ si y sólo si $f|_A = g|_A$ y $f(b_k) = g(b_k)$ para todo k.

2. Sean A un anillo y σ una permutación de $\mathbb{N}_n$ con inversa $\tau := \sigma^{-1}$, tomando $B = A[X_1,\dots,X_n]$ y $b_k = X_{\sigma(k)}$ en el punto anterior obtenemos un automorfismo $\hat{\sigma}$ en $A[X_1,\dots,X_n]$ con inversa $\hat{\tau}$ que permuta las indeterminadas.

3. $A[X_1,\dots,X_n,Y_1,\dots,Y_m] \cong A[X_1,\dots,X_n][Y_1,\dots,Y_m] \cong A[Y_1,\dots,Y_m][X_1,\dots,X_n]$, por lo que en la práctica no distinguimos entre estos anillos.

4. Todo homomorfismo de anillos conmutativos $f : A \to B$ induce un homomorfismo $\hat{f} : A[X_1,\dots,X_n] \to B[X_1,\dots,X_n]$ dado por $\hat{f}(p) := \sum_{i\in\mathbb{N}^n} f(p_i)X_1^{i_1}\cdots X_n^{i_n}$.

Llamamos **grado** de un monomio $aX_1^{i_1}\cdots X_n^{i_n}$ a $i_1+\cdots+i_n$, y grado de $p \in A[X_1,\dots,X_n]\setminus 0$, $\operatorname{gr}(p)$, al mayor de los grados de los monomios no nulos en la expresión por monomios de p. Entonces $\operatorname{gr}(p+q) \le \max\{\operatorname{gr}(p),\operatorname{gr}(q)\}$ y $\operatorname{gr}(pq) \le \operatorname{gr}(p)+\operatorname{gr}(q)$.

Un polinomio es **homogéneo** de grado n si es suma de monomios de grado n. Todo polinomio se escribe de modo único como suma de polinomios homogéneos de distintos grados, sin más que agrupar los monomios de igual grado en la expresión como suma de monomios. Así, si D es un dominio, $\operatorname{gr}(pq) = \operatorname{gr}(p)+\operatorname{gr}(q)$ para cualesquiera $p,q \in D[X_1,\dots,X_n]$.

Capítulo 4

Grupos

Podemos hablar de un grupo G con:

- **Notación multiplicativa**: Llamamos a la operación $\cdot$, aunque podemos omitirla. Llamamos 1 al neutro y a^{-1} al simétrico de $a \in G$. Definimos $a^0 := 1$ y, para $n \in \mathbb{N}$, $a^{n+1} := aa^n$ y $a^{-n} := (a^n)^{-1} = (a^{-1})^n$.
- **Notación aditiva**: Solo para grupos abelianos. Llamamos a la operación $+$. Llamamos 0 al neutro y $-a$ al simétrico de $a \in G$. Definimos $0a := 0$ y, para $n \in \mathbb{N}$, $(n+1)a = a + na$ y $(-n)a = -(na) = n(-a)$.

Llamamos **orden** de G al cardinal del conjunto. Algunos grupos:

1. Si A es un anillo, $(A, +)$ es su **grupo aditivo**, que es abeliano, y $(A^*, \cdot)$ es su **grupo de unidades**, que es abeliano cuando el anillo es conmutativo. Por ejemplo, si K es un cuerpo, $(\mathcal{GL}_n(K) = \mathcal{M}_n(K)^*, \cdot)$ es un grupo.
2. El **grupo simétrico** de un conjunto X es el conjunto S_X de las biyecciones $X \to X$ con la composición.
3. Dada una familia $(G_i)_{i\in I}$ de grupos, $\prod_{i\in I} G_i$ es un grupo con el producto componente a componente.
4. Llamamos **grupo cíclico** de orden $n \in \mathbb{N}^*$ a $C_n := \{1, a, a^2, \dots, a^{n-1}\}$ con la operación $a^i a^j := a^{[i+j]_n}$, donde $[x]_n$ es el resto de x entre n.
5. Si $n \in \mathbb{N}^*$, llamamos **grupo diédrico** de orden $2n$ a

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

   con la operación $(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) := a^{[i_1+(-1)^{j_1}i_2]_n}b^{[j_1+j_2]_2}$. Intuitivamente los elementos de D_n son los movimientos del plano que dejan fijos a un polígono regular de n lados, donde a es una rotación de ángulo $\frac{2\pi}{n}$ y b es una cierta simetría.
6. El **grupo diédrico infinito** es $D_\infty := \{a^n, a^nb\}_{n\in\mathbb{Z}}$ con

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

7. Sea B un anillo conmutativo, $B^* \propto B \coloneqq B^* \times B$ es un grupo abeliano con la operación $(u,a)(v,b) = (uv, ub + va)$, y $(u,a)^n = (u^n, nu^{n-1}a)$.

4.1. Subgrupos

Si G es un grupo, $S \subseteq G$ es un subgrupo de G si y sólo si $1 \in S \wedge \forall a,b \in S, (ab, a^{-1} \in S)$, si y sólo si $S \neq \emptyset \wedge \forall a,b \in S, (ab, a^{-1} \in S)$, si y sólo si $1 \in S \wedge \forall a,b \in S, ab^{-1} \in S$, si y sólo si $S \neq \emptyset \wedge \forall a,b \in S, ab^{-1} \in S$.

Si S es un subgrupo de G escribimos $S \leq G$.

1. Si G es un grupo, G es el **subgrupo impropio** de G, y el resto de subgrupos son **propios**. El **subgrupo trivial** es $1 \coloneqq \{1\}$.

2. Si $(A,+)$ es el grupo aditivo de un anillo y B es un subanillo de A, $(B,+) \leq (A,+)$.

3. Los subgrupos de $(\mathbb{Z},+)$ son de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.

4. Dado un cuerpo K, $\mathcal{SL}_n(K) \coloneqq \mathcal{SO}_n(K)$ es un subgrupo de $(\mathcal{GL}_n(K), \cdot)$.

5. Si A es un anillo, el conjunto $\mathrm{Aut}(A)$ de los automorfismos de anillos de A es un subgrupo de S_A.

6. Si X es un espacio topológico, el conjunto de los homeomorfismos $X \to X$ es un subgrupo de S_X.

7. Si X es un espacio métrico, el conjunto de las **isometrías** (biyecciones que conservan distancias) $X \to X$ es un subgrupo de S_X.

8. Si $X \subseteq G$, $\langle X \rangle \coloneqq \{x_1^{n_1} \cdots x_m^{n_m}\}_{m \in \mathbb{N}, x_i \in X, n_i \in \mathbb{Z}}$ es el **subgrupo generado** por X, y es el menor subgrupo de G que contiene a X. Si $X = \{g\}$, decimos que $\langle g \rangle \coloneqq \langle X \rangle$ es el **grupo cíclico** generado por g. Un grupo G es **cíclico** si existe $g \in G$ tal que $G = \langle g \rangle$, en cuyo caso g es un **generador** de G. Por ejemplo, $(\mathbb{Z},+)$ y $(\mathbb{Z}_n,+)$ son grupos cíclicos generados por 1, y C_n y C_∞ son cíclicos generados por a.

9. Si $(G_i)_{i \in I}$ es una familia de grupos, $\bigoplus_{i \in I} G_i \coloneqq \{(g_i)_{i \in I} \in \prod_{i \in I} G_i \mid \{i \in I \mid g_i \neq 1\} \text{ es finito}\}$ es un subgrupo de $\prod_{i \in I} G_i$.

10. Dado un grupo G, el **centralizador** de x en G es el subgrupo $C_G(x) \coloneqq \{g \in G \mid gx = xg\}$, y el **centro** de G es el subgrupo abeliano $Z(G) \coloneqq \{g \in G \mid \forall x \in G, gx = xg\} = \bigcap_{x \in X} C_G(x)$. Si G es abeliano, $Z(G) = G$.

Dados $H \leq G$, definimos la relación de equivalencia en G

$$a \equiv_i b \text{ mód } H :\iff a^{-1}b \in H;$$

la clase de equivalencia de $a \in G$, llamada **clase lateral módulo H por la izquierda**, es $aH = \{ah\}_{h \in H}$, y llamamos $G/H \coloneqq G/(\equiv_i \text{ mód } H)$. Definimos también la relación de equivalencia en G

$$a \equiv_d b \text{ mód } H :\iff ab^{-1} \in H;$$

la clase de equivalencia de $a \in G$, llamada **clase lateral módulo H por la derecha**, es $Ha = \{ha\}_{h\in H}$, y llamamos $H\backslash G \coloneqq G/(\equiv_d \text{ mód } H)$. La función $\sigma : G/H \to H\backslash G$ dada por $\sigma(aH) \coloneqq Ha^{-1}$ es biyectiva, luego $|G/H| = |H\backslash G|$, y llamamos **índice** de H en G a $[G : H] \coloneqq |G/H|$.

Teorema de Lagrange: Si G es un grupo finito y $H \leq G$, $|G| = |H|[G : H]$. En particular, si $|G|$ es primo, los únicos subgrupos de G son 1 y G, G es cíclico y cualquier elemento suyo distinto de 1 es generador de G.

4.2. Subgrupos normales

Dados $A, B \subseteq G$, llamamos $AB \coloneqq \{ab\}_{a\in A,b\in B}$, y es fácil ver que esta operación es asociativa.

Un subgrupo $N \leq G$ es **normal** si $N\backslash G = G/N$, si y sólo si $\forall x \in G, Nx = xN$, si y sólo si $\forall x \in G, x^{-1}Nx = N$, si y sólo si $\forall x \in G, Nx \subseteq xN$, si y sólo si $\forall x \in G, xN \subseteq Nx$, si y sólo si $\forall a, b \in G, aNbN = abN$, si y sólo si $\forall a, b \in G, NaNb = Nab$.

Si $N \leq G$ es normal, escribimos $N \trianglelefteq G$, y si además es propio, escribimos $N \triangleleft G$. Si $N \trianglelefteq G$, G/N es un grupo, el **grupo cociente** de G **módulo** N.

1. Si $H \leq G$ está contenido en $Z(G)$, $H \trianglelefteq G$. En particular, en un grupo abeliano, todo subgrupo es normal.
2. Si I es un ideal de A, $(A, +)/I$ es el grupo aditivo del conjunto cociente.
3. Si $H \leq G$ tiene índice 2, es normal.
4. $\mathcal{SL}_n(\mathbb{R}) \trianglelefteq \mathcal{GL}_n(\mathbb{R})$.

Teorema de la correspondencia: Si $N \trianglelefteq G$, $H \mapsto H/N$ es una biyección entre el conjunto de los subgrupos de G que contienen a N y el de los subgrupos de G/N que conserva las inclusiones y la normalidad en ambas direcciones. **Demostración:** Basta seguir la prueba del teorema de correspondencia de anillos. Para la normalidad, si H es normal, para $gN \in G/N$ y $hN \in H/N$, como $g^{-1}hg \in H$, $(gN)^{-1}hNgN = g^{-1}NhNgN = g^{-1}hgN \in H/N$, y $H/N \trianglelefteq G/N$. Si H/N es normal, para $g \in G$ y $h \in H$, como $g^{-1}NhNgN = g^{-1}hgN \in H/N$, $g^{-1}hg \in H$, y $H \trianglelefteq G$.

4.3. Homomorfismos

Una función $f : G \to H$ entre dos grupos es un **homomorfismo de grupos** si $\forall a, b \in G, f(ab) = f(a)f(b)$. Si $G = H$, es un **endomorfismo**. Si es biyectiva, es un **isomorfismo**, y si además $G = H$, es un **automorfismo**. Si G es un grupo, el conjunto $\mathrm{Aut}(G)$ de los automorfismos de anillos de G es un subgrupo de S_G. Llamamos $\ker f \coloneqq f^{-1}(1)$.

Si $G \xrightarrow{f} H \xrightarrow{g} K$ son homomorfismos de grupos, $G' \leq G$, $H' \leq H$, $a, a_1, \ldots, a_n \in G$ y $m \in \mathbb{Z}$:

1. $f(1) = 1$.
2. $f(a)^{-1} = f(a^{-1})$.
3. $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$.

4. $f(a^m) = f(a)^m$.
5. Si f es un isomorfismo, $f^{-1} : H \to G$ también.
6. $g \circ f : G \to K$ es un homomorfismo de grupos.
7. $f^{-1}(H') \leq G$. Si además $H' \trianglelefteq H$, $f^{-1}(H') \trianglelefteq G$. En particular, $\ker f \trianglelefteq G$.
8. f es inyectivo si y sólo si $\ker f = 1$.
9. $f(G') \leq H$. En particular $f(G) \leq H$. Si además $G' \trianglelefteq G$ y f es suprayectiva, entonces $f(G') \trianglelefteq H$.

Algunos homomorfismos:

1. Si $H \leq G$, la inclusión $H \to G$ es un homomorfismo inyectivo.
2. Si $N \trianglelefteq G$, la **proyección canónica** $\pi : G \to G/N$ dada por $\pi(x) \coloneqq xN$ es un homomorfismo suprayectivo con núcleo N.
3. Dados dos grupos G y H, $f : G \to H$ dada por $f(a) \coloneqq 1_H$ es el **homomorfismo trivial** de G en H, con núcleo G.
4. Dado $a \in \mathbb{Z}$, $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(n) \coloneqq an$ es un endomorfismo de $(\mathbb{Z}, +)$.
5. Si G es un grupo y $x \in G$, $f : \mathbb{Z} \to G$ dada por $f(n) \coloneqq x^n$ es un homomorfismo, esto es, $x^{n+m} = x^n x^m$.
6. Dado $\alpha \in \mathbb{R}^+$, $f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ dada por $f(r) \coloneqq \alpha^r$ es un isomorfismo de grupos con inversa $f^{-1}(s) \coloneqq \log_\alpha s$.

Teoremas de isomorfía para grupos:

1. Si $f : G \to H$ es un homomorfismo de grupos, existe un único isomorfismo $\tilde{f} : G/\ker f \to \mathrm{Im} f$ tal que $f = i \circ \tilde{f} \circ p$, donde $i : \mathrm{Im} f \to H$ es la inclusión y $p : G \to G/\ker f$ es la proyección canónica. En particular,
$$\frac{G}{\ker f} \cong \mathrm{Im} f.$$
2. Si $N, H \trianglelefteq G$ con $N \subseteq H$, $H/N \trianglelefteq G/N$ y
$$\frac{G/N}{H/N} \cong G/H.$$
3. Si $H \leq G$ y $N \trianglelefteq G$, entonces $NH \leq G$, $N \cap H \trianglelefteq G$ y
$$\frac{H}{N \cap H} \cong \frac{NH}{N}.$$

Así:

1. Si $f : G \to H$ es un homomorfismo de grupos, $K \mapsto f(K)$ es una biyección entre los subgrupos de G que contienen a $\ker f$ y los subgrupos de $\mathrm{Im} f$.
2. $\mathbb{C}^*/\mathcal{C}(0,1) \cong \mathbb{R}^+$.
3. $\mathcal{GL}_n(\mathbb{R})/\mathcal{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.

En general, $H, K \leq G$ no implica $HK \leq G$.

4.4. Orden de un elemento

Llamamos **orden** de $a \in G$ al orden de $\langle a \rangle$, $|a| \coloneqq |\langle a \rangle|$, y escribimos $\langle a \rangle_n$ para referirnos a $\langle a \rangle$ indicando que tiene orden n. El orden de a divide al de G.

Sea $f : \mathbb{Z} \to G$ el homomorfismo dado por $f(n) \coloneqq a^n$, $\ker f = n\mathbb{Z}$ para algún $n \geq 0$. Si $n = 0$, f es inyectivo y $(\mathbb{Z}, +) \cong \langle a \rangle$, y en otro caso $\mathbb{Z}_n \cong \langle a \rangle$, con lo que $n = |a|$ y $a^n = 1 \iff |a| \mid n$. De aquí, $a^k = a^l \iff k \equiv l \text{ mód } n$, con lo que $|a|$ es el menor entero positivo con $a^n = 1$.

Si a tiene orden finito y $n > 0$,

$$|a^n| = \frac{|a|}{\text{mcd}\{|a|, n\}}.$$

Si $G = \langle a \rangle$:

1. Si G tiene orden infinito, $G \cong (\mathbb{Z}, +) \cong C_\infty$ y los subgrupos de G son los $\langle a^n \rangle$ con $n \in \mathbb{N}$.
2. Si $|G| = n$, $G \cong (\mathbb{Z}_n, +) \cong C_n$ y los subgrupos de G son exactamente uno de orden d por cada $d \mid n$, $\langle a^{n/d} \rangle_d$.
3. Todos los subgrupos y grupos cociente de G son cíclicos.

Así, si $p \in \mathbb{N}$ es primo, todos los grupos de orden p son isomorfos a $(\mathbb{Z}_p, +)$. Si $G = \langle g_1, \ldots, g_n \rangle$ y $N \trianglelefteq G$, $G/N = \langle g_1 N, \ldots, g_n N \rangle$.

Teorema chino de los restos para grupos:

1. Si G y H son subgrupos cíclicos de órdenes respectivos n y m, $G \times H$ es cíclico si y sólo si n y m son coprimos.

   $\Longrightarrow$] Si $d \coloneqq \text{mcd}\{n, m\} > 1$, entonces G tiene un subgrupo G' de orden d y H un subgrupo H' de orden d, con lo que $G' \times 1$ y $1 \times H'$ son subgrupos distintos de $G \times H$ del mismo orden, luego $G \times H$ no es cíclico.

   $\Longleftarrow$] $G \cong (\mathbb{Z}_n, +)$ y $H \cong (\mathbb{Z}_m, +)$, y por el teorema chino de los restos para anillos, $\mathbb{Z}_n \times \mathbb{Z}_m \cong \frac{\mathbb{Z}}{nm\mathbb{Z}} = \mathbb{Z}_{nm}$ como anillos, luego los grupos aditivos también son isomorfos y $G \times H \cong (\mathbb{Z}_n, +) \times (\mathbb{Z}_m, +) \cong (\mathbb{Z}_{nm}, +)$.

2. Si $g, h \in G$ tienen órdenes respectivos n y m coprimos y $gh = hg$, entonces $\langle g, h \rangle$ es cíclico de orden nm.

   La función $f : \mathbb{Z}_n \times \mathbb{Z}_m \to G$ dada por $f(i, j) \coloneqq g^i h^j$ es un homomorfismo de grupos con imagen $\langle g, h \rangle$. Si $f(i, j) = 1$, $a^i b^j = 1 \implies a^{-i} = b^j \in \langle g \rangle \cap \langle h \rangle$ pero por el teorema de Lagrange, el orden de $\langle g \rangle \cap \langle h \rangle$ divide a n y a m y por tanto a 1, luego $a^{-i} = b^j = 1$, $(i, j) = (0, 0)$ y f es inyectiva. Por tanto $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m \cong \text{Im} f = \langle g, h \rangle$ y $\langle g, h \rangle$ es cíclico de orden nm.

4.5. Acciones de grupos en conjuntos

Dados un grupo G y $a \in G$, llamamos **conjugado** de $g \in G$ por a a $g^a \coloneqq a^{-1} g a$, y conjugado de $X \subseteq G$ por a a $X^a \coloneqq \{x^a\}_{x \in X}$. Dos elementos $x, y \in G$ o conjuntos $x, y \subseteq G$ son **conjugados** en G si existe $a \in G$ con $x^a = y$.

Si $a \in G$, llamamos **automorfismo interno** definido por a al automorfismo $\iota_a : G \to G$ dado por $\iota_a(x) \coloneqq x^a$. Su inverso es $\iota_{a^{-1}}$. El conjugado por a de un subgrupo de G es otro subgrupo de G del mismo orden.

Vemos que $\forall g, a, b \in G, g^{ab} = (g^a)^b$, y con esto es fácil comprobar que la relación de ser conjugados es de equivalencia. Las clases de equivalencia se llaman **clases de conjugación** de G, y llamamos $a^G \coloneqq [a] = \{a^g\}_{g \in G}$.

Sea X un conjunto. Una **acción por la izquierda** de G en X es una función $\cdot : G \times X \to X$ tal que $\forall x \in X, (\forall g, h \in G, (gh) \cdot x = g \cdot (h \cdot x) \wedge 1 \cdot x = x)$, y una **acción por la derecha** de G en X es una función $\cdot : X \times G \to X$ tal que $\forall x \in X, (\forall g, h \in G, x \cdot (gh) = (x \cdot g) \cdot h \wedge x \cdot 1 = x)$.

Si $\cdot : G \times X \to X$ es una acción por la izquierda de G en X y $x \in X$, llamamos **órbita** de x en G a $G \cdot x \coloneqq \{g \cdot x\}_{g \in G}$ y **estabilizador** de x en G a $\mathrm{Estab}_G(x) \coloneqq \{g \in G \mid g \cdot x = x\}$. Si $\cdot : X \times G \to X$ es una acción por la derecha de G en X y $x \in X$, llamamos órbita de x en G a $x \cdot G \coloneqq \{x \cdot g\}_{g \in G}$ y estabilizador de x en G a $\mathrm{Estab}_G(x) \coloneqq \{g \in G \mid x \cdot g = x\}$. Las órbitas forman una partición de G.

1. Llamamos **acción por traslación a la izquierda** a la acción por la izquierda de G en G/H dada por $g \cdot xH = gxH$. Entonces $G \cdot xH = G/H$ y

   $$\mathrm{Estab}_G(xH) = \{g \in G \mid gxH = xH\} = \{g \in G \mid x^{-1}gx \in H\} = xHx^{-1} = H^{x^{-1}}.$$

   Análogamente llamamos **acción por traslación a la derecha** a la acción por la derecha de G en $H\backslash G$ dada por $Hx \cdot g = Hxg$.

2. Cuando $H = 1$, la acción de traslación es de G en G, con $G \cdot x = G$ y $\mathrm{Estab}_G(x) = 1$.

3. La **acción por conjugación** de G en G es la acción por la derecha $x \cdot g \coloneqq x^g$. Entonces $x \cdot G = x^G$ y $\mathrm{Estab}_G(x) = C_G(x)$.

4. Si S es el conjunto de subgrupos de G, la **acción por conjugación de G en sus subgrupos** es la acción por la derecha de G en S $H \cdot g = H^g$. El **normalizador** de un subgrupo H en G es $N_G(H) \coloneqq \mathrm{Estab}_G(H) = \{g \in G \mid H^g = H\}$, el mayor subgrupo de G que contiene a H como subgrupo normal.

5. Si $n \in \mathbb{N}$ y X es un conjunto, $\cdot : S_n \times X^n \to X^n$ dada por $\sigma \cdot (x_1, \ldots, x_n) \coloneqq (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ es una acción por la izquierda.

6. Sean $\cdot : G \times X \to X$ una acción por la izquierda, $H \leq G$ e $Y \subseteq X$, si $\forall h \in H, y \in Y, h \cdot y \in Y$, $\cdot|_{H \times Y}$ es una acción por la izquierda de H en Y.

Sean G un grupo actuando sobre un conjunto X, $x \in X$ y $g \in G$:

1. $\mathrm{Estab}_G(x) \leq G$.

2. $[G : \mathrm{Estab}_G(x)] = |G \cdot x|$. En particular, si G es finito, $|G \cdot x| \mid |G|$.

3. Si la acción es por la izquierda, $\mathrm{Estab}_G(g \cdot x) = \mathrm{Estab}_G(x)^{g^{-1}}$, y si es por la derecha, $\mathrm{Estab}_G(x \cdot g) = \mathrm{Estab}_G(x)^g$. En particular, si $x, g \in G$ y $H \leq G$, $C_G(x^g) = C_G(x)^g$ y $N_G(H^g) = N_G(H)^g$.

4. Si R es un conjunto irredundante de representantes de las órbitas, $|X| = \sum_{r \in R} |G \cdot r| = \sum_{r \in R} [G : \mathrm{Estab}_G(r)]$.

Así, si G es un grupo y $a \in G$, $|a^G| = [G : C_G(a)]$, y en particular a^G es unipuntual si y sólo si $a \in Z(G)$. **Ecuación de clases:** Si G es finito y $X \subseteq G$ contiene exactamente un elemento de cada clase de conjugación con al menos dos elementos, entonces $|G| = |Z(G)| + \sum_{x \in X} [G : C_G(x)]$.

Dado un número primo p, un **p-grupo** es un grupo en que todo elemento tiene orden potencia de p, y un grupo finito es un p-grupo si y sólo si su orden es potencia de p.

Si G es un p-grupo finito no trivial, $Z(G) \neq 1$.

Teorema de Cauchy: Si G es un grupo finito con orden múltiplo de un primo p, G tiene un elemento de orden p.

4.6. Teoremas de Sylow

Dados un grupo finito G y un número primo p, $H \leq G$ es un **p-subgrupo de Sylow** de G si es un p-grupo y $[G : H]$ es coprimo con p, si y sólo si es un p-grupo y $|H|$ es la mayor potencia de p que divide a $|G|$. Llamamos $s_p(G)$ al número de p-subgrupos de Sylow de G.

Teoremas de Sylow: Sean p un número primo y G un grupo finito de orden $n \coloneqq p^k m$ para ciertos $k, m \in \mathbb{N}$ con $p \nmid m$. Entonces:

1. G tiene al menos un p-subgrupo de Sylow, que tendrá orden p^k.

2. Si P es un p-subgrupo de Sylow de G y Q es un p-subgrupo de G, existe $g \in G$ tal que $Q \subseteq P^g$. En particular, todos los p-subgrupos de Sylow de G son conjugados en G.

3. $s_p(G) \mid m$ y $s_p(G) \equiv 1$ mód p.

Capítulo 5

Grupos abelianos finitos

5.1. Sumas directas

Dada una familia $(B_i)_{i\in I}$ de subgrupos de un grupo abeliano, llamamos **suma** de $(B_i)_{i\in I}$ a $\sum_{i\in I} B_i := \{\sum_{i\in I} b_i \mid b_i \in B_i, \{i \in I \mid b_i \neq 0\} \text{ es finito}\}$. Si $I = \{1,\dots,n\}$, llamamos $\sum_{i\in I} B_i =: B_1 + \cdots + B_n$.

La familia $(B_i)_{i\in I}$ es **independiente** si el 0 se expresa de forma única como suma de elementos de los B_i ($\forall i, b_i \in B_i \wedge \sum_{i\in I} b_i = 0 \implies \forall i, b_i = 0$), si y sólo si cada elemento de $\sum_{i\in I} B_i$ se expresa de forma única como suma de elementos de los B_i, si y sólo si para cada $j \in I$, $B_j \cap (\sum_{i\in I\setminus\{j\}} B_i) = 0$.

Cuando $(B_i)_{i\in I}$ es independiente, su suma se llama **suma directa**, $\bigoplus_{i\in I} B_i$. Si $I = \{1,\dots,n\}$, llamamos $\bigoplus_{i\in I} B_i =: B_1 \oplus \cdots \oplus B_n$.

1. En $(\mathbb{R}^*,\cdot)$, $\mathbb{R}^* = \langle -1\rangle \oplus \mathbb{R}^+$.
2. Si A y B son grupos abelianos, $A \times B = (A \times 0) \oplus (0 \times B)$.
3. Para cada $a \in \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z} = \langle (1,0)\rangle \oplus \langle (a,1)\rangle$.
4. En $\mathbb{Z}$ y $\mathbb{Q}$ no hay dos subgrupos no triviales independientes.

Si $\hat{B}_i := 0 \times \cdots \times 0 \times B_i \times 0 \times \cdots \times 0 \leq B_1 \times \cdots \times B_n$, entonces $B_1 \times \cdots \times B_n = \tilde{B}_1 \oplus \cdots \oplus \tilde{B}_n$, con $\hat{B}_i \cong B_i$, y $f : B_1 \times \cdots \times B_n \to B_1 \oplus \cdots \oplus B_n$ dada por $f(b_1,\dots,b_n) := b_1 + \cdots + b_n$ es un isomorfismo de grupos. Por ello identificamos $B_1 \oplus \cdots \oplus B_n$ con $B_1 \times \cdots \times B_n$.

Para $(B_i)_{i\in I}$, identificamos $\bigoplus_{i\in I} B_i$ con el subgrupo de $\prod_{i\in I} B_i$ de los $(b_i)_{i\in I}$ con $\{i \in I \mid b_i \neq 0\}$ finito.

5.2. Grupos indescomponibles y p-grupos

Un grupo abeliano no trivial es **indescomponible** si no es suma directa de dos subgrupos propios. Todo grupo abeliano finito no trivial es suma directa de grupos indescomponibles. $\mathbb{Z}$ y $\mathbb{Q}$ son indescomponibles.

Un grupo cíclico $\langle a\rangle_n$ es indescomponible si y sólo si tiene orden potencia de primo.

Dado un grupo G, llamamos **exponente** o **periodo** de G, $\mathrm{Exp}(G)$, al menor $n \in \mathbb{N}^*$ tal que $\forall g \in G, g^n = 1$, o a ∞ si este no existe. G es **periódico** o **de torsión** si todo elemento de G tiene orden finito.

Si un grupo es finito tiene periodo finito, y si tiene periodo finito es periódico. Los recíprocos no se cumplen. Todo p-grupo es periódico, pero no necesariamente finito.

Dados un grupo abeliano A y un primo p, el **subgrupo de p-torsión** de A es

$$t_p(A) := \{a \in A \mid \exists n \in \mathbb{N} : p^n a = 0\} = \{a \in A \mid |a| \text{ es potencia de } p\}.$$

Si A es finito, $t_p(A)$ es el mayor p-subgrupo de A.

Sean A un grupo abeliano finito y $p_1, \ldots, p_k$ los divisores primos de $|A|$, entonces

$$A = t_{p_1}(A) \oplus \cdots \oplus t_{p_k}(A)$$

con cada $t_{p_i}(A) \neq 0$.

Si $n := p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ es una factorización prima, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$, y cada factor cumple $\mathbb{Z}_{p_i^{\alpha_i}} \cong t_p(\mathbb{Z}_n)$. Si A es un grupo abeliano, $B \leq A$, $a \in A$, $n \in \mathbb{N}$ y $na = 0$, en A/B es $|a + B| \mid |a|$. En general estos órdenes no coinciden.

Un grupo abeliano finito es indescomponible si y solo si es un p-grupo cíclico.

Esto significa que todo grupo abeliano finito es suma directa de subgrupos cíclicos, cada uno con orden potencia de primo.

5.3. Descomposiciones primarias e invariantes

Una **descomposición primaria** o **indescomponible** de un grupo abeliano finito A es una expresión de la forma

$$\begin{aligned} A = &\langle a_{11} \rangle_{p_1^{\alpha_{11}}} \oplus \cdots \oplus \langle a_{1m_1} \rangle_{p_1^{\alpha_{1m_1}}} \oplus \\ &\cdots \oplus \\ &\langle a_{k1} \rangle_{p_k^{\alpha_{k1}}} \oplus \cdots \oplus \langle a_{km_k} \rangle_{p_k^{\alpha_{km_k}}}, \end{aligned}$$

donde $p_1 < \ldots < p_k$ son los primos que dividen a $|A|$ y $\alpha_{i1} \geq \cdots \geq \alpha_{im_i} \geq 1$ para cada $i \in \{1, \ldots, k\}$.

Como **teorema**, todo grupo abeliano tiene una descomposición primaria, que podemos obtener con el algoritmo 2.

Una **descomposición invariante** de un grupo abeliano finito A es una expresión $A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle$ tal que para $i \in \{2, \ldots, n\}$, $|a_i| \mid |a_{i-1}|$, y los $\langle a_i \rangle$ son no triviales. Entonces, el periodo de A es el orden de $\langle a_1 \rangle$.

Todo grupo abeliano finito tiene una descomposición invariante. **Demostración:** Sea A este grupo, si m es el máximo de sumandos en una fila de la descomposición primaria de A, añadiendo sumandos triviales al final de cada fila con menos de m sumandos hasta llegar a m, tenemos una expresión

$$A = \langle a_{11} \rangle_{p_1^{\alpha_1}} \oplus \cdots \oplus \langle a_{1m} \rangle_{p_1^{\alpha_{1m}}} \oplus \cdots \oplus \langle a_{k1} \rangle_{p_k^{\alpha_{k1}}} \oplus \cdots \oplus \langle a_{km} \rangle_{p_k^{\alpha_{km}}}$$

con $p_1 < \ldots < p_k$ primos y, para $i \in \{1, \ldots, k\}$, $\alpha_{i1} \geq \cdots \geq \alpha_{im} \geq 0$. Entonces, para $j \in \{1, \ldots, m\}$, sean $b_j := a_{1j} + \cdots + a_{kj}$ y $d_j := p_1^{\alpha_{1j}} \cdots p_k^{\alpha_{kj}}$, por el teorema chino de los

función `descomponer(`A`)`
  $F \leftarrow \{\}$;
  para *p divisor primo de* $|A|$ **hacer**
    $T \leftarrow t_p(A)$;
    Encontrar $a \in T$ con $|a| = \mathrm{Exp}(T)$;
    Añadir $\langle a \rangle$ a F;
    para C *en* `descomponer(`$T/\langle a \rangle$`)` **hacer**
      Dado un $\gamma \in C$, obtener $x \in \gamma$ tal que $|x| = |\gamma|$; // $\gamma = x + \langle a \rangle$
      Añadir $\langle x \rangle$ a F;
    fin
  fin
  devolver F;
fin

Algoritmo 2: Método general para obtener descomposiciones primarias.

restos, $\langle b_j \rangle_{d_j} = \langle a_{1j} \rangle_{p_1^{\alpha_{1j}}} \oplus \cdots \oplus \langle a_{kj} \rangle_{p_k^{\alpha_{kj}}}$, con lo que $A = \langle b_1 \rangle_{d_1} \oplus \cdots \oplus \langle b_m \rangle_{d_m}$, y esta es una descomposición invariante.

Dados dos grupos abelianos finitos A y B, una descomposición por suma directa de A y una de B son **semejantes** si existe una biyección entre los subgrupos en la descomposición de A y la de B que a cada subgrupo de A le asocia uno de B isomorfo. En particular, dos descomposiciones primarias son semejantes si y sólo si tienen el mismo número de filas, cada fila tiene el mismo número de sumandos y sumandos correspondientes tienen el mismo orden, y dos descomposiciones invariantes son semejantes si tienen el mismo número de sumandos y las mismas listas de órdenes.

Como **teorema**, si A es un grupo abeliano finito:

1. Todas las descomposiciones primarias de A son semejantes.

   Sea $A \coloneqq A_{11} \oplus \cdots \oplus A_{1m_1} \oplus \cdots \oplus A_{k1} \oplus \cdots \oplus A_{km_k}$ con $|A_{ij}| = p_i^{\alpha_{ij}}$ para ciertos $p_1 < \ldots < p_k$ y α_{ij} con $\alpha_{i1} \geq \cdots \geq \alpha_{im_i} \geq 1$ para cada i. Para cada i, $A_{i1} \oplus \cdots \oplus A_{im_i} = t_{p_i}(A)$, luego estos subgrupos están determinados por A y basta probar la afirmación cuando A es un p-grupo finito. En este caso, sean $A = A_1 \oplus \cdots \oplus A_n = B_1 \oplus \cdots \oplus B_m$ dos descomposiciones primarias de A con $|A_i| = p^{\alpha_i}$ y $|B_i| = p^{\beta_i}$ donde p es primo, $\alpha_1 \geq \cdots \geq \alpha_n \geq 1$ y $\beta_1 \geq \cdots \geq \beta_m \geq 1$. Como $p^{\alpha_1} = \mathrm{Exp}(A) = p^{\beta_1}$, $\alpha_1 = \beta_1$. Dado un cierto i, supongamos que $\alpha_j = \beta_j$ para $j \in \{1, \ldots, i-1\}$, y podemos suponer $\alpha_i \leq \beta_i$. Si C es un grupo cíclico de orden p^r y $s \in \mathbb{N}$, $p^s C = 0$ si y sólo si $s \geq r$, mientras que si $s \leq r$, $p^s C$ es cíclico de orden p^{r-s}. Entonces, si $q \coloneqq p^{\alpha_i}$, $qA_i, \ldots, qA_n = 0$, luego $qA \cong qA_1 \oplus \cdots \oplus qA_{i-1} \cong (qB_1 \oplus \cdots \oplus qB_{i-1}) \oplus (qB_i \oplus qB_m)$, y como $|qA_1 \oplus \cdots \oplus qA_{i-1}| = |qB_1 \oplus \cdots \oplus qB_{i-1}|$, $|qB_i \oplus \cdots \oplus qB_m| = 0$, con lo que $qB_i = p^{\alpha_i} B_i = 0$ y $\alpha_i \geq \beta_i$, luego $\alpha_i = \beta_i$.

2. Todas las descomposiciones invariantes de A son semejantes.

   Basta usar la correspondencia entre descomposiciones primarias e invariantes de la demostración de existencia de descomposiciones invariantes.

Sean A un grupo abeliano finito con descomposición primaria $A = \bigoplus_{i=1}^{n} \langle a_i \rangle_{k_i}$ y descomposición invariante $A = \bigoplus_{i=1}^{m} \langle a_i \rangle_{t_i}$, llamamos **lista de los divisores elementales** de A a $(k_1, \ldots, k_n)$, y **lista de los factores invariantes** de A a $(t_1, \ldots, t_m)$.

Teorema de estructura de grupos abelianos finitos:

1. Todo grupo abeliano finito tiene una descomposición primaria y una invariante.

2. Dos grupos abelianos finitos son isomorfos si y sólo si tienen descomposiciones primarias semejantes, si y sólo si tienen descomposiciones invariantes semejantes, si y sólo si tienen la misma lista de divisores elementales, si y sólo si tienen la misma lista de factores invariantes.

Un grupo abeliano es **finitamente generado** si es suma directa de una cantidad finita de grupos cíclicos, de orden finito o infinito. **Teorema de estructura de grupos abelianos finitamente generados:**

1. Todo grupo abeliano finitamente generado tiene una descomposición primaria y una invariante.

2. Dos grupos finitamente generados son isomorfos si y sólo si tienen descomposiciones primarias semejantes, si y sólo si tienen descomposiciones invariantes semejantes.

Así, a cada grupo abeliano finitamente generado le asociamos una lista de divisores elementales $(q; p_1^{\alpha_{11}}, \ldots, p_1^{\alpha_{1m_1}}, \ldots, p_k^{\alpha_{k1}}, \ldots, p_k^{\alpha_{km_k}})$ y una de factores invariantes $(q; d_1, \ldots, d_n)$, donde q es el número de sumandos cíclicos infinitos.

Capítulo 6

Grupos de permutaciones

Si A y B son conjuntos de igual cardinal, existe una biyección $f : A \to B$, y entonces $h : S_A \to S_B$ dada por $h(\sigma) \coloneqq f \circ \sigma \circ f^{-1}$ es un isomorfismo. Por tanto, las propiedades de S_A solo dependen del cardinal.

Nos centraremos en los grupos de permutaciones entre conjuntos finitos, S_n con $n \in \mathbb{N}$. Entonces representamos una $\sigma \in S_n$ como

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

6.1. Ciclos

Una $\sigma \in S_n$ **fija** un $i \in \mathbb{N}_n$ si $\sigma(i) = i$, y lo **cambia** o **mueve** en caso contrario. Llamamos $M(\sigma) \coloneqq \{i \in \mathbb{N}_n \mid \sigma(i) \neq i\}$, y es claro que $M(\sigma) = \emptyset \iff \sigma = 1$ y que $|M(\sigma)| \neq 1$. Dos permutaciones $\sigma, \tau \in S_n$ son **disjuntas** si lo son $M(\sigma)$ y $M(\tau)$.

Si σ y τ son permutaciones disjuntas, $\sigma\tau = \tau\sigma$ y $M(\sigma\tau) = M(\sigma) \cup M(\tau)$.

Un **ciclo** de **longitud** $s \in \{2, \ldots, n\}$ o **s-ciclo** es una permutación $\sigma \in S_n$ tal que $|M(\sigma)| = s$ y podemos ordenar sus elementos como $M(\sigma) = \{i_1, \ldots, i_s\}$ de forma que $\sigma(i_k) = i_{k+1}$ para $k \in \{1, \ldots, s-1\}$ y $\sigma(i_s) = i_1$. Denotamos este ciclo como

$$\sigma = (i_1\, i_2\, \ldots\, i_s).$$

Los 2-ciclos se llaman **transposiciones** o **trasposiciones**.

Dados $\sigma \coloneqq (i_1\, \ldots\, i_s) \in S_n$ y $t \in \{1, \ldots, s\}$:

1. $\sigma = (i_t\, \ldots\, i_s\, i_1\, \ldots\, i_{t-1})$.
2. $i_t = \sigma^{t-1}(i_1)$.
3. $|\sigma| = s$.

Como **teorema**, toda permutación $\sigma \neq 1$ se puede expresar de forma única salvo orden como producto de ciclos disjuntos. **Demostración:** Razonamos por inducción en $|M(\sigma)| \geq 2$. Para $M(\sigma) = \{i, j\}$, $\sigma = (i\, j)$, y si $\sigma = \tau_1 \cdots \tau_k$ con $\tau_1, \ldots, \tau_k$ ciclos disjuntos, como $M(\sigma) =$

$\sum_i M(\tau_i)$, $k = 1$. Supongamos que esto se cumple para toda permutación no identidad que mueve menos elementos que σ. Sean $i \in M(\sigma)$ e $(i_n)_n$ dada por $i_0 := i$ e $i_n := \sigma(i_{n-1})$, como los i_n toman valores en un conjunto finito, existen $0 \leq j < k$ con $i_j = i_k$, y podemos tomar $j = 0$ porque, si el menor j que se puede tomar es positivo, $i_{j-1} = \sigma^{-1}(i_j) = \sigma^{-1}(i_k) = i_{k-1}\#$. Tomamos el menor k positivo con $i_0 = i_k$, y entonces $\tau := (i_0 \dots i_{k-1})$ es un k-ciclo. Sea $\rho \in S_n$ dada por

$$\rho(j) := \begin{cases} j, & j \in \{i_0 \dots i_{k-1}\} \vee j \notin M(\sigma); \\ \sigma(j), & \text{en otro caso.} \end{cases}$$

Claramente τ y ρ son disjuntas, $|M(\rho)| = |M(\sigma)| - k < |M(\sigma)|$ y $\sigma = \tau\rho$, y por la hipótesis de inducción, $\rho =: \rho_1 \cdots \rho_l$ con $\rho_1, \dots, \rho_l$ disjuntos dos a dos. Además, $M(\tau) \cap M(\rho_i) \subseteq M(\tau) \cap M(\rho) = \emptyset$, luego $\sigma = \tau\rho_1 \cdots \rho_l$ es un producto de ciclos disjuntos. Para la unicidad, si $\sigma = \tau_1 \cdots \tau_m$ con $\tau_1, \dots, \tau_m$ ciclos disjuntos, $i_0 \in M(\tau_j)$ para un único $j \in \{1, \dots, m\}$, y podemos suponer $j = 1$. Entonces $\tau(i_0) = \sigma(i_0) = \tau_1(i_0)$, con lo que $\tau = \tau_1$ y por tanto $\rho = \tau_2 \cdots \tau_m$, y de la unicidad de la factorización de ρ se deduce la unicidad de la de σ.

El **tipo** de una permutación $\sigma \in S_n \setminus 1$ es la lista $[s_1, \dots, s_k]$ de las longitudes de los ciclos en su factorización en ciclos disjuntos, en orden creciente. El orden de σ es el mínimo común múltiplo de las componentes de su tipo. **Demostración:** Sean $\sigma = \tau_1 \cdots \tau_k$ la factorización de σ como producto de ciclos disjuntos, $s_i = |\tau_i|$ y $m \in \mathbb{N}$. Como los τ_i conmutan y, para cada i, $M(\tau_i^m) \subseteq M(\tau_i)$, la factorización de σ^m por ciclos disjuntos es $\sigma^m = \tau_1^m \cdots \tau_k^m$. Entonces $\sigma^m = 1$ si y solo si cada $\tau_i^m = 1$, si y sólo si $s_i \mid m$ para todo i, si y sólo si $\operatorname{mcm}\{s_1, \dots, s_m\} \mid m$.

Dada una permutación α y un ciclo $\tau := (i_1 \dots i_s)$, $\tau^\alpha = (\alpha^{-1}(i_1) \dots \alpha^{-1}(i_s))$, pues $\tau^\alpha = \alpha^{-1}(i_1 \dots i_s)\alpha = (\alpha^{-1}(i_1) \dots \alpha^{-1}(i_s))$. Como **teorema**, dos elementos de S_n son conjugados si y sólo si tienen el mismo tipo, luego las clases de conjugación están formadas por los elementos de igual tipo.

$\Longrightarrow$] Es fácil ver que, si τ_1 y τ_2 son ciclos disjuntos, $\alpha\tau_1\alpha^{-1}$ y $\alpha\tau_2\alpha^{-1}$ también lo son, luego si $\tau_1, \dots, \tau_k$ son ciclos disjuntos, $\alpha\tau_1 \cdots \tau_k\alpha^{-1} = (\alpha\tau_1\alpha^{-1}) \cdots (\alpha\tau_k\alpha^{-1})$, y entonces es claro que dos elementos conjugados de S_n tienen el mismo tipo.

$\Longleftarrow$] Si σ y σ' tienen el mismo tipo, las descomposiciones en producto de ciclos disjuntos tienen forma $\sigma =: \tau_1 \cdots \tau_k$ y $\sigma' =: \tau_1' \cdots \tau_k'$ con cada $|\tau_i| = |\tau_i'|$. Por tanto existen biyecciones $\alpha_i : M(\tau_i) \to M(\tau_i')$ que conservan la estructura de los ciclos, y como $|M(\sigma)| = |M(\sigma')|$, existe una biyección $\beta : \mathbb{N}_n \setminus M(\sigma) \to \mathbb{N}_n \setminus M(\sigma')$. Sea ahora $\alpha \in S_n$ dada por $\alpha(x) := \alpha_i(x)$ si $x \in M(\tau_i)$ y $\alpha(x) := \beta(x)$ si $x \notin M(\sigma)$, entonces $\tau_i' = \alpha\tau_i\alpha^{-1}$ para todo i y por tanto $\sigma' = \alpha\sigma\alpha^{-1}$.

Para $n \geq 2$, los siguientes conjuntos son generadores de S_n:

1. El de todos los ciclos.
2. El de todas las trasposiciones.
3. $\{(1\,2), (1\,3), \dots, (1\,n)\}$.
4. $\{(1\,2), (2\,3), \dots, (n-1\,n)\}$.
5. $\{(1\,2), (1\,2\,\dots\,n-1\,n)\}$.

Si p es primo y $H \leq S_p$ contiene una transposición y un p-ciclo, $H = S_p$.

Demostración: Podemos suponer que H contiene a $(1\,2)$ y un p-ciclo $\sigma = (a_1 \dots a_p)$, y podemos suponer $a_1 = 1$. Si $a_i = 2$, $\sigma^{i-1} = (1\,2\,b_3 \dots b_p)$, y como las propiedades de las permutaciones no varían por biyecciones en el conjunto permutado, podemos renombrar los b_i de forma que $b_i = i$. Entonces $(1\,2), (1\,2 \dots p) \in H$, luego $H = S_p$.

6.2. El grupo alternado

Dados $n \geq 2$ y $\sigma \in S_n$, existe un automorfismo de anillos $\hat{\sigma}$ en $\mathbb{Z}[X_1, \dots, X_n]$ dado por $\hat{\sigma}(k) = k$ para $k \in \mathbb{Z}$ y $\hat{\sigma}(X_i) = X_{\sigma(i)}$ para $i \in \{1, \dots, n\}$. Sea

$$P := \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

Si $i < j$, puede ocurrir:

- Que sea $\sigma(i) < \sigma(j)$, y entonces el factor $X_{\sigma(j)} - X_{\sigma(i)}$ aparece en $\hat{\sigma}(P)$ y P.
- Que sea $\sigma(i) > \sigma(j)$, y entonces el factor $X_{\sigma(j)} - X_{\sigma(i)}$ aparece en $\hat{\sigma}(P)$ pero en P aparece su opuesto, y decimos que σ **presenta una inversión** para el par (i, j).

Entonces $\sigma \in S_n$ es **par** si σ presenta un número par de inversiones, si y sólo si $\hat{\sigma}(P) = P$, y es **impar** si presenta un número impar de inversiones, si y sólo si $\hat{\sigma}(P) = -P$.

La **aplicación signo**, $\operatorname{sgn} : S_n \to \mathbb{Z}^*$ dada por $\hat{\sigma}(P) = \operatorname{sgn}(\sigma)P$, es un homomorfismo de grupos.

Propiedades:

1. $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$.
2. Toda transposición es impar.
3. Si $\tau_1, \dots, \tau_r$ son transposiciones, $\operatorname{sgn}(\tau_1 \cdots \tau_r) = (-1)^r$.
4. σ es par si y sólo si es producto de un número par de transposiciones.
5. Un ciclo de longitud s tiene signo $(-1)^{s-1}$.
6. La paridad de una permutación coincide con la del número de componentes pares de su tipo.

Llamamos **grupo alternado** en n elementos a $A_n := \ker \operatorname{sgn}$, el subgrupo de S_n de las permutaciones pares. A_n es un subgrupo normal de S_n, y para $n \geq 2$, $\frac{S_n}{A_n} \cong \{-1, 1\} \cong \mathbb{Z}_2$, $[S_n : A_n] = 2$ y $|A_n| = \frac{n!}{2}$.

Son generadores de A_n:

1. El conjunto de todos los productos de dos transposiciones.

   Toda permutación par es producto de un número par de transposiciones.

2. El conjunto de todos los 3-ciclos.

   Sean $(i\,j)$ y $(k\,l)$ dos transposiciones. Si son disjuntas, $(i\,j)(k\,l) = (j\,l\,k)(i\,k\,j)$. Si son iguales, el producto es 1. En otro caso podemos suponer $i = k$ y $j \neq l$, y entonces $(i\,j)(i\,l) = (i\,l\,j)$.

6.3. Teorema de Abel

Un grupo G no trivial es **simple** si sus únicos subgrupos normales son 1 y G. Así, un grupo abeliano es simple si y sólo si tiene orden primo.

Teorema de Abel: Si $n \geq 5$, A_n es un grupo simple.

Demostración: Sea $H \neq 1$ un subgrupo normal de A_n y veamos que $H = A_n$. Supongamos primero que H contiene un 3-ciclo σ, y veamos que cualquier otro 3-ciclo σ' está en H. Sabemos que existe $\alpha \in S_n$ tal que $\sigma' = \sigma^\alpha$, por tener σ y σ' el mismo tipo. Si α es par, $\alpha \in A_n$, luego $\sigma' \in A_n$ por la normalidad de σ en A_n. En otro caso, como σ solo cambia 3 elementos y $n \geq 5$, existe una transposición β disjunta con σ tal que $\sigma^\beta = \sigma$, luego $\sigma^{\beta\alpha} = (\sigma^\beta)^\alpha = \sigma^\alpha = \sigma'$, pero $\beta\alpha \in A_n$.

Queda probar que H contiene un 3-ciclo. Sea $\sigma \in H \setminus 1$ con $r := |M(\sigma)|$ mínimo, y queremos ver que $r = 3$. No puede ser $r = 1$ y, como σ es par, tampoco puede ser $r = 2$, luego $r \geq 3$. Si suponemos $r > 3$, hay dos posibilidades:

1. Que en la factorización de σ en ciclos disjuntos haya un ciclo de longitud al menos 3. Entonces $M(\sigma) \geq 5$, pues de lo contrario, como en la factorización hay un ciclo de longitud al menos 3, σ sería un 4-ciclo y no estaría en A_n#. Podemos suponer $1, 2, 3, 4, 5 \in M(\sigma)$ y que algún ciclo de la descomposición es de la forma $(1\,2\,3\,\dots)$ con longitud al menos 3. Sea $\alpha := (3\,4\,5) \in A_n$, por la normalidad de H, $\sigma^\alpha \in H$, luego $\beta := \sigma^{-1}\sigma^\alpha \in H$. Si $\sigma(i) = i$, $i > 5$ y $\alpha(i) = i$, luego $\beta(i) = i$, con lo que $M(\beta) \subseteq M(\sigma)$, y la inclusión es estricta porque $\sigma(1) = 2$ pero $\beta(1) = 1$. Entonces $\beta \in H$ cambia menos de r elementos, luego debe ser $\beta = 1$ y $\sigma^\alpha = \sigma$, con lo que $\alpha\sigma = \sigma\alpha$, pero $(\alpha\sigma)(2) = 4$ y $(\sigma\alpha)(2) = 3$#.

2. Que σ sea un producto de 2 o más transposiciones disjuntas. Podemos suponer $\sigma = (1\,2)(3\,4)\cdots$ (puede haber más transposiciones o no. Sean $\alpha := (3\,4\,5) \in A_n$ y $\beta := \sigma^{-1}\sigma^\alpha \in H$. Si $i \neq 5$ y $\sigma(i) = i$, entonces $i \neq 3, 4, 5$, luego $\alpha(i) = i$, $\beta(i) = i$ y por tanto $M(\beta) \subseteq M(\sigma) \cup \{5\}$. Pero 1 y 2 son fijados por β y movidos por σ, luego β cambia menos de r elementos y por tanto $\beta = 1$, con lo que $\sigma\alpha = \alpha\sigma$, sin embargo $(\sigma\alpha)(3) = 3$ y $(\alpha\sigma)(3) = 5$#.