Conjuntos y números

Bibliografía:

- Curso de conjuntos y números: Apuntes, Juan Jacobo Simón Pinero (Curso 2017–2018).

Capítulo 1

Conjuntos y elementos

Podemos definir conjuntos:

- **Por extensión:** $A = \{X_1, \dots, X_n, \dots\}$
- **Por comprehensión:** $A = \{X \in B | p(X) \text{ (es verdadera)}\}$. Si es obvio quién es B, se puede omitir.

Cualquiera de ambas escrituras determina un único conjunto. **Paradoja de Russell:** si $\mathcal{U}$ es la colección de todos los conjuntos y $A = \{x \in \mathcal{U} | x \notin x\}$, entonces $A \in A$ si y sólo si $A \notin A$. Lo que ocurre es que $\mathcal{U}$ no es un conjunto.

- **Pertenencia:** $a \in A$. Contrario: $a \notin A$.
- **Inclusión:** A está contenido, o es un subconjunto, de B: $A \subseteq B :\iff (a \in A \implies a \in B)$. Es transitiva: $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$. Contrario: $A \not\subseteq B$. Subconjunto estricto: $A \subsetneq B \iff A \subseteq B \wedge A \neq B$. $A \subset B$ es ambiguo, aunque se suele usar como $A \subseteq B$.
- **Igualdad:** $A = B :\iff (a \in A \iff a \in B) \iff A \subseteq B \wedge B \subseteq A$.

Múltiplos de un número n como $n\mathbb{Z} = \{nt | t \in \mathbb{Z}\} = \{nt\}_{t \in \mathbb{Z}}$. Así, $m \in n\mathbb{Z} \implies m\mathbb{Z} \subseteq n\mathbb{Z}$. Relación «$m$ divide a n» o «n es múltiplo de m»: $m|n \iff \exists t \in \mathbb{Z} : n = tm$. Si $A = \{x \in B | p(x)\}$ y $A' = \{x \in B | p'(x)\}$, entonces $(p(x) \implies p'(x)) \implies A \subseteq A'$.

Un **conjunto vacío** es aquel que no tiene elementos. Si A es vacío, entonces $A \subseteq B$, dado que si $A \not\subseteq B$ significaría que $\exists a \in A : a \notin B$, por lo que A no estaría vacío. De aquí podemos deducir que solo hay un conjunto vacío, y lo llamamos $\emptyset$. $A = \emptyset :\iff \forall x, x \notin A$.

El conjunto $\mathcal{P}(A) = \{B | B \subseteq A\}$ es el conjunto de las **partes de** A o el conjunto **potencia** de A. También se llama 2^A porque si A tiene n elementos, $\mathcal{P}(A)$ tiene 2^n, de lo que deducimos que $A \neq \mathcal{P}(A)$.

1.1. Operaciones con subconjuntos

Los **diagramas de Venn** aportan una mejor comprensión de los conjuntos y sus operaciones. Los conjuntos se representan como formas (normalmente círculos y cuadrados), que pueden ir acompañados del nombre del conjunto, y se colorea la parte deseada. Operaciones:

- **Unión:** $A \cup B = \{x | x \in A \vee x \in B\}$.
- **Intersección:** $A \cap B = \{x | x \in A \wedge x \in B\}$.
  - A y B son **disjuntos** si $A \cap B = \emptyset$.
- **Diferencia de conjuntos:** $A \backslash B = \{x | x \in A \wedge x \notin B\}$.
- **Complemento:** Si $A \subseteq U$, siendo U un «universo» en el contexto en el que operamos, el complemento de A en U se define como $A^{\complement} = \overline{A} = U \backslash A$.

Propiedades:

- $A \cap B \subseteq A \subseteq A \cup B$
- $\forall A \subseteq B, A \cup X \subseteq B \cup X \wedge A \cap X \subseteq B \cap X$
- $A \subseteq C \wedge B \subseteq C \implies (A \cup B) \subseteq C$
- $(A \cap B) \cap C = A \cap (B \cap C)$; $(A \cup B) \cup C = A \cup (B \cup C)$
- $A \subseteq B \iff A \cup B = B \iff A \cap B = A$
- $A \cup \emptyset = A$; $A \cap \emptyset = \emptyset$
- $X \subseteq (A \cap B) \iff (X \subseteq A) \wedge (X \subseteq B)$; $(A \cup B) \subseteq X \iff (A \subseteq X) \wedge (B \subseteq X)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $(A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B)$
- **Leyes de Morgan:** $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$; $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$.

1.2. Familias de conjuntos

Una familia de conjuntos es una colección $\{A_i | i \in I\}$ donde I y A_i son conjuntos. Si todos los elementos son diferentes, tenemos un conjunto. Algunas definiciones:

- **Unión arbitraria:** $\cup \mathcal{C} = \{x | \exists A \in \mathcal{C} \mid x \in A\}$; $\cup_{i \in I} A_i = \{x | \exists i \in I \mid x \in A_i\}$
- **Intersección arbitraria:** $\cap \mathcal{C} = \{x | \forall A \in \mathcal{C} \mid x \in A\}$; $\cap_{i \in I} A_i = \{x | \forall i \in I \mid x \in A_i\}$

Propiedades:

1. $\cap \mathcal{C} \subseteq A \subseteq \cup \mathcal{C} \forall A \in \mathcal{C}$; $\cap A_i \subseteq A_j \subseteq \cup A_i \forall j \in I$
2. $X \subseteq \cap \mathcal{C} \iff X \subseteq A \forall A \in \mathcal{C}$; $\cup \mathcal{C} \subseteq X \iff A \subseteq X \forall A \in \mathcal{C}$
3. $\cup_{i \in I}(A \cap B_i) = A \cap (\cup_{i \in I} B_i)$; $\cap_{i \in I}(A \cup B_i) = A \cup (\cap_{i \in I} B_i)$

   $\subseteq]$ $x \in \cup_{i \in I}(A \cap B_i) \implies \exists i \in I : x \in (A \cap B_i) \implies (x \in A) \wedge (x \in B_i \subseteq \cup B_i)$

   $\supseteq]$ $x \in A \cap (\cup_{i \in I} B_i) \implies \exists i : (x \in A \wedge x \in B_i) \implies x \in \cup (A \cap B_i)$
4. $(\cap A_i)^{\complement} = \cup A_i^{\complement}$; $(\cup A_i)^{\complement} = \cap A_i^{\complement}$

1.3. Pares ordenados, producto cartesiano y relaciones binarias

El **par ordenado** o **pareja ordenada** formada por $a \in A$ y $b \in B$ es $(a, b) = \{\{a\}, \{a, b\}\}$. Así, $(a, b) = (c, d) \iff a = c \wedge b = d$. El **producto cartesiano** de A y B es $A \times B = \{(a, b) | a \in A \wedge b \in B\}$. Este no es asociativo, pues en general, $(A \times B) \times C \neq A \times (B \times C)$, pero son biyectivos. Por ahora no tenemos descripción en términos de conjuntos para la expresión (a, b, c). Propiedades del producto cartesiano:

- $A \times \emptyset = \emptyset \times A = \emptyset$
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Una **relación binaria** o **correspondencia** entre elementos de A y B es un subconjunto $R \subseteq A \times B$. Si $(a, b) \in R$, decimos que a está relacionado con b, escrito aRb. Si $A = B$, tenemos una relación en A. Definiciones:

- **Conjunto inicial:** A.
- **Conjunto final:** B.
- **Dominio:** $\mathrm{Dom}R = \{a \in A | \exists b \in B \mid (a, b) \in R\}$.
- **Imagen:** $\mathrm{Im}R = \{b \in B | \exists a \in A \mid (a, b) \in R\}$.

Podemos representar las relaciones en gráficas planas.

Capítulo 2

Aplicaciones

Una **aplicación** entre dos conjuntos A y B es una relación $f \subseteq A \times B$ tal que $\forall a \in A, \exists! b \in B : (a,b) \in f$. Escribimos $f : A \to B$ o $A \xrightarrow{f} B$, y llamamos $b = f(a) \iff (a,b) \in f$. Por ejemplo, podemos definir $f : \mathbb{N} \to \mathbb{N}$ tal que $f(n) = n^2$, de modo que $f = \{(n, n^2) \mid n \in \mathbb{N}\}$. Si partimos de una igualdad y queremos interpretarla como la regla de una aplicación, la llamamos **función**. Podemos representar una aplicación:

1. Como dos conjuntos representados de forma similar a un diagrama de Euler-Venn, en el que de cada elemento de A parte una flecha hacia uno de B.

2. Como una gráfica, en la que los elementos de A se representan en el eje horizontal y los de B en el eje vertical, y las relaciones se representan con puntos.

Definimos:

- **Dominio** de f: Dom$f = A$, por lo que el término «conjunto inicial» no se usa.
- **Codominio** de f: «Conjunto final».
- **Imagen** o **imagen directa** de f: Im$f = f(A) = \{b \in B \mid \exists a \mid f(a) = b\} \subseteq B$.
- **Regla de correspondencia** de f: Igualdad $b = f(a)$.
- Si $b = f(a)$, a es *una* **preimagen** de b y b es la **imagen** de a.

Una **ley de composición externa** es una aplicación $B \times A \xrightarrow{\circ} A$. Una **operación binaria** en A es una aplicación $A \times A \xrightarrow{\circ} A$.

2.1. Aplicaciones inyectivas, suprayectivas y biyectivas

La aplicación $f : A \to B$ es:

- **Inyectiva** o **uno a uno** si $f(a) = f(b) \implies a = b$.
- **Suprayectiva**, **sobreyectiva** o **exhaustiva** si $\forall b \in B, \exists a \in A : f(a) = b$.

- **Biyectiva** si es inyectiva y suprayectiva.

La **restricción de f a su imagen** es una aplicación $\hat{f} : A \to \mathrm{Im}f$ dada por $\hat{f}(a) = f(a)$. Se dice que $\hat{f}$ «actúa igual» que f. Siempre es suprayectiva.

2.2. Imágenes directas e inversas

Para $X \subseteq A$, definimos la **imagen directa** de X como $f(X) = \{f(x)|x \in X\}$. Propiedades:

1. $f(\emptyset) = \emptyset$.

   Se deriva de que $\emptyset \times B = \emptyset$.

2. $X \subseteq Y \implies f(X) \subseteq f(Y)$.

$$y \in f(X) \implies \exists x \in X, y \in Y : f(x) = y \implies f(x) \in f(Y) \implies y \in f(Y)$$

3. $X, Y \subseteq A \implies f(X \cup Y) = f(X) \cup f(Y)$; $f\left(\bigcup_{\alpha\in I} X_\alpha\right) = \bigcup_{\alpha\in I} f(X_\alpha)$.

   $\subseteq]$ Sea $y \in f(\cup_{\alpha\in I} X_\alpha)$. Entonces $\exists x \in \cup_{\alpha\in I} X_\alpha : f(x) = y$. Como $x \in \cup_{\alpha\in I} X_\alpha$ entonces $\exists \alpha \in I : x \in X_\alpha$, luego $y \in f(X_\alpha) \subseteq \cup_{\alpha\in I} f(X_\alpha)$.

   $\supseteq]$ Considérese $y \in \cup_{\alpha\in I} f(X_\alpha)$. Entonces $\exists \alpha \in I : y \in f(X_\alpha)$, por lo que $\exists x \in X_\alpha : f(x) = y$. Entonces $x \in \cup_{\alpha\in I} X_\alpha$, así que $y = f(x) \in f(\cup_{\alpha\in I} X_\alpha)$.

4. $X, Y \subseteq A \implies f(X \cap Y) \subseteq f(X) \cap f(Y)$; $f\left(\bigcap_{\alpha\in I} X_\alpha\right) \subseteq \bigcap_{\alpha\in I} f(X_\alpha)$.

   Sea $y \in f(\cap_{\alpha\in I} X_\alpha)$. Entonces $\exists x \in \cap_{\alpha\in I} X_\alpha : f(x) = y$. Como $x \in \cap_{\alpha\in I} X_\alpha$, entonces $\forall \alpha \in I, x \in X_\alpha$, luego $\forall \alpha \in I, \exists x \in X_\alpha : f(x) = y$. De aquí deducimos que $\forall \alpha \in I, y \in f(X_\alpha)$ y por tanto $y \in \cap_{\alpha\in I} f(X_\alpha)$.

Para $Y \subseteq B$, definimos la **imagen inversa** de Y como $f(Y)^{-1} \coloneqq f^{-1}(Y) \coloneqq \{a \in A|f(a) \in Y\}$. Propiedades:

1. $f(\emptyset)^{-1} = \emptyset$.

   Se deriva de que $A \times \emptyset = \emptyset$.

2. $f(B)^{-1} = A$.

3. $X \subseteq B \implies \left(f(X)^{-1}\right)^{\complement} = f\left(X^{\complement}\right)^{-1}$.

4. $X \subseteq Y \subseteq B \implies f(X)^{-1} \subseteq f(Y)^{-1}$.

5. $X, Y \subseteq B \implies f(X \cup Y)^{-1} = f(X)^{-1} \cup f(Y)^{-1}$; $f\left(\bigcup_{\alpha\in I} X_\alpha\right)^{-1} = \bigcup_{\alpha\in I} f(X_\alpha)^{-1}$.
   Sea $x \in f(\bigcup_{\alpha\in I} X_\alpha)^{-1}$. Entonces $f(x) \in \bigcup_{\alpha\in I} X_\alpha$, por lo que $\exists \alpha \in I : f(x) \in X_\alpha$, de donde $x \in f(X_\alpha)^{-1}$.

6. $X, Y \subseteq B \implies f(X \cap Y)^{-1} = f(X)^{-1} \cap f(Y)^{-1}$; $f\left(\bigcap_{\alpha\in I} Y_\alpha\right)^{-1} = \bigcap_{\alpha\in I} f(Y_\alpha)^{-1}$

   $\subseteq]$ Sea $x \in f(\bigcap_{\alpha\in I} Y_\alpha)^{-1}$. Entonces $f(x) \in \bigcap_{\alpha\in I} Y_\alpha$, por lo que $f(x) \in Y_\alpha$, y por tanto $x \in f(Y_\alpha)^{-1}$, para todo $\alpha \in I$. De aquí se tiene que $x \in \bigcap_{\alpha\in I} f(Y_\alpha)^{-1}$.

$\supseteq]$ Sea $x \in \bigcap_{\alpha\in I} f(Y_\alpha)^{-1}$. Entonces $x \in f(Y_\alpha)^{-1}$, y por tanto $f(x) \in Y_\alpha$, para todo $\alpha \in I$. Esto significa que $f(x) \in \bigcap_{\alpha\in I} Y_\alpha$, por lo que $x \in f(\bigcap_{\alpha\in I} Y_\alpha)^{-1}$.

Si $f : A \to B$ es una aplicación, para todo $X \subseteq A$, $X \subseteq f(f(X))^{-1}$, y para todo $Y \subseteq B$, $f(f(Y)^{-1}) \subseteq Y$, y ambos contenidos pueden ser estrictos.

2.3. Composición

Sean $f : A \to B$ y $g : B \to C$, definimos la **composición de f seguida de g** como la aplicación $g \circ f : A \to C$ tal que $(g \circ f)(x) = g(f(x))$. Entonces $\mathrm{Dom}(g \circ f) = \mathrm{Dom} f$ y el codominio de $g \circ f$ es igual al de g. Además, si $f : A \to B$, $g : B \to C$ y $h : C \to D$ son aplicaciones, entonces $h \circ (g \circ f) = (h \circ g) \circ f$. La demostración parte de la coincidencia entre dominios y codominios que permite considerar las distintas composiciones:

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))) = (h \circ g)(f(a)) = ((h \circ g) \circ f)(a)$$

- La composición de aplicaciones inyectivas es inyectiva.
  Sean f y g aplicaciones inyectivas y $a, a' \in A$ tales que $(g \circ f)(a) = (g \circ f)(a')$. Entonces $g(f(a)) = g(f(a'))$, y como g es inyectiva, $f(a) = f(a')$, y entonces $a = a'$.

- La composición de aplicaciones suprayectivas es suprayectiva.
  Sean f y g suprayectivas y $c \in C$. Entonces $\exists b \in B : g(b) = c$ y a su vez $\exists a \in A : f(a) = b$, por lo que $(g \circ f)(a) = c$.

- La composición de aplicaciones biyectivas es biyectiva.

- Si $g \circ f$ es inyectiva, entonces f es inyectiva.
  Sean $a, a' \in A$ tales que $f(a) = f(a')$. Entonces $g(f(a)) = g(f(a'))$, por lo que $(g \circ f)(a) = (g \circ f)(a')$, y por ello $a = a'$.
  Si $g \circ f$ es suprayectiva, g también lo es.
  Para cualquier $c \in C$, $\exists a \in A : (g \circ f)(a) = g(f(a)) = c$, y por tanto $\exists f(a) = b \in B : g(b) = c$.

Dados $f : A \to B$ y $X \subseteq A$, la **restricción** de f a X es la aplicación $f|_X : X \to B$ dada por $f|_X(x) = f(x)$. También se puede interpretar como que $f|_X = f \circ u$ con $u : X \to A$ como la **aplicación inclusión**, dada por $u(x) = x$. Al restringir una aplicación pueden variar sus propiedades.

2.3.1. Inversa de una aplicación biyectiva

Definimos la **aplicación identidad** en A como $1_A : A \to A$ con $1_A(a) = a$. Entonces decimos que $f : A \to B$ es una **aplicación invertible** o que tiene **inversa** si existe $g : B \to A$ tal que $g \circ f = 1_A$ y $f \circ g = 1_B$. Ahora supongamos que g y h son inversas de f. Entonces,

$$g = g \circ 1_B = g \circ (f \circ h) = (g \circ f) \circ h = 1_A \circ h = h$$

Por tanto la inversa de una aplicación es única, y la llamamos f^{-1}. Además f es invertible si y sólo si es biyectiva.

$\Longrightarrow$] Sean $a, a' \in A$. Si $f(a) = f(a')$ entonces $f^{-1}(f(a)) = f^{-1}(f(a'))$, luego $a = a'$ y f es inyectiva. Ahora, $\forall b \in B, \exists a = f^{-1}(b) \in A : f(a) = b$, por lo que es suprayectiva.

$\Longleftarrow$] Para cada $b \in B$ consideremos la imagen inversa $f(\{b\})^{-1}$. Como f es suprayectiva, $f(\{b\})^{-1} \neq \emptyset$, y si $a, a' \in f(\{b\})^{-1}$ entonces $b = f(a) = f(a')$, y como es inyectiva, $a = a'$. Entonces $f(\{b\})^{-1}$ tiene un solo elemento. Ahora definimos $g : B \to A$ tal que $g(b) \in f(b)^{-1}$. Es inmediato comprobar que $g = f^{-1}$.

Así, si f y g son invertibles, $g \circ f$ también lo es y su inversa es $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Un ejemplo de aplicaciones invertibles son las **permutaciones**. Sea $0 \neq n \in \mathbb{N}$ y $A = \{a_1, \ldots, a_n\}$. Entonces una permutación de A es una biyección $\sigma : A \to A$. Se suelen denotar como

$$\sigma : \begin{pmatrix} a_1 & \ldots & a_n \\ \sigma(a_1) & \ldots & \sigma(a_n) \end{pmatrix}$$

Llamamos $S(A)$ al conjunto de las permutaciones de A. Si $A = \{1, \ldots, n\}$, se escribe como S_n.

2.3.2. Producto directo

Sea I un conjunto y $F = \{A_i\}_{i \in I}$ una familia de conjuntos, se define el **producto directo** de F como el conjunto

$$\prod_{i \in I} A_i = \left\{ f \mid I \to \bigcup_{i \in I} \;\middle|\; f(i) \in A_i \forall i \in I \right\}$$

Si $f \in \prod_{i \in I} A_i$, escribimos $f = (x_i)_{i \in I}$. Si I es finito y se escribe como una lista, podemos escribir el conjunto como $A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) \mid x_i \in A_i, i = 1, \ldots, n\}$. Si no se quiere escribir el conjunto de índices, este se presupone.

Debemos tener en cuenta que el producto cartesiano se usa en la definición de relación y aplicación, por lo que el producto directo requiere de la definición del cartesiano y no puede sustituirlo, aunque exista una biyección cuando el número de factores es finito y usemos la misma escritura.

Sean I y J conjuntos y $F = \{A_i\}_{i \in I}$ y $G = \{B_j\}_{j \in J}$ familias de conjuntos. Si existe una biyección $\sigma : I \to J$ y un conjunto de biyecciones $\{f_i \mid A_i \to B_{\sigma(i)}\}_{i \in I}$, entonces existe una biyección $f : \prod_{i \in I} A_i \to \prod_{j \in J} B_j$ dada por $f(x)_j = f_{\sigma^{-1}(j)}\left(x_{\sigma^{-1}(j)}\right)$ para $x \in \prod_{i \in I} A_i$. **Demostración:** para cada $x \in \prod_{i \in I} A_i$ y cada $j \in J$ existe un único $f_{\sigma^{-1}(j)}\left(x_{\sigma^{-1}(j)}\right)$, de modo que la relación es de aplicación, y debemos ver que es biyectiva. Sea $g : \prod_{j \in J} B_j \to \prod_{i \in I} A_i$ dada por $g(y)_i = f_i^{-1}\left(y_{\sigma(i)}\right)$ $(f_i^{-1} : B_{\sigma(i)} \to A_i)$. Como también es aplicación, debemos probar que sean inversas. Entonces:

$$g(f(x))_i = f_i^{-1}(f(x)_{\sigma(i)}) = f_i^{-1}\left(f_{\sigma^{-1}(\sigma(i))}\left(x_{\sigma^{-1}(\sigma(i))}\right)\right) = f_i^{-1}(f_i(x_i)) = x_i$$

De forma análoga, $f(g(y)) = y$, y como tiene inversa, la aplicación es biyectiva.

Axioma de Elección: Si I es un conjunto no vacío y $\{A_i\}_{i \in I}$ una familia de conjuntos no vacíos, entonces $\prod_{i \in I} A_i$ es no vacío.

Capítulo 3

Órdenes en conjuntos

3.1. Relaciones de orden

Una relación R en un conjunto A se dice que es:

- **Reflexiva** si $(a, a) \in R$.
- **Transitiva** si $(a, b), (b, c) \in R \implies (a, c) \in R$.
- **Simétrica** si $(a, b) \in R \implies (b, a) \in R$.
- **Antisimétrica** si $(a, b), (b, a) \in R \implies a = b$.

Una relación $\leq$ en A es **de orden parcial** (o un orden parcial) si es reflexiva, transitiva y antisimétrica. Un ejemplo es el **orden lexicográfico** en K^n: $(x_1, \ldots, x_n) \leq (y_1, \ldots, y_n)$ si y sólo si $x_1 < y_1$, o $x_1 = y_1$ y bien los vectores son de un elemento o bien $(x_2, \ldots, x_n) \leq (y_2, \ldots, y_n)$ en K^{n-1}.

Un **conjunto parcialmente ordenado** (**CPO** o **COPO**) es un par $(A, \leq)$ donde A es un conjunto y «$\leq$» una relación de orden en A. Si el contexto no deja dudas, diremos que A es un COPO. **Notación:** $a < b :\iff a \leq b \wedge a \neq b$.

A es un **conjunto totalmente** o **linealmente ordenado**, y $\leq$ un **orden total** o **lineal**, si se satisface la **ley de la tricotomía**, es decir, si dados $a, b \in A$, ocurre que $a = b$, $a < b$ o $b < a$.

Podemos representar conjuntos ordenados mediante **diagramas de Hasse**, también llamados «upward drawing» o diagramas de grafo de un orden parcial. Se representan los elementos de A y se unen con una línea las que tienen relación de equivalencia entre sí, sin contar las que se puedan deducir de la reflexividad o transitividad, y con el elemento mayor situado más arriba. También se pueden representar mediante **ζ-matrices**, matrices ζ_A con índices en A, de forma que

$$\zeta_{a,b} = \begin{cases} 1 & \text{si } a < b \\ 0 & \text{en otro caso} \end{cases}$$

3.2. Elementos notables en un COPO

Sea $(A, \leq)$ un conjunto parcialmente ordenado y $a \in A$:

- a es **máximo** de A cuando $a \geq b \forall b \in A$. Si existe, es único, pues si fueran $a, a' \in A$ máximos de A, se tendría que $a \leq a'$ y $a' \leq a$, y por tanto $a = a'$.
- a es **mínimo** o **primer elemento** de A cuando $a \leq b \forall b \in A$. Si existe, es único, y la demostración es análoga.
- a es un **elemento maximal** de A cuando $b \geq a \implies b = a$.
- a es un **elemento minimal** de A cuando $b \leq a \implies b = a$.

Además, si $B \subseteq A$:

- a es **cota superior** de B en A si $a \geq b \forall b \in B$.
- a es **cota inferior** de B en A si $a \leq b \forall b \in B$.
- a es **supremo** o **extremo superior** de B en A si es el mínimo de las cotas superiores de B en A. Si existe es único, pues el mínimo de las cuotas superiores, al ser un mínimo, es único.
- a es **ínfimo** o **extremo inferior** de B en A si es el máximo de las cotas inferiores de B en A. Si existe es único, por razonamiento análogo al anterior.

Dado $b \in B$, b es máximo de B si y sólo si es el supremo de B en A.

$\implies$] Al ser máximo se tiene que $b' \geq b \forall b \in B$ y por tanto también es cota superior, pero si hubiera una cota superior menor, a la que llamaremos c, entonces $c < b \in B$ y por tanto no es cota superior#.

$\impliedby$] Al ser supremo, es cota superior, por lo que $a \geq b \forall b \in B$. Si a esto le unimos que $a \in B$, tenemos la definición de máximo.

Esta propiedad se cumple de forma análoga si en vez del máximo y el supremo tomamos el mínimo y el ínfimo.

3.3. Conjuntos bien ordenados

Un CPO es **bien ordenado** si todo subconjunto suyo no vacío tiene primer elemento. Todo conjunto bien ordenado es totalmente ordenado. **Demostración:** Sea A bien ordenado y $B = \{a, b\} \subseteq A$, como $\{a, b\} \neq \emptyset$, tiene primer elemento, de lo que se desprende la tricotomía.

Principio de la Buena Ordenación: Si $A \neq \emptyset$, existe un orden $\leq$ tal que $(A, \leq)$ es un conjunto bien ordenado. Esto es equivalente al Axioma de Elección.

Capítulo 4

Relaciones de equivalencia

Una relación es **de equivalencia** si es reflexiva, simétrica y transitiva. Si $(a, b) \in R$, escribimos aRb, $a \sim_R b$ o, si no causa confusión $a \sim b$.

4.1. Clases de equivalencia

Sea $A \neq \emptyset$ y R una relación de equivalencia en A. Para cada $a \in A$, su clase de equivalencia es $[a] = \{b \in A \mid a \sim b\}$. Entonces:

$$[a] \cap [b] \neq \emptyset \iff a \sim_R b \iff [a] = [b]$$

$1 \implies 2]$ $x \in [a] \cap [b] \implies a \sim x \wedge x \sim b \implies a \sim b$.

$2 \implies 3]$ Por hipótesis $a \sim b$. Entonces $x \in [a] \implies x \sim a \implies x \sim b \implies x \in [b]$. Análogamente, $y \in [b] \implies y \in [a]$.

$3 \implies 1]$ $(a, a) \in R \implies a \in [a] = [b] \implies [a] \cap [b] \neq \emptyset$.

Si C es una clase de equivalencia y $a \in C$ entonces $[a] = C$, y decimos que a es un **representante** de C.

4.2. El conjunto cociente y la proyección canónica

Se define el **conjunto cociente** de A respecto de la relación R como el conjunto de las clases de equivalencia de los elementos de A respecto de R, y se denota A/R, $A/\sim_R$, $A/\sim$ o $\frac{A}{\sim}$. Calcular los conjuntos cociente consiste en dar un **juego completo de representantes**, es decir, describir un conjunto R con uno y solo un representante de cada clase de equivalencia (**conjunto irredundante de representantes** de las clases de equivalencia).

Llamamos **proyección canónica** a la aplicación $\eta_R : A \to A/R$ con $a \mapsto [a]$. Siempre es suprayectiva, por la definición de A/R, y solo es inyectiva cuando R es la igualdad.

4.3. Relaciones de equivalencia y particiones

Sean A e I conjuntos y $P = \{B_i\}_{i\in I}$ una familia de subconjuntos de A, decimos que P forma una **partición** para A si se verifica que $B_i \cap B_j = \emptyset \iff i \neq j$ y $\bigcup_{i\in I} B_i = A$. Toda relación de equivalencia induce una partición, pues $[a] \cap [b] = \emptyset \iff a \not\sim b$, lo que se obtiene de las propiedades de las clases de equivalencia, y $\cup_{[a]\in A/\sim}[a] = A$, pues $b \sim b \implies b \in [b] \subseteq \cup_{[a]\in A/\sim}[a]$. Del mismo modo, toda partición $\{C_i\}_{i\in I}$ en A determina una clase de equivalencia, definida por $a \sim b : \iff \exists i \in I : a, b \in C_i$. Solo quedaría probar que esta es una relación de equivalencia y las clases de equivalencia son las C_i.

Capítulo 5

Conjuntos numéricos

Dos conjuntos son **equipotentes** si existe una aplicación biyectiva entre ellos. Al ser una relación reflexiva, simétrica y transitiva, podemos agrupar a los conjuntos en «clases de equipotencia» que llamamos **cardinales**, y representamos con $|A|$.

Un conjunto A es **infinito** si existe $B \subsetneq A$ equipotente a A. En caso contrario es **finito**. Si A es finito, $f : A \to A$ es inyectiva si y sólo si es suprayectiva.

$\Longrightarrow$] Se $B = \mathrm{Im} f \subseteq A$ y $\hat{f} : A \to B$ la restricción a la imagen de f. Esta es entonces biyectiva, y como A es finito, el subconjunto B no puede ser propio, por lo que es $B = A$, de modo que $\mathrm{Im} f = A$ y f es suprayectiva.

$\Longleftarrow$] Para cualquier $a \in A$ se tiene que $f(\{a\})^{-1} \neq \emptyset$, por lo que existe $g : A \to A \in \prod_{a \in A} f(\{a\})^{-1}$. Por tanto $f(g(a)) = a \forall a \in A$, es decir, $f \circ g = 1_A$, por lo que g es inyectiva y, por la implicación anterior, suprayectiva. Si $a_1, a_2 \in A$ verifican $f(a_1) = f(a_2)$ entonces existen, por la suprayectividad de g, $b_1, b_2 \in A$ con $g(b_1) = a_1$ y $g(b_2) = a_2$. Por tanto $b_1 = f(g(b_1)) = f(a_1) = f(a_2) = f(g(b_2)) = b_2$, de donde $a_1 = g(b_1) = g(b_2) = a_2$ y f es inyectiva.

Igualmente, si A y B son conjuntos finitos con $|A| = |B|$, entonces $g : A \to B$ es inyectiva si y sólo si es suprayectiva. **Demostración:** Al existir una biyección $h : B \to A$, podemos definir $f = h \circ g : A \to A$. Si g es inyectiva, f también, por lo que f es suprayectiva y $g = h^{-1} \circ f$ también. El recíproco se prueba de forma análoga.

Dados $A \subseteq B$, si A es infinito, B también lo es. **Demostración:** Existe $A_0 \subsetneq A$ y $f : A_0 \to A$ biyectiva. Sea entonces $B_0 = A_0 \dot{\cup} (B \backslash A) \subsetneq B$, basta construir una biyección $f' : B_0 \to B$ con $x \in A_0 \mapsto f(x)$ y $x \in B \backslash A \mapsto x$.

5.1. Números naturales

Un cardinal es finito si tiene un representante finito. De lo contrario es infinito. Llamamos **números naturales** ($\mathbb{N}$) a la colección de cardinales finitos. El **axioma del infinito** afirma que esta colección es un conjunto.

Dado $n = |A|$, llamamos **sucesor** de n a $n^* = |A \cup \{x\}|$ con $x \notin A$. Tenemos que $n^* \in \mathbb{N}$, y escribimos $n^* = n + 1$. Podemos entonces definir $\sigma : \mathbb{N} \to \mathbb{N}$ tal que $\sigma(n) = n^*$, con lo que σ es

inyectiva pero no suprayectiva y por tanto $\mathbb{N}$ es infinito. Vemos que $0 = |\emptyset|$ es el único número natural que no es sucesor de ningún otro. Escribimos $\mathbb{N}^* = \mathbb{N}\backslash\{0\}$, y entonces podemos definir intuitivamente la aplicación **antecesor** como $\hat{\sigma}^{-1} : \mathbb{N}^* \to \mathbb{N}$.

Definimos $|A| \leq |B| \iff \exists f : A \to B$ inyectiva, y vemos que $(\mathbb{N}, \leq)$ es bien ordenado. Entonces $n^* = \text{mín}\{x \in \mathbb{N} | n < x\}$ y por tanto, si $a, n \in \mathbb{N}$ son tales que $n \leq a \leq n^*$, entonces $a = n$ o $a = n^*$. **Demostración:** Sea $M_n = \{x \in \mathbb{N} | n < x\}$ y $a = \text{mín}\, M_n$. Sabemos que existen A y N representantes respectivos de a y n junto con $f : N \to A$ inyectiva pero no suprayectiva. Entonces existe $x \in A$ con $x \notin \text{Im} f$. Sea $g : N \cup \{N\} \to A$ con $g(b) = f(b)$ para $b \in N$ y $g(N) = x$, podemos comprobar que g es inyectiva y por tanto $n^* \leq a$, con lo que $n^* = a$.

El **principio de inducción en los números naturales** afirma que si $A \subseteq \mathbb{N}$ cumple que $0 \in A$ y $n \in A \implies n^* \in A$ entonces $A = \mathbb{N}$. Esto puede modificarse tomando que para $k \in \mathbb{N}$, si $k \in A$ y $k \leq n \in A \implies n^* \in A$ entonces $\{n \in \mathbb{N} | n \geq k\} \subseteq A$. La **inducción matemática** es un método de demostración consistente en demostrar la validez de la propiedad P en k y luego probar la validez de $P(n+1)$ suponiendo la de $P(n)$.

También, dados $A \subseteq \mathbb{N}$ y $k \in \mathbb{N}$ con $k \in A$ y $\forall m \in \mathbb{N}, (k \leq m < n \implies m \in A) \implies n \in A$, se tiene que $\{n \in \mathbb{N} | n \geq k\} \subseteq A$. La aplicación de esto se conoce como **inducción matemática fuerte**. El principio de inducción, el del buen orden y el axioma de elección son equivalentes.

Todo conjunto finito totalmente ordenado está bien ordenado y tiene máximo y mínimo. Por otro lado, $\mathbb{N}_n = \{x \in \mathbb{N} | 1 \leq x \leq n\}$ cumple que $|\mathbb{N}_n| = |\{1, \ldots, n\}| = n$ y por tanto es finito.

El conjunto de números naturales que hemos construido satisface los **axiomas de Peano**:

- $0 \in \mathbb{N}$.
- $\exists \sigma : \mathbb{N} \to \mathbb{N}$ inyectiva.
- $0 \notin \text{Im}\sigma$.
- Se cumple el principio de inducción.

Cualquier conjunto que cumpla estas condiciones es esencialmente igual a $\mathbb{N}$, lo que se conoce como **unicidad del sistema de Peano**.

Definimos la **suma** como $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $n + 0 = n$ y $n + m^* = (n + m)^*$. Esta cumple que $(n+1) + m = n + (m+1)$, y verifica las propiedades de **conmutatividad**, **asociatividad** y **cancelación** $(a + c = b + c \implies a = b)$.

Definimos el **producto** como $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ con $n \cdot 0 = 0$ y $n \cdot m^* = n \cdot m + n$, y escribimos $n \cdot m = nm$. Este cumple que $(n+1)m = nm + m$, y verifica las propiedades de **conmutatividad**, **asociatividad**, **distributividad** respecto de la suma y **cancelación** $(nm = 0 \iff n = 0 \vee m = 0)$.

Teorema para la relación del orden y las operaciones aritméticas:

1. $a \leq b \iff \exists u \in \mathbb{N} : a + u = b$; $a \leq a + u \forall u \in \mathbb{N}$.
   Sea $B = \{n \in \mathbb{N} | a + n > b\}$ y como $b^* \in B$ entonces $B \neq \emptyset$, por lo que existe $c \coloneqq \text{mín}\, B$. Sea entonces $u \in \mathbb{N}$ con $u^* = c$. De aquí, $a + u \leq b < a + u^*$, por lo que $a + u = b$.
2. $a \leq b \implies a + c \leq b + c$.
3. $a \leq b \implies ac \leq bc$.

Si $a + u = b$, llamamos $u = b - a$.

5.2. Números enteros

Llamamos **números enteros** al conjunto cociente $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ con

$$(a,b) \sim (n,m) \iff a+m = b+n$$

Tenemos entonces que $\{(a,0)\}_{a\in\mathbb{N}} \dot\cup \{(0,b)\}_{b\in\mathbb{N}^*}$ es un conjunto irredundante de representantes. Así, si $n \geq m$, $(n,m) \in [(n-m,0)]$, y si $n < m$, $(n,m) \in [(0,m-n)]$. Denotamos con n a $[(n,0)]$ y los identificamos con los naturales, y denotamos con $-n$ a $[(0,n)]$. Definimos también $\mathbb{Z}^+ = \{n \in \mathbb{Z} | 0 \neq n \in \mathbb{N}\}$, $\mathbb{Z}^- = \{-n \in \mathbb{Z} | 0 \neq n \in \mathbb{N}\}$ y $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$.

Definimos $[(a,b)] \leq [(m,n)] \iff a+n \leq b+m$, y de aquí que $(\mathbb{Z}, \leq)$ es un conjunto totalmente ordenado en el que todo entero tiene predecesor y sucesor.

Definimos la **suma** como $+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ con $[(a,b)] + [(m,n)] = [(a+m, b+n)]$. Esta está bien definida y verifica las propiedades conmutativa, asociativa, existencia de **neutro** $0 = [(0,0)]$ ($\forall a \in \mathbb{Z}, a+0 = 0$) y existencia de **opuesto** o **inverso bajo la suma** ($\forall a \in \mathbb{Z}, \exists a' : a + a' = 0$). **Demostración** de que está bien definida. Sean $a, a', b, b', m, m', n, n' \in \mathbb{N}$ con $[(a,b)] = [(a',b')]$ y $[(m,n)] = [(m',n')]$. Entonces $a + b' = b + a'$ y $m + n' = n + m'$, de donde $a + b' + m + n' = b + a' + n + m'$, luego $(a+m) + (b'+n') = (a'+m') + (b+n)$ y $[(a+m, b+n)] = [(a'+m', b'+n')]$.

Definimos el **producto** como $\cdot : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ con $[(a,b)] \cdot [(m,n)] = [(am+bn, an+bm)]$. Este está bien definido y verifica las propiedades conmutativa, asociativa, distributiva respecto a la suma y existencia de neutro $1 = [(1,0)]$.

5.3. Números racionales

Llamamos **números racionales** al conjunto cociente $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^*/\sim$ con

$$[(a,b)] \sim [(n,m)] \iff am = bn$$

Identificamos los enteros con los $[(n,1)]$, escribimos $\frac{m}{n} \coloneqq [(m,n)]$ y denotamos con m a $\frac{m}{1} = [(m,1)]$.

Definimos $\frac{n}{m} \leq \frac{a}{b} \iff nmb^2 \leq abm^2$, y decimos que un racional es **positivo** si es mayor que 0 y **negativo** si es menor. Si m y b tienen el mismo signo, podemos considerar $\frac{n}{m} \leq \frac{a}{b} \iff nb \leq ma$. Se tiene que $(\mathbb{Q}, \leq)$ es un conjunto totalmente ordenado. **Demostración:** Dados $\frac{n}{m}$ y $\frac{a}{b}$, se tiene que $nb = ma$, $nb > ma$ o $nb < ma$.

Definimos la suma como $+ : \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}$ tal que $\frac{a}{b} + \frac{m}{n} = \frac{an+bm}{bn}$. Esta está bien definida, y verifica las propiedades de conmutatividad, asociatividad, existencia de neutro $0 = [(0,1)]$ y existencia de opuesto. Además, $\frac{-n}{m} = \frac{n}{-m} = -\frac{n}{m}$.

Definimos el producto como $\cdot : \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}$ tal que $\frac{a}{b} \cdot \frac{m}{n} = \frac{am}{bn}$. Este está bien definido y verifica las propiedades de conmutatividad, asociatividad, existencia de neutro $1 = [(1,1)]$ y existencia de inverso para todo racional no cero ($\forall \frac{m}{n} \in \mathbb{Q}, \frac{m}{n} \cdot \frac{n}{m} = 1$).

Una sucesión de números naturales $(a_n)_{n\in\mathbb{N}}$ (o de cualquier subconjunto de $\mathbb{C}$) es **eventualmente periódica** si $\exists m \in \mathbb{N}, q \in \mathbb{N}^* : \forall i \geq m, a_i = a_{i+q}$. Al menor m que satisface la condición se le llama **término inicial del período**, y al menor q, **período**. Una sucesión eventualmente periódica con $p = 1$ se dice que es **eventualmente constante**. Por otro lado, una sucesión de naturales $(a_n)_{n\in\mathbb{N}}$ es **decimal** si $a_n \in \{0, \ldots, 9\}$ para $n > 0$.

Teorema: Para todo $\alpha \in \mathbb{Q}$ con $\alpha \geq 0$, existe una única sucesión decimal eventualmente periódica de naturales $(a_n)_{n\in\mathbb{N}}$ tal que $0 \leq \alpha - a_0 - \frac{a_1}{10} - \cdots - \frac{a_n}{10^n} < \frac{1}{10^n}$ para todo $n \in \mathbb{N}$. Esta relación determina una biyección entre los racionales positivos y las sucesiones decimales eventualmente periódicas que no son eventualmente constantes con término inicial 9.

Demostración. Tomamos $\alpha = \frac{k}{d}$ con $k \geq 0$, $d > 0$ y $\mathrm{mcd}(k, d) = 1$ y definimos $a_0 = E(\alpha)$ y r_0 tal que $\alpha = a_0 + \frac{r_0}{d}$, de modo que $0 \leq r_0 < d$. Definimos entonces por recurrencia $a_{n+1} = E(\frac{10r_n}{d})$ y $\frac{10r_n}{d} = a_{n+1} + \frac{r_{n+1}}{d}$, de modo que $0 \leq r_{n+1} < d$, y también $S_n = a_0 + a_1 10^{-1} + \cdots + a_n 10^{-n}$. A continuación probamos las siguientes afirmaciones:

1. **Decimal:** $0 \leq a_n < 10$.

$$0 \leq a_{n+1} \leq a_{n+1} + \frac{r_{n+1}}{d} = \frac{10r_n}{d} < 10$$

2. **Lema:** $\alpha = S_n + \frac{r_n}{d}10^{-n}$.
   Para $n = 0$, $\alpha = a_0 + \frac{r_0}{d}$. Ahora asumimos que esto se cumple para un cierto n y demostramos que se cumple también para $n + 1$:

$$\alpha = S_n + \frac{10r_n}{d}10^{-(n+1)} = S_n + \left(a_{n+1} + \frac{r_{n+1}}{d}\right)10^{-(n+1)} = S_{n+1} + \frac{r_{n+1}}{d}10^{-(n+1)}$$

3. **Aproximación:** $0 \leq \alpha - S_n < 10^n$

$$0 \leq \alpha - S_{n+1} = \frac{r_{n+1}}{d}10^{-(n+1)} < 10^{-(n+1)}$$

4. **Unicidad:** $a_{n+1} = E(10^{n+1}(\alpha - S_n))$.

$$a_{n+1} = E\left(\frac{10r_n}{d}\right) = E\left(10^{n+1}10^{-n}\frac{r_n}{d}\right) = E(10^{n+1}(\alpha - S_n))$$

5. **Periodicidad:** Como $0 \leq r_n < d \forall n$, los r_n deben repetirse, es decir, $\exists m, q \in \mathbb{N}, q > 0 : r_m = r_{m+q}$. Vemos por inducción que $a_i = a_{i+q} \forall i \geq m+1$. Para $i = m+1$, a_{m+1} y r_{m+1} son cociente y resto de $10r_m/d$, con lo que $a_{(m+q)+1} = a_{(m+1)+q}$ y $r_{(m+q)+1} = r_{(m+1)+q}$ son cociente y resto de $10r_{m+q}/d = 10r_m/d$, por lo que $a_{m+1} = a_{(m+1)+q}$ y $r_{m+1} = r_{(m+1)+q}$. El paso de inducción es análogo, partiendo de que $r_i = r_{i+q}$ para obtener que $a_{i+1} = a_{(i+q)+1}$ y $r_{i+1} = r_{(i+q)+1}$.

5.4. Estructuras algebraicas

Un conjunto $A \neq \emptyset$ con una operación suma $+ : A \times A \to A$ es un **grupo abeliano** si la suma es conmutativa, asociativa, existe un elemento neutro $0 \in A$ y todo $a \in A$ tiene opuesto ($b \in A$ con $a + b = 0$).

Si además tiene una operación producto $\cdot : A \times A \to A$, decimos que es un **anillo** si con la suma es un grupo abeliano, el producto es asociativo, distribuye a la suma y tiene neutro $1 \in A$. Un anillo en que el producto es conmutativo es un **anillo conmutativo**, y si además todo $a \in A\backslash\{0\}$ tiene inverso ($b \in A$ con $ab = 1$), decimos que es un **cuerpo**.

5.5. Números reales

Podemos construirlos partiendo de los racionales de 3 formas:

1. Identificándolos con los desarrollos decimales infinitos.
2. Mediante las **cortaduras de Dedekind**, conjuntos $\emptyset \neq \beta \subsetneq \mathbb{Q}$ acotados superiormente y sin máximo tales que $y < x \in \beta \implies y \in \beta$.
3. Considerando el conjunto cociente de cierta relación de equivalencia de las sucesiones de Cauchy en $\mathbb{Q}$.

Asumimos que es un conjunto no vacío $(\mathbb{R}, +, \cdot)$ que contiene a los racionales y satisface los siguientes axiomas:

1. **Axiomas de cuerpo:** $(\mathbb{R}, +, \cdot)$ es un cuerpo.
2. **Axiomas de orden:** $\mathbb{R}$ está totalmente ordenado, $x < y \implies x + z < y + z$ y $x, y > 0 \implies xy > 0$. $x \in \mathbb{R}$ es positivo si $x > 0$ y negativo si $x < 0$. De aquí se tiene que si $x > 0$, su opuesto $-x < 0$, pues $x > 0 \implies x - x > 0 - x \implies 0 > -x$.
3. **Axiomas de completitud:** Todo subconjunto no vacío de $\mathbb{R}$ acotado superiormente posee supremo.

5.6. Números complejos

Llamamos **números complejos** al cuerpo definido por

$$\mathbb{C} = \{(a, b) | a, b \in \mathbb{R}\}$$

junto con las operaciones $(a, b) + (c, d) = (a + c, b + d)$ y $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. Se representan en el plano cartesiano en las coordenadas (a, b). Identificamos $\mathbb{R}$ con $\{(a, 0)\}_{a \in \mathbb{R}}$. Definimos $i^2 = -1$ y escribimos $a + bi = (a, b)$. Entonces $i^n = i^m \iff 4 | n - m$.

Llamamos **conjugado** de $z = a + bi \in \mathbb{C}$ a $\overline{z} = a - bi$. Propiedades:

1. $\overline{\overline{z}} = z$.
2. $\overline{z + w} = \overline{z} + \overline{w}$.
3. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
4. $z \neq 0 \implies \overline{z^{-1}} = \overline{z}^{-1}$.
5. $z \in \mathbb{R} \iff \overline{z} = z$.

Dado $z = a + bi \in \mathbb{C}$, su **parte real** es $\mathrm{Re}(z) = a$, su **parte imaginaria** es $\mathrm{Im}(z) = b$, su **módulo** es $|z| = \sqrt{a^2 + b^2}$ y su **argumento** es $\mathrm{Arg}(z) = \theta = \arctan \frac{b}{a}$, estableciendo primero el cuadrante de forma que $\cos(\theta) = \frac{a}{|z|}$ y $\sin(\theta) = \frac{b}{|z|}$, y es único salvo múltiplos de 2π. Propiedades:

1. $|z|^2 = z\overline{z}$.

2. $|z| = |\overline{z}|$.
3. $|zw| = |z||w|$.
4. $|z^{-1}| = |z|^{-1}$.
5. $|\mathrm{Re}(z)| \leq |z|$.
6. **Desigualdad triangular:** $|z + w| \leq |z| + |w|$.
   Como $z\overline{w} = \overline{\overline{z}w}$, entonces $z\overline{w} + \overline{z}w = 2\mathrm{Re}(z\overline{w})$. Así, $|z + w|^2 = (z + w)(\overline{z} + \overline{w}) = z\overline{z} + w\overline{w} + z\overline{w} + \overline{z}w = |z|^2 + |w|^2 + 2\mathrm{Re}(z\overline{w}) \leq |z|^2 + |w|^2 + 2|z\overline{w}| = (|z| + |w|)^2$.

Sea $z = a + bi$ con módulo r y argumento θ, la **representación polar** de z es $z \mapsto (r, \theta)$, pues r es la distancia al centro cartesiano y θ el ángulo respecto del eje de abscisas. Así, su **representación trigonométrica** es $z \mapsto r(\cos\theta + i\sin\theta)$, y si $z = (r, \theta)$ y $w = (s, \sigma)$, entonces $zw = (rs, \theta+\sigma)$. De aquí se deduce el **teorema de De Moivre:** Dado $z = (r, \theta)$, $z^n = (r^n, n\theta)$. Por tanto, si $z^n = (s, \alpha)$, se tiene que $r = \sqrt[n]{s}$ y $\theta = \frac{\alpha+2k\pi}{n}, k \in \mathbb{Z}$, con lo que todo número complejo tiene exactamente n raíces n-ésimas complejas.

Para $n \geq 2$, $\omega \in \mathbb{C}$ es una raíz n-ésima de la unidad si $\omega^n = 1$, y es una **raíz n-ésima primitiva de la unidad** si además $\omega^m \neq 1$ para $0 < m < n$. Así, todo número complejo tiene

$$\phi(n) = |\{m \in \{1, \ldots, n-1\} \mid \mathrm{mcd}(m, n) = 1\}|$$

raíces n-ésimas primitivas. Esta función se conoce como **función ϕ de Euler**.

Se tiene que

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad \cos x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!} \quad \sin x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$$

Por tanto tiene sentido definir que $e^{ip} = \cos p + i\sin p$, pues $e^{ip} = 1 + ip + \frac{(ip)^2}{2!} + \cdots = 1 + ip - \frac{p^2}{2!} - \frac{ip^3}{3!} + \frac{p^4}{4!} + \cdots = \cos p + i\sin p$. Por tanto, podemos escribir $z = (r, \theta) \in \mathbb{C}$ como $z = re^{\theta i}$, y obtenemos la **identidad de Euler**:

$$e^{\pi i} + 1 = 0$$

5.7. Conjuntos numerables y no numerables

Un conjunto A es **a lo más numerable** si $|A| \leq |\mathbb{N}|$, **numerable** si $|A| = |\mathbb{N}|$ y **más que numerable** si $|A| > |\mathbb{N}|$. **Teorema de Bernstein** o **de Cantor-Schröeder-Bernstein (CSB):** Dados dos conjuntos A y B tales que existen $f : A \to B$ y $g : B \to A$ inyectivas, entonces existe una biyección entre ellos.

$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. **Demostración:** Para simplificar, interpretamos $\mathbb{N}$ sin el 0. Ordenamos las parejas de $\mathbb{N} \times \mathbb{N}$ en orden lexicográfico y luego vamos contando en diagonal. Entonces en cada diagonal de $(1, n)$ a $(n, 1)$ están los pares cuyas coordenadas suman $n + 1$, y al terminar la diagonal habremos contado $S(n) = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ pares. Entonces $(1, n) \mapsto S(n-1) + 1$, $(2, n-1) \mapsto S(n-1) + 2$, etc. Así, definimos $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ con $\varphi(i, j) = \frac{(i+j-1)(i+j-2)}{2} + i$ y vemos que es una biyección.

Teorema: $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < (0,1) = |\mathbb{R}|$. **Demostración** de que $|\mathbb{N}| < (0,1)$: La aplicación $f : \mathbb{N} \to (0,1)$ con $f(n) = \frac{1}{n+1}$ es inyectiva. Para ver que no hay aplicaciones inyectivas $(0,1) \to \mathbb{N}$ usamos el **método de la diagonal de Cantor**. Supongamos que existe y hemos numerado todos los elementos en $(0,1)$. Si los escribimos en su forma decimal, tenemos

$$\begin{aligned} x_1 &= 0, x_{11}x_{12}x_{13}\cdots \\ x_2 &= 0, x_{21}x_{22}x_{23}\cdots \\ x_3 &= 0, x_{31}x_{32}x_{33}\cdots \end{aligned}$$

etcétera. Ahora, sea $(y_n)_n$ una secuencia de dígitos con $y_n \in \{0,\ldots,9\}\backslash\{x_{nn}\}$ e $y_1 = \{1,\ldots,8\}\backslash\{x_{nn}\}$ (para evitar que el número formado sea 0 o 1). Entonces este número difiere con cada uno de la lista en al menos un dígito.

Capítulo 6

El anillo de los números enteros

6.1. Aritmética de los enteros

Propiedades de $\mathbb{Z}$:

1. **Unicidad de los neutros:** $\exists!0 \in \mathbb{Z} : \forall a \in \mathbb{Z}, 0 + a = a$; $\exists!1 \in \mathbb{Z} : \forall a \in \mathbb{Z}, 1a = a$.
2. **Unicidad de los opuestos:** $\forall a \in \mathbb{Z}, \exists!(-a) \in \mathbb{Z} : a + (-a) = 0$.
3. **Cancelación en sumas:** $\forall a, b, c \in \mathbb{Z}, (a + b = a + c \implies b = c)$.
4. **Multiplicación por cero:** $\forall a \in \mathbb{Z}, a0 = 0$.
5. **Reglas de signos:** $\forall a, b \in \mathbb{Z}, (-(-a) = a \wedge a(-b) = (-a)b = -(ab) \wedge (-a)(-b) = ab)$.
6. **Cancelación en productos:** $\forall a, b, c \in \mathbb{Z}, a \neq 0, (ab = ac \implies b = c)$.

Teorema de la división entera: $\forall a, b \in \mathbb{Z}, \exists!q, r \in \mathbb{Z} : (a = bq + r \wedge 0 \leq r < |b|)$. Llamamos a q el **cociente** de la división y a r el **resto**. **Demostración:** Sean $a, b > 0$ y $R = \{x \in \mathbb{Z} | x \geq 0 \wedge \exists n \in \mathbb{Z} \mid x = a - bn\} \subseteq \mathbb{N}$. Sabemos que $R \neq \emptyset$ porque $a = a - b \cdot 0 \in R$. Por tanto tiene primer elemento $r = a - bq \in R$. Si $r \geq b$ entonces $0 \leq r - b \in R\#$, luego $r < b$. Si $a < 0$ y $b > 0$ entonces $-a > 0$ y $-a = bq + r$ con $0 \leq r < b$. Si $r = 0$, $a = b(-q) + 0$, y si $r \neq 0$, $a = b(-q) - r = b(-q - 1) + (b - r)$. Si $a \neq 0$ y $b < 0$ entonces $-b > 0$ y $a = (-b)q + r$ con $0 \leq r < -b = |b|$, luego $a = b(-q) + r$ con $0 \leq r < |b|$. Finalmente, si $a = 0$ entonces $0 = b \cdot 0 + 0$. Para la unicidad de q y r, supongamos $a = bq + r = bq' + r'$ con $0 \leq r, r' < |b|$. Entonces $b(q - q') = r - r'$, con lo que $|b||q - q'| = |r - r'|$, pero como $0 \leq r, r' < |b|$, entonces $q - q' = 0$ y $r - r' = 0$.

Decimos que b **divide a** a o que a **es múltiplo de** b ($b|a$) si $\exists c \in \mathbb{Z} : a = bc$. Si $a \neq 0$, también decimos que b **es divisor de** a. Para $b \neq 0$, $b|a$ equivale a que la división entera de a entre b dé resto 0.

1. La divisibilidad es reflexiva y transitiva.
2. No es antisimétrica, pero $a|b \wedge b|a \implies |a| = |b|$.
3. $a|b \iff a| - b$, con lo que si $b \neq 0$, b y $-b$ tienen los mismos divisores.

4. $a|b \iff -a|b$, luego a y $-a$ tienen los mismos múltiplos.
5. $c|a \wedge c|b \implies c|ra+sb$.
6. $a|b \wedge c|d \implies ac|bd$.
7. $a|b \implies ca|cb$. El recíproco es cierto si $c \neq 0$.
8. Si $b \neq 0$, $a|b \implies |a| \leq |b|$.

Dados $a, b \in \mathbb{Z}$, su **máximo común divisor** es $\mathrm{mcd}(a,b) = \mathrm{máx}\{d \in \mathbb{Z} \mid d|a \wedge d|b\}$ (excepción: $\mathrm{mcd}(0,0) = 0$). Este existe porque el conjunto de divisores comunes es no vacío (contiene al 1) y finito, luego tiene máximo. Propiedades:

1. $\mathrm{mcd}(a,b) = \mathrm{mcd}(a,|b|) = \mathrm{mcd}(|a|,|b|)$.
2. $\mathrm{mcd}(a,0) = |a|$.
3. $\mathrm{mcd}(a,b) = 0 \iff a = b = 0$.

Dados $a, b \in \mathbb{Z}$ con alguno distinto de 0, $\mathrm{mcd}(a,b) = \mathrm{mín}\{ra+sb > 0 | r,s \in \mathbb{Z}\}$, y todo divisor común de a y b lo es de $\mathrm{mcd}(a,b)$. **Demostración:** Dado $\emptyset \neq D = \{ra+sb > 0 | r,s \in \mathbb{Z}\} \subseteq \mathbb{Z}^+$, existe $\delta = \mathrm{mín}\, D$. Existen entonces $\alpha, \beta \in \mathbb{Z}$ tales que $\delta = \alpha a + \beta b$. Por el algoritmo de la división, $a = \delta q + r$ con $0 \leq r < \delta$, luego $r = (1-\alpha q)a + (-q\beta)b$, luego r es combinación lineal y entonces $r \in D$ o $r = 0$. Lo primero es imposible porque $r < \delta = \mathrm{mín}\, D$, luego $r = 0$ y $\delta|a$. Análogamente $\delta|b$. Que sea máximo, y que todo divisor común de a y b lo sean de δ, se desprende de que $c|a \wedge c|b \implies c|\alpha a + \beta b = \delta$.

De aquí que para todo $a, b \in \mathbb{Z}$ existen $r, s \in \mathbb{Z}$ tales que $\mathrm{mcd}(a,b) = ra+sb$. Una expresión de la forma $d = ra+sb$ es una **identidad de Bézout**. En particular, si $a = da'$ y $b = db'$ con $d = \mathrm{mcd}(a,b)$, entonces $\mathrm{mcd}(a',b') = 1$.

$d = \mathrm{mcd}(a,b)$ si y sólo si $d|a$, $d|b$, $c|a \wedge c|b \implies c|d$ y $d \geq 0$.

$\implies$] Las propiedades (1) y (3) son por definición, y la (2) la acabamos de demostrar.

$\impliedby$] Si $a \neq 0$ o $b \neq 0$, d es el mayor entero que divide a a y b. Si $a = b = 0$, como $0|a, b$, entonces $0|d$, luego $d = 0$.

El máximo común divisor de $a_1, \ldots, a_n$ es $\mathrm{mcd}(a_1, \ldots, a_n) = \mathrm{máx}\{d \in \mathbb{Z} \mid \forall i, d|a_i\}$. Entonces $\mathrm{mcd}(a_1, \ldots, a_n) = \mathrm{mcd}(\mathrm{mcd}(a_1,a_2), a_3, \ldots, a_n)$. **Demostración:** Sea $d \coloneqq \mathrm{mcd}(a_1, \ldots, a_n)$, como $d||a_1, \ldots, a_n$, entonces $d|(f \coloneqq \mathrm{mcd}(a_1,a_2)), a_3, \ldots, a_n|e \coloneqq \mathrm{mcd}(\mathrm{mcd}(a_1,a_2), a_3, \ldots, a_n)$ y por tanto $d|e$. Pero $e|f, a_3, \ldots, a_n$, luego $e|a_1, \ldots, a_n$ y $e|d$, y como $d, e \geq 0$, $d = e$.

Teorema: Dados $a_1, \ldots, a_n \in \mathbb{Z}^*$, $\mathrm{mcd}(a_1, \ldots, a_n) = \mathrm{mín}\,\{\sum_{i=1}^n r_i a_i > 0 | r_i \in \mathbb{Z}\}$. Además, $d = \mathrm{mcd}(a_1, \ldots, a_n)$ si y sólo si $d|a_1, \ldots, a_n$, $c|a_1, \ldots, a_n \implies c|d$ y $d \geq 0$.

$a, b \in \mathbb{Z}$ son **coprimos** o **primos entre sí** si $\mathrm{mcd}(a,b) = 1$, es decir, si $\exists \alpha, \beta \in \mathbb{Z} : \alpha a + \beta b = 1$. Si a y b son coprimos:

1. $a|bc \implies a|c$.
   Sea $1 = \alpha a + \beta b$, multiplicando por c, $c = \alpha ac + \beta bc$. Como $a|bc$, $c = \alpha ca + \beta na$ y $a|c$.

2. $a|c \wedge b|c \implies ab|c$.

$$\begin{array}{c} 1 = ra + sb \\ \frac{c}{a}, \frac{c}{b} \in \mathbb{Z} \end{array} \implies \frac{c}{a} = \frac{c}{a}ra + \frac{c}{a}sb = \frac{c}{b}rb + \frac{c}{a}sb = b\left(\frac{c}{b}r + \frac{c}{a}s\right) \implies$$
$$\implies c = ab\left(\frac{c}{b}r + \frac{c}{a}s\right) \implies ab|c$$

Se tiene que $\mathrm{mcd}(a,b) = \mathrm{mcd}(a - sb, b) = \mathrm{mcd}(a, b - sa)$, y en particular, si $b \neq 0$ y $a = bq + r$ con $0 \leq r < b$, entonces $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,r)$. La aplicación repetida de lo anterior se conoce como **algoritmo de Euclides**. También permite obtener identidades de Bézout. Si llamamos $(a,b) = \mathrm{mcd}(a,b)$:

$$\begin{array}{ccc} a = bq_1 + r_1 & (a,b) = (b,r_1) & r_1 < b \\ b = r_1q_2 + r_2 & (b,r_1) = (r_1,r_2) & r_2 < r_1 \\ & \vdots & \\ r_{n-2} = r_{n-1}q_n + 0 & (r_{n-2},r_{n-1}) = (r_{n-1},0) = r_{n-1} & 0 < r_{n-1} \end{array}$$

Como $b > r_1 > \cdots \geq 0$, el algoritmo acaba en un número finito de pasos. Además, cada dos pasos del algoritmo, el resto se reduce a la mitad. **Demostración:** Sean $a = bq + r$, $b = rq' + s$ y $r = sq'' + t$, si $s \leq \frac{1}{2}r$ entonces $t < s \leq \frac{1}{2}r$ y hemos terminado, y si $s > \frac{1}{2}r$, entonces $q'' = 1$ y $t = r - s < r - \frac{1}{2}r = \frac{1}{2}r$.

Dados $a, b \in \mathbb{Z}^*$, su **mínimo común múltiplo** es $\mathrm{mcm}(a,b) = \mathrm{mín}\{m \in \mathbb{Z}^+ \mid a|m \wedge b|m\}$. Si a o b son 0, entonces $\mathrm{mcm}(a,b) = 0$. Propiedades:

1. $\mathrm{mcm}(a,b) = \mathrm{mcm}(a,|b|) = \mathrm{mcm}(|a|,|b|)$.
2. $\mathrm{mcm}(a,b) = 0 \iff a = 0 \vee b = 0$.
3. $\mathrm{mcm}(a,ab) = |ab|$.

Teorema:

1. $\mathrm{mcm}(a,b)\mathrm{mcd}(a,b) = |ab|$.
   Para $a, b > 0$, sea $d = \mathrm{mcd}(a,b)$ con $a = da'$ y $b = db'$, sea $m = a'b'd$. Entonces $a|m$ y $b|m$. Sea $c = \alpha a = \beta b$ con $\alpha, \beta \in \mathbb{Z}$, entonces $\alpha da' = \beta db'$, luego $\alpha a' = \beta b'$, y como a' y b' son coprimos, $a'|\beta$ y $\beta = \gamma a'$ con $\gamma \in \mathbb{Z}$. Sustituyendo, $c = \gamma a'b = \gamma a'db' = \gamma m \geq m$, luego $m = \mathrm{mcm}(a,b)$.
2. $a|c \wedge b|c \implies \mathrm{mcm}(a,b)|c$.

El mínimo común múltiplo de $a_1, \ldots, a_n$ es $\mathrm{mcm}(a_1, \ldots, a_n) = \mathrm{mín}\{m \in \mathbb{Z}^+ \mid \forall i, a_i|m\}$. Así, $m = \mathrm{mcm}(a_1, \ldots, a_n)$ si y sólo si $a_1, \ldots, a_n|m$, $a_1, \ldots, a_n|c \implies m|c$ y $m \geq 0$.

Una ecuación del tipo $ax + by = c$ en la que se buscan soluciones enteras es una **ecuación diofántica lineal**, en este caso de dos variables. Tiene solución si y sólo si $d = \mathrm{mcd}(a,b)|c$, y entonces estas son de la forma

$$\left\{ \begin{array}{rcl} x & = & x_0 + x' \\ y & = & y_0 + y' \end{array} \right.$$

donde x_0, y_0 es una solución particular y x', y' es una solución de la **ecuación homogénea asociada**, $ax + by = 0$. En particular, si $\alpha a + \beta b = d$ y $c = c'd$, entonces $x_0 = c'\alpha$ e $y_0 = c'\beta$.

$\Longrightarrow$] Sean $x, y \in \mathbb{Z}$ con $ax + by = c$. Entonces $d|ax + by = c$.

$\Longleftarrow$] Multiplicando la identidad de Bézout, $(c'\alpha)a + (c'\beta)b = c'd = c$.

Si $d = \text{mcd}(a, b)$, $a = a'd$ y $b = b'd$, las soluciones de $ax + by = 0$ son

$$\left\{ \begin{array}{rcl} x & = & -b't \\ y & = & a't \end{array} \right.$$

para cualquier $t \in \mathbb{Z}$. **Demostración:** $ax = -by$, luego $a'x = -b'y$. Como a' y b' son coprimos y $a'| - b'y$, entonces $a'|y$, luego existe $t \in \mathbb{Z}$ con $y = a't$, con lo que $a'x = -b'a't$ y $x = -b't$. Multiplicando, todos los enteros de esta forma son solución.

Un entero $p \neq 1, -1$ es **primo** si sus únicos divisores son 1, -1, p y $-p$. Así,

$$p \text{ es primo} \iff (p|ab \implies p|a \vee p|b) \iff (p|a_1 \cdots a_n \implies \exists i : p|a_i)$$

$1 \implies 2]$ Si $p|a$ ya está. Si no, $\text{mcd}(p, a) = 1$ y $p|b$.

$2 \implies 3]$ Por inducción con $a_1 \cdots a_n = a_1(a_2 \cdots a_n)$.

$3 \implies 1]$ Si $a|p$ entonces $p = ab$ para cierto b, y bien $p|a$ (con lo que $a = p$ o $a = -p$) o $p|b$ (con lo que $a = 1$ o $a = -1$).

Teorema Fundamental de la Aritmética: Todo entero distinto de 0 y ± 1 puede escribirse como producto de primos, y la factorización es única salvo signo y orden. **Demostración:** Consideremos el conjunto de todos los positivos distintos de 1 que no se factorizan en primos y, si este no es vacío, sea $a \in \mathbb{Z}$ su mínimo. a no es primo, luego $a = bc$ con $b, c \in \mathbb{Z}^+ \backslash \{1\}$. Pero como a es mínimo, entonces b y c sí se factorizan en primos, luego a también.# Ahora sea $a = p_1 \cdots p_n = q_1 \cdots q_m$ con $p_1 \cdots p_n, q_1 \cdots q_m$ primos y supongamos $n \leq m$. Procedemos por inducción sobre n. Si $n = 1$, $a = p_1 = q_1 \cdots q_m$, y como p_1 no tiene más divisores primos que $-p_1$ y p_1, debe ser $m = 1$ y $q_1 = p_1$. Si suponemos el resultado válido para $n - 1$, entonces p_n divide a $a = q_1 \cdots q_n$ y por tanto divide a algún $i \in \{1, \ldots, m\}$. Reordenamos los factores para obtener $i = m$, es decir $p_n|q_m$, con lo que $q_m = \pm p_n$. Entonces $p_1 \cdots p_{n-1}p_n = q_1 \cdots q_{m-1}(\pm p_n)$, con lo que $p_1 \cdots p_{n-1} = \pm q_1 \cdots q_{m-1}$ y $n - 1 = m - 1$, luego $n = m$ y además, después de ordenar si hiciera falta, $q_i = \pm p_i$.

Así, para $a \in \mathbb{Z}, a \neq 0, \pm 1$, $a = \pm p_1^{n_1} \cdots p_s^{n_s}$ y estos primos y sus exponentes son únicos (salvo orden). Entonces podemos calcular el $\text{mcd}(a, b)$ tomando el producto de primos comunes a a y b elevados a la mínima potencia y el $\text{mcm}(a, b)$ tomando el producto de primos entre ambos elevados a la máxima potencia.

Como **teorema**, el conjunto de los números primos es infinito. Si no lo fuera, y fuera $\{p_1, \ldots, p_n\}$, el número $N \coloneqq p_1 \cdots p_n + 1$ también lo es.#

6.2. Congruencias

Dados $x, y \in \mathbb{Z}, m \in \mathbb{Z}^+$, x e y son **congruentes módulo** m, $x \equiv y \pmod{m}$ ó $x \equiv y\,(m)$, si $m|x - y$. Esta relación es de equivalencia. Propiedades:

1. Si r es el resto de a/m entonces $a \equiv r\,(m)$.

2. $a \equiv b\,(m) \wedge 0 \leq a, b < m \implies a = b$.

3. $a \equiv b\,(m)$ si y sólo si a y b dan el mismo resto entre m.

4. $a \equiv a'\,(m) \wedge b \equiv b'\,(m) \implies a + b \equiv a' + b'\,(m)$.
   $a - a' = \lambda m$ y $b - b' = \mu m$ para ciertos $\lambda, \mu \in \mathbb{Z}$, luego $(a + b) - (a' + b') = (\lambda + \mu)m$

5. $a \equiv a'\,(m) \wedge b \equiv b'\,(m) \implies ab \equiv a'b'\,(m)$.

$$ab - a'b' = (a' + \lambda m)(b' + \mu m) - a'b' = a'b' + (a'\mu + b'\lambda + \lambda\mu m)m - a'b' \equiv 0\,(m)$$

6. $a \equiv b\,(m) \implies ac \equiv bc\,(m)$. El recíproco es cierto si c y m son coprimos.
   La primera parte se sigue de lo anterior. Para la segunda, $m|ac - bc = (a - b)c \implies m|a - b \implies a \equiv b\,(m)$.

7. $c \neq 0 \implies (a \equiv b\,(m) \iff ac \equiv bc\,(mc))$.
   $a - b = \lambda m \iff ac - bc = \lambda mc$

Denotamos la clase de equivalencia (llamada **clase de congruencia módulo** m) de $a \in \mathbb{Z}$ por $\overline{a}$, y su **representante canónico** es el resto de a/m. Llamamos entonces $\mathbb{Z}/(m)$ o $\mathbb{Z}_m$ al conjunto cociente, que tiene exactamente m elementos. Así, para $\overline{a}, \overline{b} \in \mathbb{Z}_m$, definimos $\overline{a} + \overline{b} = \overline{a + b}$ y $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, y vemos que están bien definidas y que $\mathbb{Z}_m$ es un anillo conmutativo. Dado $\overline{a} \in \mathbb{Z}_m$:

$$\overline{a} \text{ tiene inverso } (\exists \overline{b} \in \mathbb{Z}_m : \overline{a} \cdot \overline{b} = 1) \iff \overline{a} \text{ es cancelable } (\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y} \implies \overline{x} = \overline{y}) \iff$$
$$\iff \operatorname{mcd}(a, m) = 1$$

$1 \implies 2]$ Multiplicando por $\overline{a}^{-1}$ en ambos lados de $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y}$.

$2 \implies 3]$ Si $\operatorname{mcd}(a, m) = d > 1$, sean $a = a'd$ y $m = m'd$, entonces $\overline{a} \cdot \overline{m'} = \overline{a'} \cdot \overline{d} \cdot \overline{m'} = \overline{a'} \cdot \overline{m} = \overline{0} = \overline{a} \cdot \overline{0}$, pero $\overline{m'} \neq \overline{0}$.

$3 \implies 1]$ Existen $r, s \in \mathbb{Z}$ con $ra + sm = 1$, luego $\overline{r} \cdot \overline{a} = 1$.

Así, $\mathbb{Z}_m$ es un cuerpo si y sólo si m es primo, pues entonces todos los elementos tienen inverso.

Un entero es divisible por 3 si y sólo si la suma de sus cifras lo es. **Demostración:** $3|m \iff m \equiv 0\,(3)$. $10 \equiv 1\,(3)$, luego $10^s \equiv 1\,(3)$ para todo s y si m se escribe como $a_n \cdots a_0$, entonces $m = a_n 10^n + \cdots + a_0 \equiv a_n + \cdots + a_0\,(3)$. De forma parecida se pueden sacar reglas para el 9 y el 11.

Dados $a, b, t \in \mathbb{Z}$:

$$\overline{t} \text{ es sol. de } \overline{a}x = \overline{b} \in \mathbb{Z}_m \iff t \text{ es sol. de } ax \equiv b\,(m) \iff \exists s \in \mathbb{Z} : (t, s) \text{ es sol. de } ax - my = b$$

La ecuación $ax \equiv b\,(m)$ tiene solución si y sólo si $d := \operatorname{mcd}(a, m)|b$, y las soluciones son todos los enteros $x = x_0 + \lambda\frac{m}{d}$ con $\lambda \in \mathbb{Z}$, donde x_0 es una solución particular, de modo que la ecuación tiene d soluciones distintas módulo m. **Demostración:** $ax \equiv b$ equivale a la ecuación diofántica $ax - my = b$, que tiene solución si y sólo si $d|b$. Sean pues $b = db'$, $a = da'$ y $m = dm'$, entonces $ax - my = b$ equivale a $a'x - m'y = b'$ y las soluciones son

$$\begin{cases} x &= x_0 + m'\lambda \\ y &= y_0 + a'\lambda \end{cases}$$

Entonces $x_0 + \lambda m' \equiv x_0 + \mu m'\,(m) \iff \lambda m' \equiv \mu m'\,(dm') \iff \lambda \equiv \mu\,(d)$.

6.3. Teorema Chino de los Restos

Sean $b_1, \ldots, b_k \in \mathbb{Z}$ arbitrarios y $m_1, \ldots, m_k \in \mathbb{Z}^+$ coprimos dos a dos, el sistema de congruencias

$$\begin{cases} x \equiv b_1 & (m_1) \\ \quad \vdots & \\ x \equiv b_k & (m_k) \end{cases}$$

tiene solución única módulo $M \coloneqq m_1 \cdots m_k$. En particular, esta es $b_1 M_1 N_1 + \cdots + b_k M_k N_k$, donde $M_i = \frac{M}{M_i}$ y N_i es tal que $M_i N_i \equiv 1\,(m_i)$.

Demostración: Si p es un número primo que divide a M_i y m_i, entonces divide a algún m_j con $j \neq i$, lo cual contradice que $\mathrm{mcd}(m_i, m_j) = 1$, luego M_i y m_i son coprimos y M_i tiene inverso N_i módulo m_i, teniendo en cuenta que $M_i N_i \equiv 0\,(m_j)$ para $j \neq i$. Entonces $x_0 = b_1 M_1 N_1 + \cdots + b_k M_k N_k$ es solución del sistema. Ahora bien, si x e y son soluciones del sistema, $x, y \equiv b_i\,(m_i)$, luego $x \equiv y\,(m_i)$, con lo que $x - y$ es múltiplo de todos los m_i y por tanto $x \equiv y\,(M)$.

Si los módulos no son coprimos, intentamos simplificar cada ecuación dividiéndola entre un número, pues $a'dx \equiv b'd\,(m'd) \iff a'x \equiv b'\,(m')$. Si esto no es posible, resolvemos una ecuación y sustituimos en el resto.

6.4. Teoremas de Euler y Fermat

Denotamos $\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m | x \text{ es invertible}\}$, y definimos la **función ϕ de Euler** como $\phi : \mathbb{N} \to \mathbb{N}$ tal que $\phi(m) = |\{x \in \mathbb{N} | 1 \leq x \leq m \wedge \mathrm{mcd}(x, m) = 1\}| = |\mathbb{Z}_m^*|$. Así:

1. Si p es primo, $\phi(p) = p - 1$.
2. Si p es primo, $\phi(p^n) = p^{n-1}(p-1)$.

   Los no-coprimos con p^n son precisamente los múltiplos de p, por lo que estos son $\frac{p^n}{p} = p^{n-1}$ y $\phi(p^n) = p^n - p^{n-1} = p^n(p-1)$.
3. Si $\mathrm{mcd}(n, m) = 1$, entonces $\phi(nm) = \phi(n)\phi(m)$.

   Definimos $f : \mathbb{Z}_{nm}^* \to \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ tal que $f(x) = (x_n, x_m)$, donde x_n y x_m son los restos de dividir x entre n y m, respectivamente. Para abreviar asumimos que está bien definida, y pasamos a ver que es biyectiva. Si $f(x) = (x_n, x_m) = f(y)$ entonces $x \equiv y\,(m)$ y $x \equiv y\,(n)$, luego $nm | (x - y)$ y en $\mathbb{Z}_{nm}^*$ es inyectiva. Para ver que es suprayectiva, consideramos $(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Al existir una identidad de Bézout $1 = rn + sm$, podemos hacer $x = brn + asm$, con lo que $x \equiv a\,(n)$ y $x \equiv b\,(m)$.
4. Si $m = p_1^{n_1} \cdots p_s^{n_s}$ es la descomposición de m en factores primos, entonces

$$\phi(m) = \prod_{i=1}^{s} p_i^{n_i - 1}(p_i - 1) = m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$

Teorema de Euler: Sea $1 < m \in \mathbb{Z}$. Si a es coprimo con m entonces $a^{\phi(m)} \equiv 1\,(m)$. **Demostración:** Esto equivale a que $\overline{a}^{\phi(m)} = \overline{1} \in \mathbb{Z}_m$. Sea $\mathbb{Z}_m^* = \{\overline{x_1}, \ldots, \overline{x_{\phi(m)}}\}$ y $\overline{a} \cdot \mathbb{Z}_m^* = \{\overline{ax} | \overline{x} \in \mathbb{Z}_m^*\}$. Demostramos que $\overline{a} \cdot \mathbb{Z}_m^* = \mathbb{Z}_m^*$:

$\subseteq]\ x = \overline{ax_i} \in \overline{a} \cdot \mathbb{Z}_m^* \implies x\overline{a}^{-1}\overline{x_i}^{-1} = \overline{1} \implies x \in \mathbb{Z}_m^*.$

$\supseteq]\ \overline{x_i} \in \mathbb{Z}_m^* \implies \overline{x_i} = \overline{a}\,\overline{a}^{-1}\overline{x_i} \in \overline{a} \cdot \mathbb{Z}_m^*.$

Entonces $\prod_{i=1}^{\phi(m)} \overline{x}_i = \prod_{i=1}^{\phi(m)} \overline{ax_i} = \overline{a}^{\phi(m)} \prod_{i=1}^{\phi(m)} \overline{x_i}$, y dividiendo entre $\prod_{i=1}^{\phi(m)} \overline{x_i}$, porque es invertible, se obtiene el resultado.

Teorema Pequeño de Fermat: Si $a \in \mathbb{Z}$ y p es un número primo que no divide a a, entonces $a^{p-1} \equiv 1\,(p)$, y para todo $x \in \mathbb{Z}$, $x^p \equiv x\,(p)$. Esto se deriva del teorema de Euler y de que $\phi(p) = p - 1$.

Capítulo 7

Polinomios

7.1. Polinomios con coeficientes en un cuerpo

Un **polinomio** con coeficientes en el cuerpo K es una expresión de la forma

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX_i$$

con $a_0, \ldots, a_n \in K$. El símbolo X se llama **indeterminada** y llamamos **coeficiente** de grado i a a_i, **término independiente** a a_0 y **coeficiente principal** o **líder** a a_n si es $a_n \neq 0$. Un polinomio es **mónico** si $a_n = 1$. Los polinomios de forma a_0 se llaman **constantes** y los identificamos con los elementos de K. El conjunto de todos los polinomios con coeficientes en K se denota $K[X]$, y dos polinomios $P = a_0 + \cdots + a_nX^n, Q = b_0 + \cdots + b_mX^m \in K[X]$ con $n \leq m$ son iguales si $a_i = b_i$ para $i \in \{1, \ldots, n\}$ y $b_j = 0$ para $j \in \{n+1, \ldots, m\}$.

Definimos $P + Q = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n$, y $PQ = c_0 + c_1X + \cdots + c_{n+m}X^{n+m}$ si $c_k = \sum_{i+j=k} a_ib_j = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$. Así, $K[X]$ es un anillo conmutativo.

P tiene **grado** n si $P = \sum_{i=0}^{n} a_iX^i$ con $a_n \neq 0$, y se denota con $\mathrm{gr}(P)$. Por convención, si $P(X) = 0$, $\mathrm{gr}(P) = -\infty$. Si tomamos el convenio de que $-\infty + n = -\infty$, $(-\infty) + (-\infty) = -\infty$ y $-\infty < n$, se tiene que:

1. $\mathrm{gr}(PQ) = \mathrm{gr}(P) + \mathrm{gr}(Q)$.
2. $\mathrm{gr}(P + Q) \leq \mathrm{máx}\{\mathrm{gr}(P), \mathrm{gr}(Q)\}$.
3. $PQ = 0 \implies P = 0 \vee Q = 0$.
4. $\exists P^{-1} : P^{-1}P = 1 \iff \mathrm{gr}(P) = 0$.

Se define el **valor de** $P(x)$ **en** b como $P(b) = a_0 + a_1b + \cdots + a_nb^n \in K$, con lo que P define una aplicación $P : K \to K$ que llamamos **función polinomial asociada a** K.

Teorema de la división: Para $A, B \in K[X]$ existen dos únicos polinomios, Q (**cociente**) y R (**resto**) en $K[X]$ tales que $A = BQ + R$ y $\mathrm{gr}(R) < \mathrm{gr}(B)$. **Teorema del resto:** El resto de la división de $P/X - a$ es $P(a)$.

Decimos que A divide a B, o que B es múltiplo de A ($A|B$) si $\exists C : B = AC$. Si $A|B \neq 0$, A es un **divisor** de B. Propiedades:

1. $A|B \wedge A|C \implies A|PB + QC$.
2. $A|B \wedge B|C \implies A|C$.
3. $A|B \wedge B|A \implies \exists \mu \in K\backslash\{0\} : A = \mu B$.

Los polinomios de la forma λA para $0 \neq \lambda \in K$ se llaman **polinomios asociados** de A. Cada polinomio tiene un único polinomio asociado mónico.

D es el máximo común divisor de $A, B \in K[X]$ si $D|A, B$, $S|A, B \implies S|D$ y D es mónico. Si D' verifica las dos primeras condiciones, entonces es asociado a D. Además, si $A, B \neq 0$, entonces D es el único polinomio mónico de grado mínimo que es combinación lineal de A y B.

$A, B \in K[X]$ son coprimos o primos entre sí si $\text{mcd}(A, B) = 1$, es decir, si existen $S, T \in K[X]$ tales que $SA + TB = 1$. En tal caso, $A|BC \implies A|C$. Además, si $A, B \in K[X]$ con alguno de los dos no nulo y $D = \text{mcd}(A, B)$, entonces $\frac{A}{D}$ y $\frac{B}{D}$ son coprimos.

M es el mínimo común múltiplo de $A, B \in K[X]$ si $A, B|M$, $A, B|N \implies M|N$ y M es mónico. Si M' cumple las dos primeras condiciones, entonces es asociado a M. Además, existe $\mu \in K$ tal que $\text{mcm}(A, B) = \mu \frac{AB}{\text{mcd}(A,B)}$.

7.2. Raíces de polinomios

$r \in K$ es una **raíz** de $P \in K[X]$ si $P(r) = 0$. Si $\frac{p}{q}$, con p y q coprimos, es raíz de P, entonces $p|a_0$ y $q|a_n$. La **regla de Ruffini** se basa en que a es raíz de P si y sólo si $X - a|P$. Así, decimos que a es una raíz de **multiplicidad** $s \geq 1$ de P si $(X - a)^s|P$ pero no $(X - a)^{s+1}|P$. Una raíz es **múltiple** si tiene multiplicidad mayor que 1, de lo contrario es una raíz **simple**. Si $\text{gr}(P) = n \neq -\infty$, entonces P tiene a lo sumo n raíces en K, contando cada raíz tantas veces como su multiplicidad. Así:

1. Si $\text{gr}(P) = n$ y existen $m > n$ raíces de P en K, entonces $P = 0$.
2. Si $\text{gr}(P) = n \geq 0$ y existen $a_1, \ldots, a_m \in K$ tales que $P(a_i) = Q(a_i)$ con $m > n$, entonces $P = Q$.
3. Si K es un cuerpo infinito y $P, Q \in K[X]$ son distintos, entonces las funciones $P, Q : K \to K$ son distintas.
4. Sea $P = a_0 + \cdots + a_n X^n \in K[X]$ con $\text{gr}(P) = n$ y raíces $r_1, \ldots, r_n$ (no necesariamente distintas), entonces $P = a_n(X - r_1) \cdots (X - r_n)$.

7.3. Factorización y raíces de polinomios

$P \in K[X]$ con $\text{gr}(P) > 0$ es **irreducible** o **primo** si $Q|P \implies \text{gr}(Q) = 0 \vee \exists k \in K : Q = kP$. Así:

$$P \text{ es irreducible} \iff (P|QR \implies P|Q \vee P|R) \iff (P|Q_1 \cdots Q_n \implies \exists i : P|Q_i)$$

Teorema: Todo $P \in K[X]$ con $\text{gr}(P) \geq 1$ factoriza como producto de polinomios irreducibles, y esta factorización es única salvo asociados y orden.

7.4. Polinomios irreducibles en $\mathbb{R}[X]$ y $\mathbb{C}[X]$. Teorema Fundamental del Álgebra

El **Teorema Fundamental del Álgebra** afirma que todo $P \in \mathbb{C}[X]$ con $\text{gr}(P) > 0$ tiene al menos una raíz en $\mathbb{C}$. Así:

1. $P \in \mathbb{C}[X]$ es irreducible si y sólo si $\text{gr}(P) = 1$.
2. $\forall P \in \mathbb{C}[X], \text{gr}(P) = n \geq 1, \exists r, r_1, \ldots, r_n \in \mathbb{C} : P = r(X - r_1) \cdots (X - r_n)$.
3. Si $z \in \mathbb{C}$ es raíz de $P \in \mathbb{R}[X]$, entonces $\overline{z}$ también lo es.
4. Si $P \in \mathbb{R}[X]$ es irreducible, entonces, o $\text{gr}(P) = 1$, o $\text{gr}(P) = 2$ y no tiene raíces reales.