Resultados fundamentales.-

Teorema (Fórmula de De Moivre).- Para todo número natural n, se tiene

$$(\cos(\alpha) + i\text{sen}(\alpha))^n = \cos(n\alpha) + i\text{sen}(n\alpha).$$

Proposición.– Dados tres conjuntos A, B y C se verifican las siguientes igualdades:

(a) Leyes distributivas:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

(b) Leyes de De Morgan (supongamos $A, B \subset C$):

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B), \quad C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$$

Proposición.– Sea A un conjunto, R una relación de equivalencia en A. Entonces se verifican las siguientes propiedades:

(a) Todo elemento pertenece a una clase de equivalencia.

(b) Dos clases de equivalencia son disjuntas o iguales.

Proposición.– Toda permutación distinta de la identidad se puede descomponer en producto de ciclos disjuntos, de manera única (salvo reordenación de los ciclos).

Teorema de división.- Sean $a, b \in \mathbf{Z}_+$, $b > 0$; Existen unos enteros únicos $q, r \in \mathbf{Z}$ tales que:

1. $a = bq + r$
2. $0 \leq r < b$

Al entero q se le llama el *cociente* de la división y a r el *resto*.

Teorema.- Identidad de Bézout Sean $a, b > 0$ enteros y sea $d = \text{mcd}(a, b)$. Existen enteros α, β tales que

$$\alpha a + \beta b = d$$

A cualquier igualdad de este tipo se le llama *identidad de Bézout*.

Teorema de Euclides. Sean $a, b, c > 0$ tales que $c|ab$ y $\text{mcd}(c, a) = 1$; entonces $c|b$. En particular, si p es primo, $p|ab$ y p no divide a a, entonces $p|b$.

Teorema fundamental de la divisibilidad: Toda no unidad distinta de cero se descompone en producto finito de números primos. Esta descomposición es única salvo orden y producto por unidades.

Teorema Chino del resto.- Sean $m_1, m_2, \ldots, m_n$ enteros, mayores que 1, primos entre sí dos a dos, $a_1, a_2, \ldots, a_n \in \mathbf{Z}$. El sistema de congruencias:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

tiene solución. Además, si x y x' son dos soluciones, entonces $x \equiv x' \pmod{M}$, donde $M = m_1 m_2 \cdots m_n$. Recíprocamente, si x es una solución y $x' \equiv x \pmod{M}$, entonces x' es solución.

Teoremas de Fermat y Euler.

Teorema de la raíz.- Sea $f(x) \in k[x]$ un polinomio de grado positivo. Entonces $f(x)$ tiene una raíz $a \in k$ (i.e. existe a en k tal que $f(a) = 0$) si y sólo si es divisible por $x - a$.

Lema de Gauss.- El producto de dos polinomios primitivos es primitivo.

Proposición.- Sean $(G, \cdot)$ un grupo y $H \subset G$ un subconjunto no vacío. Las condiciones siguientes son equivalentes:

1. H es un subgrupo de $(G, \cdot)$.
2. $\forall x, y \in H, x \cdot y^{-1} \in H$.

Teorema de Lagrange.-. Sea G un grupo finito, $H \subset G$ un subgrupo. Entonces $|H|$ divide a $|G|$.

Proposición.- Sea H un subgrupo de un grupo G. Las condiciones siguientes son equivalentes:

1. Las relaciones $\sim_H$ y ${}_H\sim$ coinciden, es decir, $xH = Hx$ para todo $x \in G$.
2. $(xH)(x'H) = (xx')H$, para cualesquiera $x, x' \in G$.
3. Para todo $x \in G$, se tiene $xHx^{-1} \subset H$.
4. Para todo $x \in G$, se tiene $xHx^{-1} = H$.

Proposición.- Sea $f\colon G \to G'$ un homomorfismo de grupos:

1. Si $H \subset G$ es un subgrupo, $f(H)$ es un subgrupo de G'. En particular, la imagen $\mathrm{Im}(f)$ es un subgrupo de G'.
2. Si $H' \subset G'$ es un subgrupo (normal), $f^{-1}(H')$ es un subgrupo (normal) de G. En particular, el núcleo de f, $\ker(f) = f^{-1}(e')$, es un subgrupo normal de G.
3. f es un monomorfismo si y sólo si $\ker(f) = \{e\}$.

Teorema.- *(Primer teorema de isomorfía).* Sea $f\colon G \to G'$ un homomorfismo de grupos. Se induce de modo natural un ismorfismo $\overline{f}\colon G/\ker(f) \to \mathrm{Im}(f)$ que factoriza $f = i \circ \overline{f} \circ \pi$, siendo π el epimorfismo de G sobre $G/\ker(f)$ e i la inclusión de $\mathrm{Im}(f)$ en G'.