INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Física y Matemática

Álgebra Moderna I

Apuntes Álgebra Moderna I

Profesor:
Escobar García César Alberto

Alumnos:
Ramírez León Christian Yael
Silva Sierra Joshua Joaquín

5FM1

22 de diciembre de 2025

Índice general

CAPÍTULO 1
Conceptos Previos

1.1. Divisibilidad

Definición 1.1.1 (Divisibilidad). *Sean* $a, b \in \mathbb{Z}$*, con* $a \neq 0$*, se dice que* $a|b$ *si* $\exists k \in \mathbb{Z}$ *tal que* $b = ak$*.*

Definición 1.1.2 (Máximo Común Divisor). *Sea* $a, b \in \mathbb{Z}$*, al menos uno distinto de cero, definimos a* $d \in \mathbb{Z}$ *un máximo común divisor de* a *y* b*, denotado por* (a, b)*, si cumple:*

i) $d > 0$.

ii) $d|a$ *y* $d|b$.

iii) *Si* $c|a$ *y* $c|b$*, entonces* $c|d$.

Proposición 1.1.1 (Propiedades de la Divisibilidad). *Sean* $a, b, c \in \mathbb{Z}$*, con* $a, b \neq 0$*, entonces:*

i) *Si* $a|b$ *y* $b|c$*, entonces* $a|c$.

ii) *Si* $a|b$ *y* $a|c$*, entonces* $a|(b + c)$.

iii) *Si* $a|b$*, entonces* $a|bk$ *para todo* $k \in \mathbb{Z}$.

iv) *Si* $a|b$ *y* $b \neq 0$*, entonces* $|a| \leq |b|$.

v) *Si* $a|b$ *y* $b|a$*, entonces* $a = \pm b$.

vi) *Si* $a|b$*, entonces* $(a, b) = |a|$.

vii) *Si* $c|a$ *y* $c|b$*, entonces* $c = ax + by$ *para algunos* $x, y \in \mathbb{Z}$.

Proposición 1.1.2. *Sea* $a, b \in \mathbb{Z}$*, al menos uno distinto de cero, entonces existe un único máximo común divisor de* a *y* b*.*

Teorema 1.1.1 (Algoritmo de la división)**.** *Sean $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen únicos $q, r \in \mathbb{Z}$ tales que:*

$$a = bq + r, \quad 0 \leq r < |b|.$$

1.2. Cardinalidad de conjuntos

Dado un conjunto A, se denotará su cardinalidad (número de elementos) como $|A|$. Si A es un conjunto finito, entonces $|A|$ es un número natural. Si A es infinito, entonces $|A| = \infty$.

Observación 1.1. *Sean A, B, conjuntos finitos, con $B \subseteq A$. Entonces:*

$$|A \setminus B| = |A| - |B|$$

En efecto, basta notar que $B \cup (A \setminus B) = A$ y que $B \cap (A \setminus B) = \emptyset$, luego $|A| = |B \cup (A \setminus B)| = |B| + |A \setminus B|$, así $|A \setminus B = |A| - |B|$. □

Observación 1.2 (Observación)**.** *Sean A y B dos conjuntos finitos, entonces:*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

En efecto, Sean A y B conjuntos finitos, note que:

$$A \cup B = (A \setminus (A \cap B)) \cup (B \setminus (A \cap B)) \cup (A \cap B)$$

Además: $(A \setminus (A \cap B))$, $(B \setminus (A \cap B))$, $(A \cap B)$, son disjuntos, más aún:

$$\begin{aligned} |A \setminus (A \cap B)| &= |A| - |A \cap B| \\ |B \setminus (A \cap B)| &= |B| - |A \cap B| \end{aligned}$$

Así:

$$\begin{aligned} |A \cup B| &= |A \setminus (A \cap B)| + |B \setminus (A \cap B)| + |A \cap B| \\ &= |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B| \\ &= |A| + |B| - |A \cap B| \end{aligned}$$

□

Teorema 1.2.1 (Proposición (Principio inclusión exclusión))**.** *Sean $A_1, \ldots, A_n$ conjuntos finitos, se tiene:*

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|$$

Observación 1.3 (Observación)**.** *Suponga que C_1 es la condición que cumplen los elementos A y C_2 los de B, i.e.:*

$$A = \{x \in \Omega : x \textit{ cumple } C_1\}$$
$$B = \{x \in \Omega : x \textit{ cumple } C_2\}$$

Denotemos $N(C_i)$ a la cantidad de elementos que cumplen C_i, $N(C_1, C_2)$ a los que cumplen ambas, $N(\bar{C}_i)$ a los que no cumplen y $N(\bar{C}_1, \bar{C}_2)$ los que no cumplen C_1 ni C_2, entonces:

$$N(\bar{C}_1, \bar{C}_2) = |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2))$$

En efecto, Note que:

$$\begin{aligned} N(\bar{C}_1, \bar{C}_2) &= |A^c \cap B^c| = |(A \cup B)^c| = |\Omega \setminus (A \cup B)| = |\Omega| - |A \cup B| \\ &= |\Omega| - (|A| + |B| - |A \cap B|) \\ &= |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2)) \end{aligned}$$

□

Ejemplo 1.1. *Sea $\Omega = \{x \in \mathbb{Z} : 1 \leq x \leq 1000\}$ ¿Cuántos enteros de estos no son divisibles por 3 o 5?*

Sol. Consideremos:

$$C_1 : x \text{ sea divisible por } 3$$
$$C_2 : x \text{ sea divisible por } 5$$

Así $N(C_1) = 333$, $N(C_2) = 200$, $N(C_1, C_2) = 66$.
Luego:

$$\begin{aligned} N(\bar{C}_1, \bar{C}_2) &= |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2)) \\ &= 1000 - (333 + 200 - 66) \\ &= 533 \end{aligned}$$

Sea $A_1, \ldots, A_n$ una colección finita de conjuntos finitos, definidos:

$$A_i = \{x \in \Omega : x \text{ cumpla } C_i\}, \quad C_i \text{ condición.}$$

Definamos de este modo:

$$
\begin{aligned}
S_1 &= N(C_1) + \cdots + N(C_n) \\
S_2 &= N(C_1, C_2) + \cdots + N(C_1, C_n) + N(C_2, C_3) + \cdots + N(C_{n-1}, C_n) \\
&\vdots \\
S_i &= \sum_{1 \leq j_1 < \ldots < j_i \leq n} N(C_{j_1}, \ldots, C_{j_i}) \\
&\vdots \\
S_n &= N(C_1, \ldots, C_n)
\end{aligned}
$$

Por el principio de inclusión exclusión generalizado:

$$N(\bar{C}_1, \ldots, \bar{C}_n) = |\Omega| - \big(S_1 - S_2 + \cdots + (-1)^{n-1} S_n\big)$$

1.3. Enteros Módulo n

Definición 1.3.1. *Sea $n \in \mathbb{Z}$, $n > 1$, se define la relación de $a \sim b$ si y sólo si $n \mid (a - b)$, es decir, a es congruente con b módulo n.*

Es fácil ver que esta es una relación de equivalencia en $\mathbb{Z}$. Ahora, definamos en el conjunto cociente $(\mathbb{Z}/\sim)$ las siguientes operaciones:

$$
\begin{aligned}
\bar{a} + \bar{b} &= \overline{a + b} \\
\bar{a} \cdot \bar{b} &= \overline{a \cdot b}
\end{aligned}
$$

Con $a, b \in \mathbb{Z}$. Entonces las operaciones están bien definidas, i.e., no dependen del representante de clase.

En efecto, sea $\bar{a} = \bar{a}_1$, $\bar{b} = \bar{b}_1 \iff a \sim a_1$ y $b \sim b_1 \iff n \mid (a - a_1) \wedge n \mid (b - b_1)$.
Esto implica:

$$n \mid (a - a_1) + (b - b_1) = (a + b) - (a_1 + b_1) \iff (a + b) \sim (a_1 + b_1) \iff \overline{a + b} = \overline{a_1 + b_1}$$

Análogamente para el producto.

$\square$

Al conjunto de clases de equivalencia módulo n junto con las operaciones definidas se les denotará por $\mathbb{Z}/n\mathbb{Z}$ o $\mathbb{Z}_n$.