

Teoria de Numeros

Christian Cardenas

Table of Contents

Información	4
1. Clase 2025-08-25	5
1.1. Principio del buen orden PBO	5
1.2. Algoritmo de la division	5
1.3. Principio de inducción matemática (débil) PIM(D)	5
1.4. Ejercicios	5
2. Clase 2025-08-28	6
2.1. $PBO \iff PIM(D)$	6
2.2. Principio de inducción matemática (general) PIM(G)	6
2.3. Principio de inducción matemática (fuerte) PIM(F)	6
2.4. Ejercicios	6
3. Clase 2025-09-01	7
3.1. Sumatorias y Productorios	7
3.2. Suma Telescópica	7
3.3. Ejercicios	7
4. Clase 2025-09-04	8
4.1. Monotonía de una sucesión	8
4.2. Acotamiento de una sucesión	8
4.3. Ejercicios	8
5. Clase 2025-09-08	9
6. Clase 2025-09-11	10
6.1. Quiz	10
7. Clase 2025-09-16	11
7.1. Divisibilidad	11
7.2. Estructuras algebraicas	11
8. Clase 2025-09-18	12
8.1. Ejemplos Estructuras Algebraicas	12
8.2. Anillos	12
8.3. Algoritmo de la division	12
8.4. Máximo Común Divisor	12

9. Clase 2025-09-22	13
10. Clase 2025-09-25	13
11. Clase 2025-09-29	13
12. Clase 2025-10-02	14
12.1. Parcial	14

Información

Profesor: Carlos Andres Giraldo Hernandez

Notas:

Corte 1		
Taller	10%	?
Quiz	5%	11 Sep
Parcial	20%	25 Sep
Corte 2		
Taller	10%	?
Quiz	5%	16 Oct
Parcial	20%	30 Oct
Corte 3		
Parcial	30%	1 Dec

Tutorías: Jueves 10-12, Viernes 8-10 (Biblioteca)

Contenidos:

- Números Naturales
- Números Entero
- Numero Primos
- Divisibilidad
- Teorema Fundamental de la Aritmética
- Congruencias
- Teorema Chino del residuo
- Funciones de la Teoría de Números
- Ecuaciones Diofánticas

Bibliografía: ?

- Niven. I, Zuckerman. N, and Montgomery. H.L, An Introduction to the Theory of Numbers.
- T. Koshy, Elementary Number Theory with applications.

2. Clase 2025-08-28

2.1. PBO \iff PIM(D)

Teorema 2.1

El Principio del buen orden es equivalente al Principio de inducción matemática

Demostración de Teorema 2.1: PBO \iff PIM(D)

1. PBO \implies PIM(D): Sea $S \subseteq \mathbb{N}$, tal que
1. $0 \in S$

2. Si $n \in S$, entonces $n + 1 \in S$.

Supongamos que $S \subsetneq \mathbb{N}$. Como S es no vacío y $S \subsetneq \mathbb{N}$, S^c no es vacío, luego por PBO, S^c tiene mínimo, Sea $m = \min(S)$. Veamos que $m - 1 \in S$. Si $m - 1 \notin S \implies m - 1 \in S^c$. Como $m - 1 < m$, entonces m no sería el mínimo de S^c . Luego $m - 1 \in S$.

- Por 2. Se tiene que $(m - 1) + 1 = m \in S$ lo cual es una contradicción $\rightarrow \leftarrow$
2. PIM(D) \implies PBO: Sea $S \subseteq \mathbb{N}$ no vacío.

Caso 1 ($0 \in S$): Entonces $\min(S) = 0$

Caso 2 ($0 \notin S$): Sea $T = \{x \in \mathbb{N} : \forall s \in S, \quad x < s\} \subseteq S^c$. Como 0 es cota inferior de S y $0 \notin S$, entonces $0 \in T$, además $T \neq \mathbb{N}$, para T se satisfase 1. ($0 \in T$), si 2. es satisfecho por T , entoncecs por el PIM(D) se concluye que $T = \mathbb{N}$ lo cual es una contradicción $\rightarrow \leftarrow$

Por lo tanto PBO \iff PIM(D) □

2.2. Principio de inducción matemática (general) | PIM(G)

Definición 2.2

PIM(G)

Sea $S \subseteq \{x \in \mathbb{N} : x \geq k\} = \mathbb{N}_{\geq k}$ que satisface

1. $k \in S$

2. Si $n \in S$, entonces $n + 1 \in S$

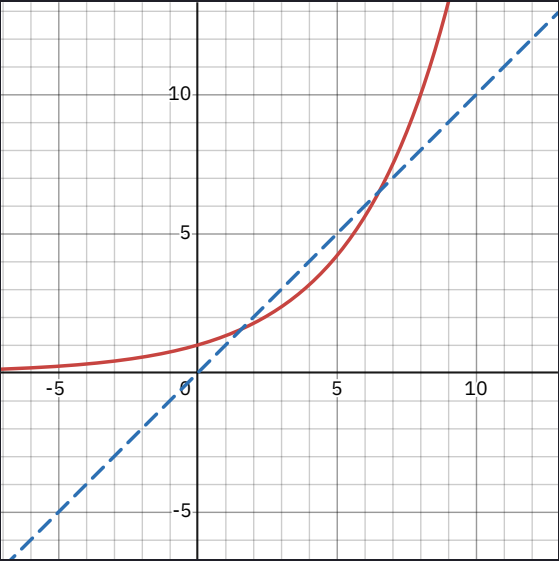
Entonces $S = \mathbb{N}_k = \{k, k + 1, k + 2, \dots\}$

Ejemplo

PIM(G)

Demuestre que $\left(\frac{4}{3}\right)^n > n$

n	$\left(\frac{4}{3}\right)^n > 0$
0	$1 > 0$
1	$1.33 > 1$
2	$1.71 \not> 2$
3	$2.37 \not> 3$
4	$3.16 \not> 4$
5	$4.21 \not> 5$
6	$5.62 \not> 6$
7	$7.49 > 7$
8	$9.99 > 8$



Demostración:

Caso Base: $n = 7, \left(\frac{4}{3}\right)^7 \approx 7.49 > 7$

Paso Inductivo: Supongamos que $\left(\frac{4}{3}\right)^k > k$ para $k \geq 7$ (HI)

$$\left(\frac{4}{3}\right)^k > k$$
$$\left(\frac{4}{3}\right)\left(\frac{4}{3}\right)^k > \frac{4}{3}k$$
$$\left(\frac{4}{3}\right)^{k+1} > \left(1 + \frac{1}{3}\right)k$$
$$\left(\frac{4}{3}\right)^{k+1} > k + \frac{k}{3}$$

Como $k \geq 7$, entonces $\frac{k}{3} \geq \frac{7}{3} > 1$, ahora $k + \frac{k}{3} > k + 1$ por lo tanto

$$\left(\frac{4}{3}\right)^{k+1} > k + 1$$

□

2.3. Principio de inducción matemática (fuerte) | PIM(F)

Definición 2.3

PIM(F)

Sea $S \subseteq \mathbb{N}_{\geq k} = \{k, k + 1, k + 2, \dots\}$ tal que

1. $k \in S$

2. Cada vez que $m \in S$, entonces $m + 1 \in S$ para $m \geq k$

Entonces $S = \mathbb{N}$

2.4. Ejercicios

Desarrollar Ejercicios Libro Rubiano sección 1.3

3. Clase 2025-09-01

3.1. Sumatorias y Productorios

Tanto en las sumatorias como productorios podemos utilizar elementos de un conjuntos y tambien definir condiciones Algunos tipos de sumatorias y productorios

Ejemplo

Sea $I = \{2, 3, 5, 7, 11, 13\}$

$$\sum_{\substack{x \in I \\ x|12}} x = 2 + 3 = 5$$

Ejemplo

Sea $K = \{7, 9, 11\}$

$$\prod_{\substack{i, j \in K \\ i < j}} i^j = 7^9 \cdot 7^{11} \cdot 9^{11}$$
$$\prod_{\substack{i, j \in K \\ i \leq j}} i^j = 7^7 \cdot 7^9 \cdot 7^{11} \cdot 9^9 \cdot 9^{11} \cdot 11^{11}$$

3.2. Suma Telescópica

Definición 3.1

Suma Telescópica

Una suma de la forma $\sum_{i=m+1}^n (a_i - a_{i-1}) = a_n - a_m$ con $n > m + 1$. Se llama suma telescópica

Demostración de la Suma Telescópica por inducción:

- CB: $n = m + 1$

$$\sum_{i=m+1}^{m+2} (a_i - a_{i-1}) = \cancel{a_{m+1}} - a_m + a_{m+2} - \cancel{a_{m+1}} = a_{m+2} - a_m$$

- PI: Supongamos que $\sum_{i=m+1}^n (a_i - a_{i-1}) = a_n - a_m$

$$\begin{aligned} & \sum_{i=m+1}^{n+1} (a_i - a_{i-1}) \\ &= \sum_{i=m+1}^n (a_i - a_{i-1}) + (a_{n+1} - a_n) \\ &= (\cancel{a_n} - a_m) + (a_{n+1} - \cancel{a_n}) \\ &= a_{n+1} - a_m \end{aligned}$$

□

3.3. Ejercicios

Desarrollar Ejercicios Libro Kochi 1.2

4. Clase 2025-09-04

4.1. Monotonía de una sucesión

Definición 4.1

Una sucesión $\{a_n\} = \{a_1, a_2, \dots, a_n, a_{n+1}, \dots\}$ es:

1. Monótona creciente si: $a_1 \leq a_2 \leq \dots \leq a_n \leq a_{n+1} \leq \dots$
2. Monótona decreciente si: $a_1 \geq a_2 \geq \dots \geq a_n \geq a_{n+1} \geq \dots$

4.2. Acotamiento de una sucesión

Definición 4.2

Una sucesión es acotada si $|a_n| \leq M, M \in \mathbb{R}^+$

Nota
Una sucesión es acotada inferiormente si $a_n \geq k, k \in \mathbb{R}$

Nota
Una sucesión es acotada superiormente si $a_n \leq k, k \in \mathbb{R}$

4.3. Ejercicios

Ejercicio 4.3

Demostrar que la siguiente sucesión es monótona y acotada

$$x_1 = 3, \quad x_{n+1} = 2 - \frac{1}{x_n}, \quad n \geq 1$$

Demostración de monotonía:

- Caso base: $x_1 = 3, x_2 = 2 - \frac{1}{3} = 1.\bar{6} \implies x_1 \geq x_2$
- Paso inductivo: Supongamos que $x_n \geq x_{n+1}$, Por hipótesis de inducción

$$\begin{aligned} x_n &\geq x_{n+1} \\ \frac{1}{x_{n+1}} &\geq \frac{1}{x_n} \\ -\frac{1}{x_{n+1}} &\leq -\frac{1}{x_n} \\ 2 - \frac{1}{x_{n+1}} &\leq 2 - \frac{1}{x_n} \\ x_{n+2} &\leq x_{n+1} \end{aligned}$$

Por lo tanto $\{x_n\}$ es monótona decreciente. □

Demostración de acotamiento:

Acotamiento inferior:	Acotamiento superior:
• <i>CB</i> : $x_1 = 3, \quad x_1 \geq 1$	• <i>CB</i> : $x_1 = 3, \quad x_1 \leq 3$
• <i>PI</i> : Supongamos que $x_n \geq 1$, por hipótesis de inducción	• <i>PI</i> : Supongamos que $x_n \leq 3$, por hipótesis de inducción

$\begin{aligned} x_n &\geq 1 \\ 1 &\geq \frac{1}{x_n} \\ -1 &\leq -\frac{1}{x_n} \\ 2 - 1 &\leq 2 - \frac{1}{x_n} \\ 1 &\leq x_{n+1} \end{aligned}$	$\begin{aligned} x_n &\leq 3 \\ \frac{1}{3} &\leq \frac{1}{x_n} \\ -\frac{1}{3} &\geq -\frac{1}{x_n} \\ 2 - \frac{1}{3} &\geq 2 - \frac{1}{x_n} \\ 3 &\geq 1.\bar{6} \geq x_{n+1} \end{aligned}$
---	--

Por lo tanto $\{x_n\}$ es acotada. □

Ejercicio 4.4

Demostrar que la siguiente sucesión es monótona y acotada:

$$x_1 = 4, \quad x_{n+1} = 1 + \sqrt{x_n - 1}, \quad n \geq 1$$

Demostración de monotonía:

- *CB*: $x_1 = 4, \quad x_2 = 1 + \sqrt{3} \approx 2.73$
- *PI*: Supongamos que $x_n \geq x_{n+1}$, por HI

$$\begin{aligned} x_n &\geq x_{x+1} \\ x_n - 1 &\geq x_{x+1} - 1 \\ \sqrt{x_n - 1} &\geq \sqrt{x_{x+1} - 1} \\ 1 + \sqrt{x_n - 1} &\geq 1 + \sqrt{x_{x+1} - 1} \\ x_{n+1} &\geq x_{n+2} \end{aligned}$$

Por lo tanto la sucesión $\{x_n\}$ es monótona decreciente □

Demostración de acotamiento:

- *CB*: $x_1 = 4, \quad 1 \leq x_1 \leq 5$
- *PI*: Supongamos que $1 \leq x_n \leq 5$, por HI.

$$\begin{aligned} 1 &\leq x_n \leq 5 \\ 0 &\leq x_n - 1 \leq 4 \\ 0 &\leq \sqrt{x_n - 1} \leq 2 \\ 1 &\leq 1 + \sqrt{x_n - 1} \leq 3 \\ 1 &\leq x_{n+1} \leq 3 \\ 1 &\leq x_{n+1} \leq 5 \end{aligned}$$

Por lo tanto la sucesión $\{x_n\}$ es acotada. □

Ejercicio 4.5

Demostrar que la siguiente sucesión es monótona y acotada:

$$x_1 = 1, \quad x_{n+1} = \sqrt{2 + x_n}, \quad n \geq 1$$

n	x_n
1	1
2	$\sqrt{3} \approx 1.73$
3	$\sqrt{3.73} \approx 1.93$
4	$\sqrt{3.93} \approx 1.98$
5	$\sqrt{3.98} \approx 1.99$

Demostración de monotonía:

- *CB*: $x_1 = 1, \quad x_2 = \sqrt{3} \approx 1.73 \implies x_1 \leq x_2$
- *PI*: Supongamos que $x_n \leq x_{n+1}$, por hipótesis de inducción

$$x_n \leq x_{n+1} \implies 2 + x_n \leq 2 + x_{n+1} \implies \sqrt{2 + x_n} \leq \sqrt{2 + x_{n+1}} \implies x_{n+1} \leq x_{n+2}$$

Por lo tanto la sucesión $\{x_n\}$ es monótona creciente □

Demostración de acotamiento:

- *CB*: $x_1 = 1, \quad 1 \leq x_1 \leq 2$
- *PI*: Supongamos que $1 \leq x_n \leq 2$, Por hipótesis de inducción

$$\begin{aligned} 1 \leq x_n \leq 2 &\implies 3 \leq 2 + x_n \leq 4 \implies \sqrt{3} \leq \sqrt{2 + x_n} \leq \sqrt{4} \implies 1.73 \leq x_{n+1} \leq 2 \\ &\implies 1 \leq x_{n+1} \leq 2 \end{aligned}$$

Por lo tanto la sucesión $\{x_n\}$ es acotada □

Ejercicio 4.6

Demostrar que la siguiente sucesión es monótona y acotada:

$$x_1 = \sqrt{5}, \quad x_{n+1} = \sqrt{\sqrt{5} + x_n}, \quad n \geq 1$$

n	x_n
1	2.236
2	2.114
3	2.085
4	2.078
5	2.077

Demostración de monotonía:

- *CB*: $x_1 = \sqrt{5} \approx 2.23, \quad x_2 = \sqrt{\sqrt{5} + x_1} \approx 2.11 \implies x_1 \geq x_2$
- *PI*: Supongamos que $x_n \geq x_{n+1}$, por hipótesis de inducción

$$\begin{aligned} x_n &\geq x_{n+1} \implies \sqrt{5} + x_n \geq \sqrt{5} + x_{n+1} \implies \sqrt{\sqrt{5} + x_n} \geq \sqrt{\sqrt{5} + x_{n+1}} \implies \\ x_{n+1} &\geq x_{n+2} \end{aligned}$$

Por lo tanto la sucesión $\{x_n\}$ es monótona decreciente □

Demostración de acotamiento:

- *CB*: $x_1 = \sqrt{5} \implies 2 \leq x_1 \leq 3$
- *PI*: Supongamos que $2 \leq x_n \leq 3$, por hipótesis de inducción

$$\begin{aligned} 2 &\leq x_n \leq 3 \\ \sqrt{5} + 2 &\leq \sqrt{5} + x_n \leq \sqrt{5} + 3 \\ \sqrt{\sqrt{5} + 2} &\leq \sqrt{\sqrt{5} + x_n} \leq \sqrt{\sqrt{5} + 3} \\ 2.05 &\leq x_{n+1} \leq 2.28 \\ 2 &\leq 2.05 \leq x_{n+1} \leq 2.28 \leq 3 \end{aligned}$$

Por lo tanto la sucesión $\{x_n\}$ es acotada □

5. Clase 2025-09-08

Se desarrollaron Ejercicio 4.3 y Ejercicio 4.4

6. Clase 2025-09-11

6.1. Quiz

Ejercicio 6.1

Calcule el valor exacto de $\sum_{n=1}^{1023} \log_2\left(1 + \frac{1}{n}\right)$

$$\begin{aligned} \sum_{n=1}^{1023} \log_2\left(1 + \frac{1}{n}\right) &= \sum_{n=1}^{1023} \log_2\left(\frac{n+1}{n}\right) \\ &= \sum_{n=1}^{1023} (\log_2(n+1) - \log_2(n)) \\ &= \log_2(1024) - \log_2(1) \\ &= 10 - 0 \end{aligned}$$

Ejercicio 6.2

Ejercicio 1.7

Se definen los números F_n de Fermat por $F_n = 2^{2^n} + 1$, $n = \{0, 1, 2, \dots\}$

Demuestre que para todo $n \geq 1$

$$F_0 F_1 F_2 \dots F_{n-1} + 2 = F_n$$

Demostración:

- CB: $n = 1$

$$\begin{aligned} F_0 + 2 &= (2^{2^0} + 1) + 2 = 5 \implies F_0 + 2 = F_1 \\ F_1 &= 2^{2^1} + 1 = 5 \end{aligned}$$

- PI: Supongamos que $F_0 F_1 F_2 \dots F_{n-1} + 2 = F_n$

$$\begin{aligned} F_0 F_1 F_2 \dots F_{n-1} F_n + 2 &= (F_n - 2) F_n + 2 \\ &= (F_n)^2 - 2 F_n + 2 \\ &= (2^{2^n} + 1)^2 - 2(2^{2^n} + 1) + 2 \\ &= (2^{2^n})^2 + \cancel{2 \cdot 2^{2^n}} + 1 - \cancel{2 \cdot 2^{2^n}} - 2 + 2 \\ &= 2^{2^n \cdot 2} + 1 \\ &= 2^{2^{n+1}} + 1 \\ &= F_{n+1} \end{aligned}$$

□

Ejercicio 6.3

Demuestre por que por PBO 1.1 si $x, y \in \mathbb{N}$, entonces $x \geq y$ o $y \geq x$

Demostración: Sean $x, y \in \mathbb{N}$, entonces $\{x, y\} \subseteq \mathbb{N}$. Como $\{x, y\}$ es no vacío, entonces existe $m = \min(\{x, y\})$

- Caso 1: $m = x \wedge m = x \leq y$
- Caso 2: $m = y \wedge m = y \leq x$

□

7. Clase 2025-09-16

7.1. Divisibilidad

Definición 7.1

Divisibilidad

Sean $a, b \in \mathbb{Z}$ con $a \neq 0$, decimos que a divide a b lo cual se denota por $a|b$, si existe $x \in \mathbb{Z}$ tal que $ax = b$, también decimos que b es múltiplo de a . Si lo anterior no se tiene, decimos que a no divide a b lo cual se denota por $a \nmid b$.

En algunos contextos $a^n \parallel b$ significa que $a^n | b$ pero $a^{n+1} \nmid b$

Ejemplo

- 1. $4, 2 : 2(2) = 4 \implies 2|4$
- 2. $2, 8 : 2|8 \wedge 2^2|8 \implies 2 \nmid 8$
- 3. $3, 6 : 3|6 \wedge 3^2 \nmid 6 \implies 3 \parallel 6$

Propiedades

- 1. $a|b \implies a|bc, \quad \forall c \in \mathbb{Z}$
- 2. $a|b \wedge b|c \implies a|c$
- 3. $a|b \wedge a|c \implies a|(bx + cy), \quad \forall x, y \in \mathbb{Z}$
- 4. $a|b \wedge b|a \implies a = \pm b$

Definición 7.2

Sean $a, b \in \mathbb{Z}$, decimos $a \leq b$ si existe $k \in \mathbb{Z}_{\geq 0}$ tal que $a + k = b$

- 5. $a|b \wedge a > 0 \wedge b > 0 \implies a \leq b$
- 6. $a|b \iff am|bm, \quad m \in \mathbb{Z} \wedge m \neq 0 :$

Demostración de propiedades:

- 1. **Demostración:** Por hipótesis $b = ax, \quad x \in \mathbb{Z}$
$$bc = axc \implies a|bc$$

□
- 2. **Demostración:** Por hipótesis $b = ax \wedge c = by, \quad x, y \in \mathbb{Z}$
$$c = by = axy \implies a|c$$

□
- 3. **Demostración:** Por hipótesis $b = an \wedge c = am, \quad n, m \in \mathbb{Z}$
$$bx + cy = anx + amy = a(nx + my) \implies a | (bx + cy)$$

□
- 4. **Demostración:** Por hipótesis $b = ax \wedge a = by, \quad x, y \in \mathbb{Z}$
$$\begin{aligned} a &= by = axy \implies axy - a = 0 \\ &\implies a(xy - 1) = 0 \\ &\implies \begin{cases} a = 0 \\ xy = 1 \end{cases} \implies \begin{cases} x=1=y \\ x=-1=y \end{cases} \end{aligned}$$
 - 1. $b = a(1) \implies b = a$
 - 2. $b = a(-1) \implies b = -a$

□
- 5. **Demostración:** Por hipótesis $b = ax \wedge a > 0 \wedge b > 0, \quad x \in \mathbb{Z}$
$$a > 0 \wedge b > 0 \implies x > 0$$
 - 1. $x = 1 \implies b = a$
 - 2. $x \geq 2 \implies b = ax = \underbrace{a + a + \dots + a}_{x \text{ veces}} = a + (k - 1)a$, donde $(k - 1) > 0$, entonces
$$a < b$$

Por lo tanto $a \leq b$

□
- 6. **Demostración:**
 - $a|b \implies am|bm :$ Por hipótesis $b = ax, \quad x \in \mathbb{Z}$
$$bm = axm = (am)x \implies am | bm$$
 - $am|bm \implies a|b :$ Por hipótesis $bm = amx, \quad x \in \mathbb{Z}$
Como $m \neq 0$
$$bm = amx \implies b = ax \implies a|b$$

□

7.2. Estructuras algebraicas

Definición 7.3

Dado un conjunto no vacío A , una **operación binaria** $*$ sobre A , es una función

$$\begin{aligned} * : A \times A &\longrightarrow A \\ (a, b) &\longrightarrow * (a, b) \end{aligned}$$

Notación: $*(a, b) = a * b$

Ejemplo

- 1. Suma en naturales es una operación binaria
$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (x, y) &\longrightarrow x + y \end{aligned}$$
- 2. Multiplicación en enteros es una operación binaria
$$\begin{aligned} \cdot : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\longrightarrow x \cdot y \end{aligned}$$
- 3. La suma en $\mathbb{Z}_3 = \{0, 1, 2\}$ es una operación binaria

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$$\begin{aligned} +_3 : \mathbb{Z}_3 \times \mathbb{Z}_3 &\longrightarrow \mathbb{Z}_3 \\ (2, 1) &\longrightarrow 2 +_3 1 = 0 \end{aligned}$$
- 4. La resta en \mathbb{N} no es una operación binaria
$$(\mathbb{N}, -) \quad 5 - 7 = -2$$
- 5. La division en \mathbb{R} no es una operación binaria
$$(\mathbb{R}, \div) \quad \frac{5}{0} \text{ no esta definido}$$
- 6. La division en $\mathbb{R} \setminus \{0\}$ es una operación binaria
$$\begin{aligned} (\mathbb{R} \setminus \{0\}, \div) \\ \div : \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (x, y) &\longrightarrow \frac{x}{y} \end{aligned}$$

Definición 7.4

Sea A un conjunto no vacío y $*$ una operación binaria sobre A . Decimos que:

- 1. $*$ es asociativa si:
$$(\forall x, y, z \in A)((x * y) * z = x * (y * z))$$
- 2. $*$ es modulativa si:
$$(\exists e \in A)(\forall x \in A)(e * x = x * e = x)$$
- 3. $*$ es invertiva si:
$$(\forall x \in A)(\exists x' \in A)(x * x' = e = x' * x)$$
- 4. $*$ es conmutativa si:
$$(\forall x, y \in A)(x * y = y * x)$$

Una pareja $(A, *)$ se dice:

- 1. **Semi-grupo** si $*$ es asociativa.
- 2. **Monoide** si $*$ es asociativa y modulativa.
- 3. **Grupo** si $*$ es asociativa, modulativa e invertiva.
- 4. **Grupo Abelian** si $*$ es asociativa, modulativa, invertiva y conmutativa.

8. Clase 2025-09-18

8.1. Ejemplos Estructuras Algebraicas

EjemploSemi-grupos

1. $(\mathbb{N}_{>0}, +)$
Sea $x, y, z \in \mathbb{N}$
 \checkmark Es asociativa $x + (y + z) = (y + x) + z$
 \checkmark No existe e tal que $x + e = e + x = x$

2. $(A, *)$:

$*$	a	b
a	a	a
b	b	b

 \checkmark Es asociativa
 $a * (a * a) = a = (a * a) * a$
 $a * (a * b) = a = (a * a) * b$
 $a * (b * a) = a = (a * b) * a$
 $b * (a * a) = b = (b * a) * a$
 \checkmark No existe $e \in A$ tal que $e * x = x * e = x$
$$e = a \implies \begin{cases} a * e = a = e * a \\ b * e = b \neq a = e * b \end{cases} \implies a \text{ no es neutro}$$

$$e = b \implies \begin{cases} a * b = a \neq b = b * a \\ b * b = b = b * b \end{cases} \implies b \text{ no es neutro}$$

EjemploMonoides

1. $(\mathbb{N}, +)$
Sea $x, y, z \in \mathbb{N}$
 \checkmark Es asociativa: $x + (y + z) = (y + x) + z$
 \checkmark Es modulativa: Existe $0 \in \mathbb{N}$ tal que $x + 0 = 0 + x = x$
 \checkmark No es invertiva: No existe x' tal que $x + x' = 0 = x' + x$

2. $(\mathcal{P}(A), \cup)$
Sea $x, y \in \mathcal{P}(A)$
 \checkmark Es asociativa: $x \cup y = y \cup x$
 \checkmark Es modulativa: Existe $\emptyset \in \mathcal{P}(A)$ tal que $x \cup \emptyset = \emptyset \cup x = x$
 \checkmark No es invertiva: No existe $x' \in \mathcal{P}(A)$ tal que $x \cup x' = \emptyset = x' \cup x$

EjemploGrupos

1. $(GL_n(\mathbb{R}), \cdot)$

EjemploGrupos Abelianos

1. $(\mathbb{Z}, +)$
Sea $x, y, z \in \mathbb{Z}$
 \checkmark Es asociativa: $x + (y + z) = (x + y) + z$
 \checkmark Es modulativa: Existe $0 \in \mathbb{Z}$ tal que $x + 0 = 0 + x = x$
 \checkmark Es invertiva: Existe x' tal que $x + x' = 0 = x' + x$
 \checkmark Es conmutativa: $x + y = y + x$

2. $(\mathbb{R}, +)$ Sea $x, y, z \in \mathbb{R}$
 \checkmark Es asociativa: $x + (y + z) = (x + y) + z$
 \checkmark Es modulativa: Existe $0 \in \mathbb{R}$ tal que $x + 0 = 0 + x = x$
 \checkmark Es invertiva: Existe x' tal que $x + x' = 0 = x' + x$
 \checkmark Es conmutativa: $x + y = y + x$

8.2. Anillos

Definición 8.1Anillos

Sea A un conjunto y $*_1, *_2$ operaciones binarias sobre A la tripla $(A, *_1, *_2)$ se dice anillo si:

1. $(A, *_1)$ es un grupo abeliano.

2. $*_2$ es asociativa.

3. Se cumple:
$$(\forall x, y \in A) (\quad x *_2 (y *_1 z) = (x *_2 y) *_1 (x *_2 z) \wedge$$
$$(y *_1 z) *_2 x = (y *_2 x) *_1 (z *_2 x) \quad)$$

La operación $*_1$ se suele llamar **suma** y se suele denotar por $+$.
La operación $*_2$ se suele llamar **producto** y se suele denotar por \cdot .

- Si $*_2$ es conmutativa en A , se llama **anillo conmutativo**.
- Si $*_2$ es conmutativa y modulativa en A , se llama **anillo conmutativo de identidad**.
- Si $*_2$ es invertiva en $A \setminus \{e\}$, siendo e el modulo de $*_1$, se llama **anillo de division**.
- A se dice **dominio de integridad (DI)** si cada vez que $a *_2 b = e$ se tiene que $a = e \vee b = e$

Ejemplo

1. $(\mathbb{Z}, +, \cdot)$

- $(\mathbb{Z}, +)$ es un grupo abeliano.
- \cdot es distributivo con respecto a $+$.
- \cdot es asociativo.
- 1 es el modulo multiplicativo.
- Siempre que $a \cdot b = 0 \implies a = 0 \vee b = 0$

 $(\mathbb{Z}, +, \cdot)$ es **Anillo conmutativo con identidad que es dominio de integridad**.

2. $(2\mathbb{Z}, +, \cdot), \quad 2\mathbb{Z} = \text{enteros pares}$

- $(2\mathbb{Z}, +)$ es grupo abeliano.
- \cdot distribuye con respecto a $+$.
- \cdot es asociativo.
- No hay modulo multiplicativo.
- Siempre que $a \cdot b = 0 \implies a = 0 \vee b = 0$.

 $(2\mathbb{Z}, +, \cdot)$ es **Anillo conmutativo sin identidad que es dominio de integridad**

3. $(\mathbb{R}, +, \cdot)$

- $(\mathbb{R}, +)$ es grupo abeliano.
- \cdot distribuye con respecto a $+$.
- \cdot es asociativo.
- 1 es modulo multiplicativo.
- \cdot es invertiva en $\mathbb{R} \setminus \{0\}$ siendo 0 modulo de $+$
- Siempre que $a \cdot b = 0 \implies a = 0 \vee b = 0$.

 $(\mathbb{R}, +, \cdot)$ es **Anillo conmutativo con identidad que es de division y dominio de integridad**

4. $(\mathbb{Z}_4, +, \cdot)$
 $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

\cdot	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- $(\mathbb{Z}_4, +)$ es grupo abeliano.
- \cdot es conmutativo.
- No hay modulo multiplicativo.
- No se cumple que $a \cdot b = e \implies a = e \vee b = e$ ya que $2 \cdot 2 = 0$

 $(\mathbb{Z}_4, +, \cdot)$ es **Anillo conmutativo sin identidad (no es DI)**.

8.3. Algoritmo de la division

Definición 8.2Algoritmo de la division

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tal que:

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

Ejemplo

$-7, 3 :$

$-7 = 3(-3) + 2, \quad 0 \leq 2 < 3$
 $3 = -7(0) + 3, \quad 0 \leq 3 < |-7|$

8.4. Máximo Común Divisor

Definición 8.3

Sean $a, b \in \mathbb{Z}$ no nulos simultáneamente, el **máximo común divisor** de a y b , denotado por (a, b) o $\text{mcd}(a, b)$ es el mas grande de los divisores comunes de a y b . Si $(a, b) = 1$, decimos que a y b son co-primos o primos relativos.

Ejemplo

14, 42 : $\text{div}(14) = \{\pm 1, \pm 2, \pm 7, \pm 14\}$
 $\text{div}(42) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}$

Divisores comunes de 14 y 42 son $\{\pm 1, \pm 2, \pm 7, \pm 14\}$

$\max\{\pm 1, \pm 2, \pm 7, \pm 14\} = 14 \implies (14, 42) = 14$

Nota

1. $a|0$ si existe $x \in \mathbb{Z}$ tal que $0 = ax$
Entonces $\text{div}(0) = \mathbb{Z}, a|0$ porque $a \cdot \underbrace{0}_x = 0$
Por ello no se puede considerar $(0, 0)$ porque los divisores comunes de 0 y 0 es \mathbb{Z}

2. $a \neq 0, \quad (a, 0) = |a|$

Teorema 8.4

Sea $a, b \in \mathbb{Z}$ no nulos simultáneamente, entonces existen $x_0, y_0 \in \mathbb{Z}$ tal que:

$$(a, b) = ax_0 + by_0$$

Demostración: Sea $S = \{ax + by : x, y \in \mathbb{Z} \wedge ax + by > 0\} \subseteq \mathbb{N}$

1. Si $a \leq b$ entonces:

- $a = b \wedge a > 0 \implies a(1) + b(1) \in S$
- $a = b \wedge a < 0 \implies a(-1) + b(-1) \in S$
- $a < b \implies b - a > 0 \implies a(-1) + b(1) \in S$

«El razonamiento para $a \geq b$ es análogo.»
Entonces S es no vacío, por PBO tiene mínimo

2. Como $\min(S) \in S$, existe $x_0, y_0 \in \mathbb{Z}$ tal que
$$\min(S) = ax_0 + by_0$$

$$(a, b)|a \wedge (a, b)|b \implies (a, b)|\min(S)$$

Como $(a, b)|\min(S) \wedge (a, b) > 0 \wedge \min(S) > 0 \implies \boxed{(a, b) \leq \min(S)}$
Por algoritmo de Euclides existen q, r únicos tal que
$$a = \min(S)q + r, \quad 0 \leq r < \min(S)$$

$$\begin{aligned} r &= a - \min(S)q \\ &= a - q(ax_0 + by_0) \\ &= a - ax_0q - by_0q \\ &= a(1 - x_0q) + b(-y_0q) \end{aligned}$$

Si $r > 0$, entonces $r \in S \implies r \geq \min(S)$ Lo cual es una contradicción, por lo tanto $r = 0 \implies a = \min(S)q \implies \min(S)|a$
«El razonamiento para $\min(S)|b$ es análogo»

Duda: Como $\min(S)|a \wedge \min(S)|b \implies \min(S)|(a, b) \implies \min(S) \leq (a, b)$

Por lo tanto $\min(S) \leq (a, b) \wedge \min(S) \geq (a, b) \implies \min(S) = (a, b)$

□

Ejemplo

$(42, 105) = 21$

42	2	105	3
21	3	35	5
7	7	7	7
1		1	

$21 = 42(-2) + 105(1)$
 $21 = 42(3) + 105(-1)$

9. Clase 2025-09-22

Se hizo demostración de Teorema 8.4

10. Clase 2025-09-25

No clase por evento

11. Clase 2025-09-29

Se hizo demostración de Ejercicios 1,3,4 del Taller 1

12. Clase 2025-10-02

12.1. Parcial

Ejercicio 12.1

Realizar los siguientes cálculos:

1. $\sum_{j=1}^5 \sum_{i=1}^4 (i^2 - j + 1)$

$$\begin{aligned} \sum_{j=1}^5 \sum_{i=1}^4 (i^2 - j + 1) &= \sum_{j=1}^5 (2 - j + 5 - j + 10 - j + 17 - j) \\ &= \sum_{j=1}^5 (34 - 4j) \\ &= \sum_{j=1}^5 34 - \sum_{j=1}^5 4j \\ &= 5 \cdot 34 - (4 + 8 + 12 + 16 + 20) \\ &= 170 - 60 \\ &= 110 \end{aligned}$$

2. $\prod_{\substack{d \geq 1 \\ d|12}} \left(\frac{12}{d}\right)$

$d \in \{1, 2, 3, 4, 6, 12\}$

$$\begin{aligned} \prod_{\substack{d \geq 1 \\ d|12}} \left(\frac{12}{d}\right) &= \frac{12}{1} \cdot \frac{12}{2} \cdot \frac{12}{3} \cdot \frac{12}{4} \cdot \frac{12}{6} \cdot \frac{12}{12} \\ &= 12 \cdot 6 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= 12^3 \\ &= 1728 \end{aligned}$$

3. $(963, 657)$

$$\begin{array}{r|l} 963 & 3 \\ 321 & 3 \\ 107 & 107 \\ 1 & 1 \end{array} \quad \begin{array}{r|l} 657 & 3 \\ 219 & 3 \\ 73 & 73 \\ 1 & 1 \end{array}$$
$$\begin{aligned} 963 &= 3^2 \cdot 73^0 \cdot 107^1 \\ 657 &= 3^2 \cdot 73^1 \cdot 107^0 \\ (963, 657) &= 3^2 \cdot 73^0 \cdot 107^0 = 9 \end{aligned}$$

4. Expresé $(36, 63)$ como combinación lineal entera de 36 y 63.

$$\begin{array}{r|l} 36 & 2 \\ 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & 1 \end{array} \quad \begin{array}{r|l} 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & 1 \end{array}$$
$$\begin{aligned} 36 &= 2^2 \cdot 3^2 \cdot 7^0 \\ 63 &= 2^0 \cdot 3^2 \cdot 7^1 \\ (36, 63) &= 2^0 \cdot 3^2 \cdot 7^0 = 9 \end{aligned}$$

$$(36, 63) = 36(2) + 63(-1) = 72 - 63 = 9$$

Ejercicio 12.2

Demuestra que si $m > 0$, entonces $(ma, mb) = m(a, b)$

Demostración: Sea $S_1 = \{max + mby : x, y \in \mathbb{Z} \wedge max + mby > 0\}$

$$(ma, mb) = \min(S_1) = max_0 + mby_0 = m(ax_0 + by_0)$$

Como $m(ax_0 + by_0) > 0$ y $m > 0$, entonces $ax_0 + by_0 > 0$

Sea $S_2 = \{ax + by : x, y \in \mathbb{Z} \wedge ax + by > 0\}$

$$m(ax_0 + by_0) = m \cdot \min(S_2) = m(a, b)$$

Por lo tanto $(ma, mb) = m(a, b)$ □

Ejercicio 12.3

Considere la sucesión de números reales (x_n) , la cual se define por

$$x_1 = 3, \quad x_{n+1} = 2 - \frac{1}{x_n}, \quad n \geq 1$$

1. Explícite los primeros 6 términos de la sucesión.

$$\begin{aligned} x_1 &= 3 \\ x_2 &= 2 - \frac{1}{3} = \frac{5}{3} = 1.\bar{6} \\ x_3 &= 2 - \frac{3}{5} = \frac{7}{5} = 1.4 \\ x_4 &= 2 - \frac{5}{7} = \frac{9}{7} \approx 1.285 \\ x_5 &= 2 - \frac{7}{9} = \frac{11}{9} = 1.\bar{2} \\ x_6 &= 2 - \frac{9}{11} = \frac{13}{11} = 1.\bar{18} \end{aligned}$$

n	1	2	3	4	5	6
x_n	3	$\frac{5}{3}$	$\frac{7}{5}$	$\frac{9}{7}$	$\frac{11}{9}$	$\frac{13}{11}$

2. Demuestre por inducción que $1 \leq x_n \leq 3$

Demostración:

- Caso base: $n = 1$, $x_1 = 3$, $1 \leq x_1 \leq 3$
- Paso inductivo: Supongamos que $1 \leq x_n \leq 3$.

Por HI

$$1 \leq x_n \implies \frac{1}{x_n} \leq 1 \implies -\frac{1}{x_n} \geq -1 \implies 2 - \frac{1}{x_n} \geq 1 \implies x_{n+1} \geq 1$$

Por HI

$$x_n \leq 3 \implies \frac{1}{3} \leq \frac{1}{x_n} \implies -\frac{1}{3} \geq -\frac{1}{x_n} \implies 2 - \frac{1}{3} \geq 2 - \frac{1}{x_n} \implies \frac{5}{3} \geq x_{n+1}$$

Por lo tanto $1 \leq x_{n+1} \leq \frac{5}{3} < 3$

□

3. Demuestre por inducción que (x_n) es monótona decreciente

Demostración:

- Caso base: $n = 2$, $x_1 = 3$, $x_2 = \frac{5}{3}$, $x_1 > x_2$
- Paso inductivo: Supongamos $x_n > x_{n+1}$

Por HI

$$\begin{aligned} x_n > x_{n+1} &\implies \frac{1}{x_{n+1}} > \frac{1}{x_n} \implies -\frac{1}{x_{n+1}} < -\frac{1}{x_n} \implies 2 - \frac{1}{x_{n+1}} < 2 - \frac{1}{x_n} \\ &\implies x_{n+2} < x_{n+1} \end{aligned}$$

□