Álgebra I - Teoría I

Silvano Picard

Abril 2024

Índice general

Capítulo 1

Conjuntos, Relaciones y Funciones

1.1. Conjuntos

Se dice conjunto a una colección de objetos, los cuales son llamados elementos. Un ejemplo de conjunto puede ser: $A = 1, 2, 3, 7, 8$. Al definir un conjunto no importa el orden y tampoco la repetición, ya que en este último caso cuentan como si aparecieran una sola vez. Un conjunto puede describirgse de dos maneras:

- Por comprensión: $\mathbb{Q} = \left\{\frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{N}\right\}$
- Por extensión: $\mathbb{N} = \{1, 2, 3, 4, ...\}$

1.1.1. Pertenencia

Respecto al conjunto vacío éste no pertenece a otro conjunto a menos que sea explicitado. Entonces si A es un conjunto definido como $A = \{1, 2, 3, 4\} \Rightarrow \emptyset \notin A$ luego si B es otro conjunto definido como $B = \{3, 5, \emptyset, 8\} \Rightarrow \emptyset \in B$.

1.1.2. Inclusión

Sean A y B conjuntos. Se dice que B está incluido en A cuando todos los elementos de B pertenecen a A: $B \subseteq A \iff \forall x : x \in B \Rightarrow x \in A$.

Se dice que B no está incluido en A cuando algún elemento de B no pertenece a A: $B \nsubseteq A \iff \exists x \in B : x \notin A$.

Entonces tenemos las siguientes afirmaciones tautológicas:

- $A \subseteq A$
- $\emptyset \subseteq A$

1.1.3. Conjunto de partes

Los elemtos de $p(a)$ son los subconjuntos de A: $B \in p(a) \iff B \subseteq A$. Así tengo que $p(\emptyset) = \{\emptyset\}$ por tanto $\emptyset \in p(\emptyset)$ pues $\emptyset \subseteq \emptyset$

1.1.4. Operaciones entre conjuntos

Complemento

Siendo A y U conjuntos defino el complemento de A como: $A \subseteq U \Rightarrow A^c \subseteq U, x \in A^c \iff x \in U \wedge x \notin A$

Unión

Siendo A,B,U conjuntos y $A, B \subseteq U$, la unión de A y B se define como: $A \cup B = \{x \in U : x \in A \vee x \in B\}$. Entonces tengo que $A \cup B = B \cup A$, $A \cup \emptyset = A$, $A \cup U = U$ y $A \cup A^c = U$

Intersección

Siendo A,B,U conjuntos tales que $A, B \subseteq U$. La intersección de A y B se escribe como: $A \cap B = \{x \in U : x \in A \wedge x \in B\}$.

Entonces tengo que:

- $A \cap B = B \cap A$
- $A \cap \emptyset = \emptyset$
- $A \cap U = A$
- $A \cap A^c = \emptyset$
- $A \cap B = B \iff B \subseteq A$

Por tanto puedo decir que $\emptyset \subseteq (A \cap B) \subseteq (A \cup B) \subseteq U$.

Leyes de De Morgan

Siendo A,B,U conjuntos tales que $A, B \subseteq U$ tengo que:

- $(A \cup B)^c = A^c \cap B^c$
- $(A \cap B)^c = A^c \cup B^c$

Diferencia

Sean A,B,U conjuntos y $A, B \subseteq U$ defino la diferencia entre A y B como: $A \setminus B = \{x \in A : x \notin B\}$

Entonces si $A \cap B = \emptyset \Rightarrow [(A \setminus B = A) \wedge (B \setminus A = B)]$ y además:

- $A \setminus B \neq B \setminus A$ (en general)
- $A \setminus \emptyset = A$
- $A \setminus U = \emptyset$
- $\emptyset \setminus A = \emptyset$
- $U \setminus A = A^c$

Diferencia Simétrica

Sean A,B,U conjuntos tales que $A, B \subseteq U$ defino la diferencia simétrica como: $A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

Entonces tengo que:

- $A \triangle B = B \triangle A$
- $A \triangle \emptyset = A$
- $A \triangle U = A^c$
- $A \triangle A = \emptyset$
- $A \triangle A^c = U$

Propiedad distributiva en conjuntos

- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
- $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

Producto cartesiano

Siendo A,B,U,V conjuntos tales que $A \subseteq U$ y $B \subseteq V$ defino el producto cartesiano como: $A \times B = \{(a, b) : a \in A \wedge b \in B\} \subseteq U \times V$

De esta forma puedo establecer las siguientes afirmaciones:

- $A \times B = B \times A \iff A = B$
- $A \times \emptyset = \emptyset$
- $\emptyset \times B = \emptyset$
- $U \times V = \{(x, y)/x \in V \wedge y \in V\}$

1.2. Relaciones

Sean A,B conjuntos, una relación R de A en B es un subconjunto (cualquiera) de $A \times B$ osea que: R relación de A en B $\iff R \subseteq A \times B \iff R \in p(A \times B)$.

Un ejemplo puede ser $A = \{a, b, c\}$ y $B = \{1, 2\}$ y $R_1 = \{(a, 1), (b, 1), (b, 2)\}$. Otros útiles pueden ser $R_2 = \emptyset$ (nadie está relacionado con nadie) y $R_3 = A \times B$ (todos están relacionados con todos).

1.2.1. Relaciones de un conjunto en sí mismo

Sea A un conjunto. Una relación en A es un subconjunto (cualquiera) de $A \times A$ (A^2). R relación en A $\iff R \subseteq A^2 \iff R \in p(A^2)$

Propiedades

Sea $R \in p(A^2)$ una relación en A:

- R es reflexiva si $\forall x \in A$ se tiene xRx
- R es simétrica si $\forall x, y \in A$ x tiene xRy $\Rightarrow$ yRx
- R es transitiva si $\forall x, y, z \in A$ se tiene xRy $\wedge$ yRz $\Rightarrow$ xRz
- R es antisimétrica si $\forall x, y \in A$ se tiene xRy $\wedge$ yRx $\Rightarrow$ x=y, lo cual es lo mismo que decir $\forall x, y \in A$ si $x \neq y$ y xRy $\Rightarrow y \not R x$

1.2.2. Relaciones de equivalencia y relaciones de orden

Sea R una relación en A entonces R es una relación de equivalencia si R es reflexiva, simétrica y transitiva.

Luego, se dice que R es una relación de orden si R es reflexiva, antisimétrica y transitiva

1.2.3. Particiones y clases de equivalencia

Se dice clase de equivalencia de x cuando tengo un conjunto de todos los elementos relacionados con ese x. Por ejemplo si tengo un $R = \{(2,5),(2,8)\}$ tengo que la clase de equivalencia de 2 es: $[2] = \{5, 8\}$

1.3. Funciones

Dados X, Y conjuntos. Una funcion $f : X \to Y$ es una asignación que a cada elemento $x \in X$ le asigna un elemento y (solo uno) de Y. Se nota $y = f(x)$.

$R = \{(x, y) \in X \times Y\}$. R relación es una fucnión $\iff \forall x \in X, \exists y \in Y : (x, y) \in R$ y además y es único. Es decir que a $\forall x \in X, \exists! y \in Y : (x, y) \in R$ se lo llama $y = f(x)$.

$f : X \to Y$ es la función nula si $f(x) = 0, \forall x \in X$. Además f y g son iguales como funciones si: $f, g : X \to Y : f = g \iff f(x) = g(x), \forall x \in X$

1.3.1. Imagen y dominio de f

Se define la imagen de f como: $Im(f) = \{y \in Y : \exists x \in X : f(x) = y\} \subseteq Y$. La imagen es un subconjunto del conjunto de llegada, $Im(f) \subseteq Y$.

El dominio es lo mismo que el conjunto de partida (para nosotros).

1.3.2. Inyectividad, sobreyectividad y biyectividad

Sea $f : X \to Y$,

- f es inyectiva $\iff \forall x_1, x_2 \in X, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ o también se puede ver como: f es inyectiva $\iff \forall x_1, x_2 \in X, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

- f es sobreyectiva $\iff Im(f) = Y$
- f es biyectiva $\iff$ f es inyectiva y sobreyectiva

1.3.3. Función inversa

Sea $f : X \to Y$ biyectiva, osea $\forall y \in Y, \exists ! x : y = f(x)$, entonces $f^{-1} : Y \to X, f^{-1}(y) = x \iff f(x) = y$. Por definición, la función inversa f^{-1} es biyectiva y $(f^{-1})^{-1} = f$.

1.3.4. Composición de funciones

Sea $f : X \to Y$ entonces tengo que: $f^{-1}(f(x)) = x, \forall x \in X$ es decir que $f^{-1} \circ f = id_x \to f^{-1} \circ f(x) = f^{-1}(f(x))$.

También vale que $(f \circ f^{-1})(y) = f(f^{-1}(y)) = y, \forall y \in Y : f \circ f^{-1} = id_y$. Entonces podemos concluir que se cumple $f \circ f^{-1} = id_y$ y $f^{-1} \circ f = id_x$.

Capítulo 2

Numeros Naturales e Inducción

2.1. Sumatoria y productoria

- Suma de Gauss: $\forall n \in \mathbb{N}, S_n = \frac{n(n+1)}{2} = \sum_{i=1}^{n} i$
- Suma geométrica: $Q_n = \sum_{k=0}^{n} q^k$. Escrito de otra manera implica que si $q \neq 1$ entonces $Q_n = \frac{q^{n+1}-1}{q-1}$ y si q = 1 entonces $Q_n = n + 1$.

2.1.1. Propiedades de la sumatoria y la productoria

- $\sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k = \sum_{k=1}^{n}(a_k + b_k)$
- $c \cdot \sum_{k=1}^{n} a_k = \sum_{k=1}^{n}(c \cdot a_k)$
- $\sum_{k=1}^{n+1} a_k = \sum_{k=1}^{n} a_k + a_{n+1}$

Las propiedades escritas para la sumatoria también aplican para la productoria.

2.1.2. Principios de Inducción

Sea p(n) una proposición sobre $\mathbb{N}$ $(\forall n, p(n)V \vee p(n)F)$ tengo la pregunta: ¿p(n) verdadero para todo $n \in \mathbb{N}$?. Además tengo que un conjunto inductivo se define de la siguiente manera:

Sea $H \subseteq \mathbb{N}$ es inductivo si:

- $1 \in H$
- $\forall h \in \mathbb{R}, h \in H \Rightarrow h + 1 \in H$

Principio de Inducción I

Sea p(n) una proposición sobre $\mathbb{N}$, si se cumple:

- p(1)V
- $\forall h \in \mathbb{N}, p(h)V \Rightarrow p(h+1)V$

Entonces tengo que p(n) es verdadero $\forall n \in \mathbb{N}$

Principio de Inducción II

Sea $n_0 \in \mathbb{Z}$ y sea p(n) una proposición sobre $\mathbb{Z}_{\geq n_0}$, si se cumple:

- p(n_0) es V
- $\forall h \in \mathbb{Z}_{\geq n_0}$, p(h) V $\Rightarrow$ p(h+1)V

Entonces puedo afirmar que p(n) es V $\forall n \geq n_0$

Principio de Inducción III

Sea p(n) una proposición sobre $\mathbb{N}$, si se cumple:

- p(1)V $\wedge$ p(2)V
- $\forall h \in \mathbb{N}$, p(h)V $\wedge$ p(h+1)V $\Rightarrow$ p(h+2)V

Entonces puedo afirmar que p(n) es V $\forall n \in \mathbb{N}$

Principio de Inducción IV

Sea p(n) una proposición sobre $\mathbb{Z}_{\geq n_0}$, si se cumple:

- p(n_0)V $\wedge$ p($n_0 + 1$)V
- $\forall h \in \mathbb{Z}_{\geq n_0}$, p(h)V $\wedge$ p(h+1)V $\Rightarrow$ p(h+2)V

Entonces puedo afirmar que p(n) es V $\forall n \geq n_0$

Principio de Inducción V

Este es el principio de induccion completa o también llamada global. Sea p(n) una proposición sobre $\mathbb{N}$, si se cumple:

- p(1) V
- $\forall h \in \mathbb{N}$: p(k)V $\Rightarrow$ p(h+1)V para $1 \leq k \leq h$

Entonces puedo afirmar que p(n) es V $\forall n \in \mathbb{N}$

Principio de Inducción VI

Sea $n_0 \in \mathbb{Z}$ y sea p(n) una proposición en $\mathbb{Z}_{\geq n_0}$, si se cumple:

- p(n_0) V
- $\forall h \geq n_0$: p(k)V $\Rightarrow$ p(h+1)V para $n_0 \leq k \leq h$

Entonces puedo afirmar que p(n) es V, $\forall n \geq n_0$

2.1.3. Sucesión de Fibonacci

Tengo que $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n \ \forall n \geq 0$. Ahi la sucesión está definida por recurrencia, luego de una breve demostración podemos llegar a que el término general de la sucesión de Fibonacci es

$$F_n = \frac{1}{\sqrt{5}}(\varphi^n - \hat{\varphi}^n)\forall n \in \mathbb{N}_0 \tag{2.1}$$

2.1.4. Sucesiones de Lucas

Sea $(a_n)_{n\in\mathbb{N}_0}$ una sucesión por recurrencia que satisface

$$a_0 = \alpha, a_1 = \beta \text{ y } a_{n+2} = \gamma a_{n+1} + \delta a_n, \alpha, \beta, \gamma, \delta \text{ dados }, \forall n \in \mathbb{N}_0 \tag{2.2}$$

Entonces se puede decir que se trata de una sucesión de Lucas.

Capítulo 3

Combinatoria de conjuntos, relaciones y funciones

3.1. Combinatoria de conjuntos

Sea A un conjunto. El cardinal de A (notado $\#A$) es la cantidad de elementos que tiene A. Algunos ejemplos son:

- $\#\emptyset = 0$
- $\#\mathbb{N} = \infty$
- $\#\mathbb{R} = \infty$
- $\#\{1, ..., n\} = n$

Sea A un conjunto finito, #A $\in \mathbb{N}_0$ Sean A,B conjuntos: $\#A : \#B \iff \exists f : A \Rightarrow B$ biyectiva

Algunas observaciones que se pueden hacer son:

- $A \subseteq B \Rightarrow \#A \leq \#B$ (si A, B finitos, $A \subseteq B$ y $\#A = \#B \Rightarrow A = B$)
- Unión

  Sean A, B tal que $A \cap B = \emptyset$, entonces $\#(A \cup B) = \#A + \#B$

  Sean A, B cualesquiera, entonces $\#(A \cup B) = \#A + \#B - \#(A \cap B)$

  $\#A^c = \#U - \#A, \#(A \setminus B) = \#A - \#(A \cap B)$

3.1.1. Cardinal de un producto cartesiano

Sean A, B finitos, $\#(A \times B) = \#A \cdot \#B$ pues $(A \times B) = \{(x, y) : x \in A, y \in B\}$. En combinatoria el "$\vee$"se suma y el "$\wedge$"se multiplica. Otras observaciones que podemos hacer son:

- Sean $A_1, A_2, ..., A_n$ conjuntos tengo que $\#(A_1 \times A_2 \times ... \times A_n) = \prod_{k=1}^{n} \#A_k$

- $\#(A^n) = (\#A)^n$
- $\#(p(a)) = 2^{\#A}$

3.2. Combinatoria de relaciones de A en B

Sean A, B conjuntos y $\#A_m = m$ y $\#B_n = n$ tengo que la cantidad de relaciones será:

$$\#\left\{\text{Relaciones de } A_m \text{ en } B_n\right\} = \#(p(A_m \times B_n)) = 2^{A-m \times B_n} = 2^{m \cdot n} \tag{3.1}$$

3.3. Combinatoria de funciones

Usando los mismos conjuntos A y B de la sección anterior tengo que $\#\left\{f : A_m \to B_n\right\} = n^m = \#(B_n)^{\#(A_m)}$. Es decir que la cantidad de funciones de un conjunto A con m elementos a un conjunto B con n elementos es el cardinal del codominio elevado al cardinal del dominio.

Algunas observaciones antes de avanzar a la cantidad de funciones inyectivas y biyectivas:

- Sea $f : A_m \to B_n$ una funcion inyectiva, tengo que $Im(f) \subseteq B_n \Rightarrow \#(Im(f)) \leq n \Rightarrow m \leq n$
- Sea $f : A_m \to B_n$ sobreyectiva $\iff n \leq m$
- Sea $f : A_m \to B_n$ biyectiva $\iff m = n$

Ya con estas observaciones en cuenta tengo que la cantidad de funciones biyectivas es:

$$\#\left\{f : A_n \to B_n \text{ biyectivas}\right\} = n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 1 = n! \tag{3.2}$$

Y también tengo que la cantidad de funciones inyectivas es:

$$\#\left\{f : A_m \to B_n \text{ inyectivas}\right\}, \text{sea } m \leq n = \frac{n!}{(n-m)!} = \binom{n}{m} \cdot m! \tag{3.3}$$

3.3.1. Numero combinatorio

Sea A_n un conjunto con n elementos y sea $0 \leq k \leq n$:

$$\binom{n}{k} := \text{cantidad de subconjuntos que tiene } A_n \text{ con exactamente k elementos} \tag{3.4}$$

Propiedades

Sea $n \in \mathbb{N}$ y sea $0 \leq k \leq n$:

- $\binom{n}{0} = 1 = \binom{n}{n}$
- $\binom{n}{1} = n$
- $\binom{n}{k} = \binom{n}{n-k}$

- $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ pues $2^n = \#(p(A_n))$
- $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

3.4. Binomio de Newton

La definición del binomio de Newton es la siguiente:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k} \tag{3.5}$$

Tiene los mismos coeficientes que el triangulo de Pascal.

Capítulo 4

Numeros Enteros

4.1. Propiedades del conjunto $\mathbb{Z}$

Sean $a, b \in \mathbb{Z}$ tengo que:

- $a + b \in \mathbb{Z}$
- $a \cdot b \in \mathbb{Z}$
- $0 \in \mathbb{Z}$, 0 es el elemento neutro
- $a - b \in \mathbb{Z}$
- Existencia de opuesto: $\forall a \in \mathbb{Z}, \exists -a \in \mathbb{Z} : a + (-a) = 0$

4.2. Divisibilidad

Sean $a, d \in \mathbb{Z}, d \neq 0$, d siendo el divisor. Se dice que d divide a a $\iff$ $\exists k \in \mathbb{Z}$ tal que $a = k \cdot d$. Es decir que

$$d|a \iff \exists k \in \mathbb{Z} : a = k \cdot d \tag{4.1}$$

Por tanto el conjunto de divisores de a se definirá como $Div(a) = \{d \in \mathbb{Z}, d \neq 0 \text{ tal que } d|a\}$. Es una relación de orden ya que es reflexiva, antisimétrica y transitiva.

4.2.1. Propiedades

- $d|a \iff |d|\,|\,|a|$
- $d|a \Rightarrow |d| \leq |a|$
- $d|a \Rightarrow d|c \cdot a, \forall c \in \mathbb{Z}$
- En general: $d|c \cdot a \not\Rightarrow d|a \vee d|c$
- $d|a \iff c \cdot d|c \cdot a$

- $d|a \wedge a|b \Rightarrow d|(a+b)$
- En general: $d|(a+b) \nRightarrow d|a \vee d|b$
- $d|(a+b) \wedge d|a \Rightarrow d|b$
- Si $(d|a_1 \wedge d|a_2 \wedge ... \wedge d|a_n) \Rightarrow d|a_1 + a_2 + ... + a_n$ y también $d|c_1 a_1 + ... + c_n a_n, \forall c_1, ..., c_n \in \mathbb{Z}$
- $(d|a \wedge d|b) \Rightarrow d^2|a \cdot b$
- En general: $d^2|a \cdot b \nRightarrow (d|a \wedge d|b)$
- $d|a \Rightarrow d^2|a^2$
- $(d|a_1 \wedge d|a_2 \wedge ... \wedge d|a_n) \Rightarrow d^n|a_1 \cdot a_2 \cdot ... \cdot a_n$
- En particular: $d|a \Rightarrow d^n|a^n$
- $d|a \vee d|b \Rightarrow d|a \cdot b$
- $(d|a \cdot b \wedge d \perp a) \Rightarrow d|b$
- $d|a \cdot b \iff d|b$ si $d \perp a$
- $(c|a \wedge d|a) \iff c \cdot d|a$ si $c \perp d$
- $Div(0) = \mathbb{Z} - \{0\}$
- $Inv(\mathbb{Z}) = \{-1, 1\}$

4.3. Definiciones de numeros primos y compuestos

Sea $a \in \mathbb{Z}$, se dice que a es primo $\iff a \neq 0, \pm 1$ y a tiene únicamente dos divisores positivos $\iff Div_+(a) = \{1, |a|\} \iff (d|a \Rightarrow d = \pm 1, \pm a)$

Se dice que a es compuesto $\iff a \neq 0, \pm 1$ y a no es primo $\iff Div_+(a) \subsetneq \{1, |a|\} \iff \exists d \in \mathbb{Z}$ con $1 < d < |a| : d|a$

4.4. Congruencia

Sea $d \in \mathbb{Z}, d \neq 0$ tengo que a es congruente con modulo b mientras (a-b) sea divisible por d. Es decir,

$$a \equiv b(d) \iff d|(a-b) \tag{4.2}$$

4.4.1. Propiedades

- $a \equiv b(d) \Rightarrow c \cdot a \equiv c \cdot b(d)$
- En general: $c \cdot a \equiv c \cdot b(d) \not\Rightarrow a \equiv b(d)$
- $a \equiv b(d) \iff c \cdot a \equiv c \cdot b(c \cdot d)$
- $(a_1 \equiv b_1(d) \wedge a_2 \equiv b_2(d)) \Rightarrow a_1 + a_2 = b_1 + b_2(d)$ y también vale $c_1a_1 + c_2a_2 \equiv c_1b_1 + c_2b_2(d), \forall c_1, c_2 \in \mathbb{Z}$
- $(a_1 \equiv b_1(d) \wedge ... \wedge a_n \equiv b_n(d)) \Rightarrow a_1 + ... + a_n \equiv b_1 + ... + b_n(d)$ y también vale que $c_1a_1 + ... + c_na_n \equiv c_1b_1 + ... + c_nb_n(d), \forall c_1, ..., c_n \in \mathbb{Z}$
- Producto

  $(a_1 \equiv b_1(d)) \wedge (a_2 \equiv b_2(d)) \Rightarrow a_1a_2 \equiv b_1b_2(d)$

  $a \equiv b(d) \Rightarrow a^2 \equiv b^2(d)$ y también vale que $a \equiv b(d) \Rightarrow a^n \equiv b^n(d), \forall n \in \mathbb{N}$

4.5. Algoritmo de división

Sean $a, d, q \in \mathbb{Z}$ con $d \neq 0$. Entonces $\exists q, r \in \mathbb{Z}$ con $a = qd + r$ con $0 \leq r < |d|$.
Además q y r son únicos con estas dos condiciones:

- q: cociente de dividir a a por d
- $r = r_d(a)$ es el resto

4.5.1. Propiedades

- Si $a = kd + r$ con $0 \leq r < |d|$ y $k \in \mathbb{Z}$, entonces $r = r_d(a)$
- $r_d(a) = 0 \iff a = qd \iff d|a$

Congruencia y restos

- $a \equiv r_d(a)(d)$
- $a \equiv r(d)$ con $0 \leq r < |d| \Rightarrow r_d(a) = r$ pues $a - r = k \cdot d$ con $k \in \mathbb{Z}$
- $r_1 \equiv r_2(d)$ con $0 \leq r_1, r_2 < |d| \Rightarrow r_1 = r_2$
- $a \equiv b(d) \iff r_d(a) = r_d(b)$

4.6. Sistemas de numeración

4.6.1. Desarrollo en base d

Sea $d \in \mathbb{N}, d \geq 2$, $\forall a \in \mathbb{N}$ existe un único $n \in \mathbb{N}$ y $r_0, ..., r_n$ con $0 \leq r_k < d$ y $r_n \neq 0$ tal que

$$a = r_n d^n + r_{n-1} d^{n-1} + ... + r_1 d + r_0 = \sum_{k=0}^{n} r_k d^k \tag{4.3}$$

4.7. Máximo Común Divisor (MCD)

Definición: Sean $a, b \in \mathbb{Z}$ no ambos nulos , el máximo común divisor entre a y b es el divisor común más grande que tienen a y b, se escribe (a:b)

Se tiene:

- (a:b) $\in \mathbb{N}$
- $(a : b)|a$ y $(a : b)|b$
- $\forall d \in \mathbb{Z} : d|a \wedge d|b \Rightarrow d \leq (a : b)$
- (a:b) siempre existe y es único

4.7.1. Propiedades

- $a \neq 0, (a : 0) = |a|$
- $(a : \pm 1) = 1$
- (a:b) $= (|a| : |b|)$
- (a:b) = (b:a)
- $(a : b)|a$ y $(a : b)|b$
- $(a^n : b^n) = (a : b)^n$

4.8. Algoritmo de Euclides (para mcd)

Sean $a, b \in \mathbb{Z}, b \neq 0$

- $\forall k \in \mathbb{Z}, (a : b) = (b : a - kb)$
- $a \equiv c(b) \Rightarrow (a : b) = (c : b)$ pues $b|a - c \Rightarrow a - c = kb \Rightarrow c = a - kb$
- En particular $a \equiv r_b(a)(b) \Rightarrow (a : b) = (b : r_b(a))$

También tengo que $\exists s, t \in \mathbb{Z}$ tal que $(a : b) = s \cdot a + t \cdot b$ y que si $d|a \wedge d|b \Rightarrow d|(a : b)$ pues si los divide individualmente, multiplicados por cualquier c entero también los dividirá, si divide a la suma también divide el mcd.

4.9. Numeros coprimos

Sea $a, b \in \mathbb{Z}$ no ambos nulos se dice que a y b son coprimos cuando (a:b) = 1. Entonces tengo que:

$$a \perp b \iff (a : b) = 1 \iff \exists s, t \in \mathbb{Z} : 1 = s \cdot a + t \cdot b \tag{4.4}$$

4.9.1. Coprimizar

Sean $a, b \in \mathbb{Z}$ tengo que: $\frac{a}{(a:b)} \in \mathbb{Z}$, $\frac{b}{(a:b)} \in \mathbb{Z}$ son coprimos pues $(a : b) = s \cdot a + t \cdot b \Rightarrow 1 = \frac{s \cdot a}{(a:b)} + \frac{t \cdot b}{(a:b)}$. Entonces tomo $a = (a : b) \cdot a'$ y $b = (a : b) \cdot b'$ con $a' \perp b'$

Observaciones

- $(a : b) = 1$ y $(a : c) = 1 \Rightarrow (a : bc) = 1$
- $(a : b) = 1 \Rightarrow (a : b^2) = 1 \Rightarrow (a : b^n) = 1 \Rightarrow (a^m : b^n) = 1$
- $(a : b) = d \Rightarrow (a^n : b^n) = d^n$

4.10. Numeros primos

Sea $a \in \mathbb{Z}, a \neq 0, \pm 1$ entonces $\exists p \in \mathbb{N}$ primo tal que $p|a$, defino la propiedad fundamental de los primos en la siguiente sección.

Propiedad fundamental de los números primos

Sea p primo, y $a \in \mathbb{Z}$ entonces $p \nmid a \iff p \perp a$ entonces como consecuencia puedo decir que $p|ab \iff p|a \vee p|b$ con p primo. Además puedo afirmar que si $p|a^n \Rightarrow p|a$.

4.10.1. Teorema Fundamental de la Aritmética (TFA)

Sea $a \in \mathbb{Z}$ con $a \neq 0, \pm 1$ entonces a se escribe en forma única como $\pm$ producto de primos positivos. O sea que $\exists p_1, ..., p_r$ primos positivos distintos y $m_1, ..., m_r \in \mathbb{N}$ tal que:

$$a = \pm p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_r^{m_r} \tag{4.5}$$

y esa escritura es única.

4.10.2. Divisores de un número

Sea $a = \pm p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_r^{m_r}$ con $m_1, m_2, ..., m_r > 0$. Entonces $d|a \iff \begin{cases} \exists j_1 \text{ con } 0 \leq j_1 \leq m_1 \\ \exists j_2 \text{ con } 0 \leq j_2 \leq m_2 \\ ... \\ \exists j_r \text{ con } 0 \leq j_r \leq m_r \end{cases}$

tal que $d = \pm p_1^{j_1} \cdot p_2^{j_2} \cdot ... \cdot p_r^{j_r}$.

Respecto al número de divisores positivos de un número a de la misma forma que el anterior mencionado tengo que $\#Div_{+}(a) = (m_1 + 1)(m_2 + 1)...(m_r + 1)$

4.10.3. Factorización y mcd

Sea $a, b \in \mathbb{Z}$ no nulos, $a = \pm p_1^{m_1} \cdot ... \cdot p_r^{m_r}$ con $m_1, ..., m_r \geq 0$ y $b = \pm p_1^{n_1} \cdot ... \cdot p_r^{n_r}$ con $n_1, ..., n_r \geq 0$ tengo que $(a : b) = p_1^{\text{mín}(m_1,n_1)} \cdot \ldots \cdot p_r^{\text{mín}(m_r,n_r)}$

Sean $p, q \in \mathbb{Z}$ primos $\neq / p^m \perp q^n$ y por lo tanto $p^m|a$ y $q^n|a \Rightarrow p^n q^m|a$. Como no se superponen pero están en a, está en su producto.

4.11. Mínimo común múltiplo (MCM)

Sean $a, b \in \mathbb{Z}$ no nulos, el MCM [a:b] entre a y b es el menor múltiplo común en $\mathbb{N}$.

4.11.1. Propiedades

- $[a : b] \in \mathbb{N}$
- $a|[a : b]$ y $b|[a : b]$
- Sea $n \in \mathbb{Z}/a|m$ y $b|n \Rightarrow [a : b]|m$
- $a \perp b \Rightarrow [a : b] = ab$

4.11.2. Cálculo

Sea $a, b \in \mathbb{Z}$, escritos en su factorización única en primos y recordando que el MCD consiste en ver el minimo de los exponentes entre las dos potencias del mismo factor de forma repetida con cada uno (ver 4.10.3), entonces $[a : b] = p_1^{\text{máx}(m_1,n_1)} \cdot p_2^{\text{máx}(m_2,n_2)} \cdot ... \cdot p_r^{\text{máx}(m_r,n_r)}$.

También voy a tener que el módulo de ab es el producto del MCD y MCM entre éstos, es decir, $(a : b) \cdot [a : b] = |a \cdot b| \Rightarrow [a : b] = \frac{|ab|}{(a:b)}$

4.12. Bibliografía

Krick, T. (2017). Fascículo 9: Álgebra I. Departamento de Matemática de la Facultad de Ciencias Exactas y Naturales (Universidad de Buenos Aires).