

Algebra

Gianfranco Zamboni

20 de enero de 2019

Índice

1. Conjuntos, relaciones y funciones	2
1.1. Conjuntos	2
1.2. Relaciones	5
1.2.1. Relaciones de equivalencia y de orden	5
1.2.2. Partición de un conjunto	5
1.3. Funciones	6
1.3.1. Composición de funciones y función inversa	6
2. Números naturales e inducción	7
2.1. Operaciones y propiedades básicas	7
2.2. Sumatorias y sucesiones conocidas	7
2.3. Conjunto inductivo y principio de inducción	7
2.3.1. Principio inductivo:	8
2.3.2. Principio de inducción corrido	8
2.3.3. Principio de inducción global	8
2.4. Propiedades y otras definiciones	8
2.5. Los números naturales	9
2.5.1. Axiomas de Peano	9
2.6. El número combinatorio	9
2.6.1. Propiedades	9
2.6.2. Ejemplo de ejercicio	9
3. Números enteros	10
3.1. Divisibilidad	10
3.1.1. Números primos (Primera parte)	10
3.2. Algoritmo de la división	11
3.2.1. Codificación en base d	11
3.3. Relación de congruencia	11
3.3.1. Criterios de divisibilidad	12
3.4. Máximo común divisor (MCD)	12
3.5. Algoritmo de euclides	13

3.5.1. Números coprimos	13
3.6. Factorización	14
3.7. Mínimo Común Múltiplo (MCM)	14
3.8. Ecuaciones lineales diofánticas	15
3.9. Ecuaciones lineales de congruencia	15
3.10. Sistemas equivalentes	16
3.11. Teorema chino del resto	16
3.12. Pequeño teorema de fermat	17
3.12.1. Teorema de Euler	17
3.13. Anillos y cuerpos	17
3.13.1. Elementos inversibles	17
4. Polinomios	19
4.1. Números complejos	19
4.2. Raíces n-ésimas	20
4.2.1. Raíces de la unidad	20
4.2.2. Raíces primitivas	21
4.3. Polinomios	21
4.3.1. Divisibilidad	22
4.3.2. Reducibilidad	22
4.3.3. Algoritmo de la división	22
4.3.4. Máximo Común Divisor (MCD)	23
4.3.5. Polinomios coprimos	23
4.3.6. Reducibilidad de un polinomio	23
4.3.7. Raíces de un polinomio	24
4.3.8. Polinomios cuadráticos	24
4.3.9. Multiplicad de raíces	24
4.3.10. Derivadas	24
4.3.11. Polinomios en \mathbb{C}	25
4.4. Polinomios en \mathbb{R}	26
4.4.1. Lema de Gauss (Algoritmo)	26

1. Conjuntos, relaciones y funciones

1.1. Conjuntos

Conjunto: Es una colección de objetos tales que, dado un objeto cualquiera v , se puede determinar si v pertenece o no a la misma.

Conjunto vacío: Es el conjunto que no tiene elementos y se lo denota con la letra ϕ .

Cardinal: de un conjunto A es el número de elementos distintos que posee el mismo y lo notamos $|A|$.

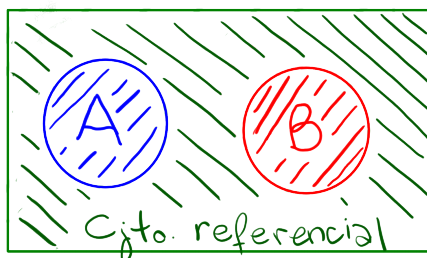
Subconjunto: Se dice que un conjunto B está contenido en un conjunto A si todo elemento de B es un elemento de A .

$$B \subseteq A \iff [(\forall x : \alpha) x \in B \rightarrow x \in A]$$

Igualdad: Dos conjuntos A y B son iguales si tienen exactamente los mismos elementos.

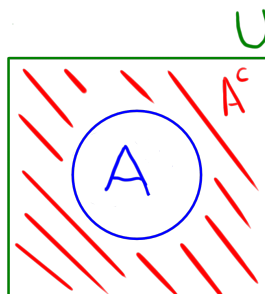
$$A = B \iff (A \subseteq B \wedge B \subseteq A)$$

Conjunto referencial: Conjunto que incluye a todos los conjuntos que se están considerando. Sean A y B dos conjuntos cualesquiera:



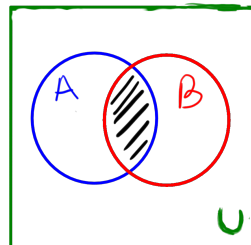
Complemento: Sea $A \subset U$ entonces, el complemento A^c de A es el conjunto que incluye todos los elementos de U que no pertenecen a A .

$$A^c = \{x \in U : x \notin A\}$$



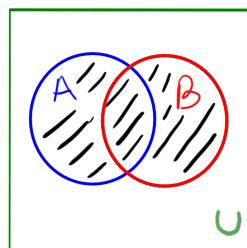
Intersección: Sean $A \subset U$ y $B \subset U$, la intersección de A y B es el conjunto de elementos que pertenecen tanto a A como a B .

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}$$



Union: Sean $A \subset U$ y $B \subset U$, la **union** de A y B es el conjunto de elementos que pertenecen a A o a B .

$$A \cup B = \{x \in U : x \in A \vee x \in B\}$$



Propiedades

- ϕ está contenido en todos los conjuntos.
- Sean A y B dos conjuntos tal que $B \subseteq A \rightarrow |B| \leq |A|$
- Si $A \cap B = \phi \rightarrow |A \cup B| = |A| + |B|$
- $|A \cup B| = |A| + |B| - |A \cap B|$
- Si U es finito, $|A^c| = |U| - |A|$
- Si $A \subseteq B \wedge B \subseteq C$ entonces $A \subseteq C$
- Si $A \subseteq B \wedge A \subseteq C$ entonces $A \subseteq (B \cap C)$
- $A \subseteq (A \cup B) \wedge B \subseteq (B \cup A) \rightarrow A = B$
- $A \cap (B \cap C) = (A \cap B) \cap C$
- $A \cap B = B \cap A$
- $A \cap A^c = \phi$
- $A \cap \phi = \phi$
- $A \cup (B \cup C) = (A \cup B) \cup C$
- $A \cup B = B \cup A$
- $A \cup A^c = U$
- $A \cup \phi = A$

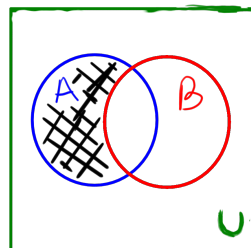
Leyes de Morgan: Sean A y B contenidos en U , entonces valen:

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

Diferencia: Sean $A \subset U$ y $B \subset U$, la diferencia entre A y B se define como:

$$A - B = A \cap B^c$$

$$= \{x \in U : x \in A \wedge x \notin B\}$$

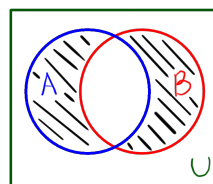


Propiedades:

- $A - B = A - (A \cap B)$
- $|A - B| = |A| - |A \cap B|$

Diferencia simétrica: Sean $A \subset U$ y $B \subset U$, la diferencia simétrica entre A y B es el conjunto de elementos que pertenecen a A o a B pero no los dos a la vez.

$$A \Delta B = (A - B) \cup (B - A)$$



Propiedades: Sean A, B y C subconjuntos de U :

- $|A \Delta B| = |A| + |B| - 2 \times |A \cap B|$
- $A \Delta \phi = A$
- $A \Delta B = (A \cup B) - (A \cap B)$
- $(A \Delta B) - C = (A - C) \Delta (B - C)$
- $A \Delta B = B \Delta A$
- $(A \Delta B) \subseteq (A \Delta C)$
- $A \Delta A = \phi$

Conjunto de partes: de A se nota $\mathcal{P}(A)$ y es el conjunto formado por todos los subconjuntos de A .

$$\mathcal{P}(A) = \{B : B \subseteq A\} \wedge (B \in \mathcal{P}(A) \iff B \subseteq A)$$

Propiedades :

- $\mathcal{P}(A) \subseteq \mathcal{P}(B) \iff A \subseteq B$
- $|\mathcal{P}(A)| = 2^{|A|}$

Producto cartesiano Sean A y B conjuntos, el producto cartesiano de A con B es el conjunto de pares ordenados $A \times B = \{(x, y) : x \in A \wedge y \in B\}$

Propiedades:

- $|A \times B| = |A| |B|$
- $|A_1 \times \cdots \times A_n| = |A_1| \times \cdots \times |A_n|$
- $A \neq B$ entonces $A \times B \neq B \times A$
- Si $A \subseteq U \wedge B \subseteq V$ entonces $A \times B \subseteq U \times V$

1.2. Relaciones

Sean A y B dos conjuntos. Un subconjunto \mathcal{R} del producto cartesiano $A \times B$ se llama relación de A en B .

Dados $x \in A$ e $y \in B$ y una relación \mathcal{R} de A en B , se dice que x está relacionado con y si $(x, y) \in \mathcal{R}$. Y, en ese caso, se nota $x\mathcal{R}y$.

Se dice que \mathcal{R} es una relación en A cuando $\mathcal{R} \subseteq A \times A$. Una relación \mathcal{R} en A puede ser:

- **Reflexiva:** si $(\forall x \in A) (x, x) \in \mathcal{R}$
- **Simétrica:** si $(\forall x, y \in A) (x\mathcal{R}y \rightarrow y\mathcal{R}x)$
- **Asimétrica:** si $(\forall x, y \in A) (x\mathcal{R}y \wedge y\mathcal{R}x \rightarrow x = y)$.
- **Transitiva:** Si $(\forall x, y, z \in A) (x\mathcal{R}y \wedge y\mathcal{R}z \rightarrow x\mathcal{R}z)$.

1.2.1. Relaciones de equivalencia y de orden

\mathcal{R} es una **relación de equivalencia** si es reflexiva, simétrica y transitiva.

\mathcal{R} es una **relación de orden** cuando es una relación reflexiva, asimétrica y transitiva.

Dada \sim una relación de equivalencia en A , la **clase de equivalencia** de un elemento $x \in A$, es el conjunto $C_x = \bar{x} = \{y \in A : y \sim x\}$

- Si $y \in C_x$ entonces $x \in C_y$
- $x \in C_x$
- $x \sim y \iff C_x = C_y$
- $x \not\sim y \iff C_x \cap C_y = \emptyset$

1.2.2. Partición de un conjunto

Sea A un conjunto y \mathcal{P} un conjunto formado por subconjuntos de A . Decimos que \mathcal{P} es una **partición** si cumple:

- $\mathcal{P} \neq \emptyset$
- Si $P, Q \in \mathcal{P} \wedge P \neq Q$ entonces $P \cap Q = \emptyset$
- Para todo elemento a de A , $(\exists P \in \mathcal{P}) a \in P$

Para todo conjunto A , hay una manera natural de asociar una relación de equivalencia en A a una partición de A .

Sea \sim una relación de equivalencia en un conjunto A :

- Sean $a, b \in A$, entonces $a \sim b \iff$ existe $c \in A$ tal que $a, b \in C_c$.
- $\mathcal{P} = \{C_a : a \in A\}$ es una partición de A .

Si \mathcal{P} es una partición de A , entonces la relación \sim en A definida por " $a \sim b \iff \exists P \in \mathcal{P}$ tal que $a, b \in P$ " es de equivalencia.

Si A y B son conjuntos finitos con m y n elementos, respectivamente, entonces, la cantidad de relaciones que hay de A en B es igual a 2^{mn}

1.3. Funciones

Dada f una relación de A en B , se dice que f es una **función** cuando todo elemento $x \in A$ está relacionado con algún elemento $y \in B$ y además es el único elemento con el que se relaciona. Si pasa esto, se dice que y es la imagen de x por f ($y = f(x)$).

La $\mathcal{R} = \{(x, x) : x \in A\}$ para cualquier conjunto $A \neq \emptyset$, es la **función identidad** de A y se nota id_A . ($id_A(x) = x \forall x \in A$)

Si A es un conjunto, una sucesión de elementos de A puede ser tomada como una función $f : \mathbb{N} \rightarrow A$.

Sean $f, g : A \rightarrow B$, f y g son **iguales** ($f = g$) cuando $f(x) = g(x) \forall x \in A$

Sea $f : A \rightarrow B$:

- A se llama **dominio** de f
- B se llama **codominio** de f
- La **imagen** $\text{Im}(f)$ es el subconjunto de elementos de B que están relacionados con algún elemento de A

$$\text{Im}(f) = \{y \in B : \exists x \in A / f(x) = y\}$$

- f es **inyectiva** si $\forall y \in B$ existe a lo sumo un elemento $x \in A / f(x) = y$
- f es **sobreyectiva** si $\forall y \in B$ existe al menos un elemento de $x \in A / f(x) = y$.
- f es **biyectiva** si es inyectiva y sobreyectiva.

Sean A y B dos conjuntos de m y n elementos respectivamente, entonces hay n^m funciones de A en B distintas y dada una función $f : A \rightarrow B$ vale que:

- Si f es inyectiva $\rightarrow |A| \leq |B|$
- Si f es sobreyectiva $\rightarrow |A| \geq |B|$
- Si f es biyectiva $\rightarrow |A| = |B|$

Además hay $n!$ funciones biyectivas de A en B y $\frac{n!}{(m-n)!}$ funciones inyectivas de A en B .

1.3.1. Composición de funciones y función inversa

Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ funciones, entonces la **composición** $g \circ f$ de f con g está definida por:

$$g \circ f : A \rightarrow C, (g \circ f)(x) = g(f(x))$$

Si f es una función biyectiva, entonces para todo $y \in B$ existe exactamente un elemento $x \in A / f(x) = y$. Sea $\mathcal{R} = \{(y, x) : f(x) = y\}$ una relación de A en B , se puede ver que \mathcal{R} satisface las propiedades para ser función. Notamos \mathcal{R} con f^{-1} y se llama **función inversa**.

Propiedades: Sea $f : A \rightarrow B$ una función:

- Si f es biyectiva, entonces $f^{-1} \circ f = id_A$ es igual a la función identidad.
- Si existe $g : B \rightarrow A$ tal que $f \circ g = id_B$ y $g \circ f = id_A$, entonces f es biyectiva y $g = f^{-1}$.
- f es inversible si y solo si f es biyectiva.

2. Números naturales e inducción

2.1. Operaciones y propiedades básicas

Sean m , n y k tres números naturales, entonces valen:

- $m + n \in \mathbb{N}$ y $m - n \in \mathbb{N}$
- **Conmutatividad:** $m + n = n + m$ y $m \times n = n \times m$
- **Asociatividad:** $m + (n + k) = (m + n) + k$ y $m \times (n \times k) = (m \times n) \times k$
- $\sum_{i=1}^n a_i + \sum_{i=1}^n b_i = \sum_{i=1}^n (a_i + b_i)$
- $\prod_{i=1}^n a_i * \prod_{i=1}^n b_i = \prod_{i=1}^n (a_i * b_i)$

2.2. Sumatorias y sucesiones conocidas

Suma de Gauss

$$\sum_{i=0}^n i = \frac{n(n+1)}{2}$$

Serie geométrica

$$\sum_{i=0}^n q^i = \frac{q^{n+1} - 1}{q - 1}$$

Sucesión de Fibonacci

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-2} + F_{n-1} \end{aligned}$$

Sucesión de Lucas

$$\begin{aligned} a_1 &= 5 \\ a_2 &= 13 \\ a_n &= 5a_{n-1} - 6a_{n-2} \end{aligned}$$

2.3. Conjunto inductivo y principio de inducción

El **principio de inducción** funciona en dos pasos. El primero, conocido como **caso base**, es probar que la afirmación en cuestión es verdadera para el primer número natural. El segundo paso, conocido como **paso inductivo**, es probar que la afirmación para un número natural cualquiera implica la afirmación para el número natural siguiente.

Sea $H \subseteq \mathbb{N}$ un conjunto, se dice que H es un conjunto inductivo si se cumplen las siguientes condiciones:

- $1 \in H$
- $(\forall x \in \mathbb{N}) (x \in H \rightarrow x + 1 \in H)$

Si $H \subseteq \mathbb{N}$ es un conjunto inductivo, entonces $H = \mathbb{N}$.

Todos los conjuntos inductivos cumplen el **principio de buena ordenación**, o sea que contienen un elemento que es menor o igual que todos los demás elementos del conjunto.

2.3.1. Principio inductivo:

Sea $n \in \mathbb{N}$ y $p(n)$ una afirmación sobre los números naturales, si p satisface:

- **Caso base:** $p(1)$ es verdadera y
- **Paso inductivo:** $(\forall n \in \mathbb{N}) (p(n) \text{ es verdadera} \rightarrow p(n+1) \text{ es verdadera})$

entonces p es verdadera para todo $n \in \mathbb{N}$.

La hipótesis " $p(n)$ es verdadera" se denomina **hipótesis inductiva**.

2.3.2. Principio de inducción corrido

Sea $n_0 \in \mathbb{Z}$ y sea $p(n)$ tal que $n \geq n_0$ una afirmación sobre $\mathbb{Z}_{\geq n_0}$. Si p satisface:

- **Caso base:** $p(n_0)$ es verdadera y
- **Paso inductivo:** $(\forall n \in \mathbb{N}, n \geq n_0) (p(n) \text{ es verdadera} \rightarrow p(n+1) \text{ es verdadera})$

entonces p es verdadera para todo $n \in \mathbb{N}$ que sea mayor o igual a n_0 .

2.3.3. Principio de inducción global

Sea $n_0 \in \mathbb{Z}$ y sea $p(n)$ una afirmación sobre \mathbb{N} . Si p satisface:

- **Caso base:** $p(n_0)$ es verdadera y
- **Paso inductivo:** $((\forall n \in \mathbb{N}, n \leq n_0) p(n) \text{ es verdadera}) \rightarrow p(n+1) \text{ es verdadera})$

entonces p es verdadera para todo $n \in \mathbb{N}$.

2.4. Propiedades y otras definiciones

- Todo subconjunto $A \subseteq \mathbb{N}$ tal que $A \neq \emptyset$ tiene un primer elemento.
- Las sucesiones que dependen de valores ya conocidos se llaman **sucesiones recursivas** o sucesiones por recurrencia.
- Una **fórmula cerrada** es una formula en la que el elemento a_n de una sucesión no depende de los anteriores, sino solo de n .
- **Función cerrada:** Dado un conjunto A cualquiera, una r -upla (a_1, \dots, a_r) de elementos de A y una función $G : \mathbb{N} \times A \times \dots \times A \rightarrow A$ es una función $f : \mathbb{N} \rightarrow A$ tal que:
 - $f(i) = a_i$ para $1 \leq i \leq r$ y
 - $f(n) = G(n, f(n-1), f(n-2), \dots, f(n-r))$

- **Identidad de Casini:** $F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$

- **Término general de la sucesión de Fibonacci:**

$$\Phi = \frac{1 + \sqrt{5}}{2} \text{ y } F_n = \frac{1}{\sqrt{5}} \left(\Phi^n - \bar{\Phi}^n \right)$$

- **Término general de la sucesión de Lucas:**

$$a_n = 2^n + 3^n$$

2.5. Los números naturales

2.5.1. Axiomas de Peano

El conjunto de números naturales es un conjunto que cumple los siguientes axiomas:

1. 1 es un número natural
2. Existe una función *sucesor* S definida sobre los números naturales que satisface:
 - $\forall n \in \mathbb{N}, S(n)$ es un número natural.
 - $\forall n \in \mathbb{N}, S(n) = 1$ es falso. Es decir, 1 no es sucesor de ningún $n \in \mathbb{N}$
 - $\forall n, m \in \mathbb{N}$, si $S(n) = S(m)$, entonces $n = m$. (S es inyectiva)
3. Si K es un conjunto cualquiera que satisface $1 \in K$ y $\forall n \in \mathbb{N}, n \in K \rightarrow S(n) \in K$, entonces $K = \mathbb{N}$

2.6. El número combinatorio

El número combinatorio es la cantidad de subconjuntos distintos de k elementos que contiene un conjunto A de n elementos y se define de la siguiente manera:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

2.6.1. Propiedades

- $\binom{0}{0} = 1$
- $\binom{n}{0} = \binom{n}{n} = 1$
- $\binom{n}{1} = \binom{n}{n-1} = n$
- $\binom{n}{k} = \binom{n}{n-k}$
- $\sum_{i=0}^n \binom{n}{i} = 2^n$
- $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$
- **Binomio de Newton**
- $(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$
- $\binom{2n}{n} \leq (n+1)!$
- $\sum_{k=0}^{2n} \binom{2n}{k} = 4^n$

2.6.2. Ejemplo de ejercicio

Enunciado: Si tenemos n bolitas indistinguibles y las queremos repartir en k cajas, ¿Cuántas formas posibles hay de hacerlo?

Solución:

$$\binom{n+k-1}{n}$$

3. Números enteros

El grupo de números enteros (\mathbb{Z}) satisface las siguientes propiedades:

- **Conmutatividad:** $a + b = b + a$ y $a \cdot b = b \cdot a$
- **Asociatividad:** $(a + b) + c = a + (b + c)$ y $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **Tiene un elemento neutro:** Para la suma es el 0 ($a + 0 = a$) y para la multiplicación el 1 ($a \cdot 1 = a$)
- **Existe el opuesto:** respecto de la suma $a + (-a) = 0$
- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $a \cdot b = a \cdot c$ y $a \neq 0 \rightarrow b = c$
- $a \cdot b = 0 \rightarrow a = 0$ ó $b = 0$
- \mathbb{Z} es un conjunto inductivo bien ordenado.

3.1. Divisibilidad

Sean $a, d \in \mathbb{Z}$, $d \neq 0$. Se dice que d divide a a ($d|a$) si existe un elemento $k \in \mathbb{Z}$ tal que $a = kd$.

$$d|a \iff \exists k \in \mathbb{Z} / a = kd$$

El conjunto de **divisores** de un elemento $a \in \mathbb{Z}$ es $\text{Div}(a) = \{d \in \mathbb{N} : d|a\}$ y el conjunto de **divisores positivos** del mismo elementos es $\text{Div}_+(a) = \{d \in \mathbb{N} : d|a \wedge d > 0\}$

Propiedades

- $\forall d \in \mathbb{Z}, d|0$
- $d|a \iff -d|a \iff d|-a \iff -d|-a$
- Si $a \neq 0$ y $d|a \rightarrow |d| \leq |a|$
- $d|a$ y $a|d \iff a = \pm d$
- $(\forall a \in \mathbb{Z}) 1|a \wedge -1|a \wedge a|a \wedge -a|a$
- $0|a \iff a = 0$
- $a|b \wedge b|c \rightarrow a|c$
- $a|b \wedge a|c \rightarrow a|(a+b) \wedge a|(a-b)$
- $a|b \rightarrow a|bc$ ($\forall c \in \mathbb{Z}$)
- $a|(b \pm c) \wedge a|b \rightarrow a|c$
- $a|b \iff ac|bc$ ($\forall c \in \mathbb{Z}$)
- $d|a \iff d^n|a^n$ ($\forall n \in \mathbb{N}$)
- $n|m \rightarrow (a^n - 1)|(a^m - 1)$

3.1.1. Números primos (Primera parte)

Se dice que $a \in \mathbb{Z}$ es un **número primo** si $a \neq 0, \pm 1$ y tiene únicamente 4 divisores (o 2 divisores). En cambio, se dice que a es **compuesto** si $a \neq 0, \pm 1$ y tiene más de 4 divisores (o más de 2 divisores positivos).

Propiedades

- Si $d \in \mathbb{Z}$ y $d|ab \rightarrow d|a$ ó $d|b$
- Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$, entonces $\exists p$ primo tal que $p|a$
- Existen infinitos primos
- Si a no es primo, entonces existe $p < a$ tal que $p|a$
- Si a no es primo, entonces existe p tal que $1 \leq p \leq \sqrt{a}$ y $p|a$.

3.2. Algoritmo de la división

Dados $a, d \in \mathbb{Z}$ con $d \neq 0$, existen $k, r \in \mathbb{Z}$ que satisfacen $a = k \cdot d + r$ con $0 \leq r < |d|$. Además, k y r son únicos en tales condiciones. Llamamos **cociente** a k , **resto** a r , **dividendo** a a y **divisor** a d . A partir de ahora notaremos $r_d(a)$ a r .

Propiedades

- $r_d(a + b) = r_d(r_d(a) + r_d(b))$
- $r_d(a \cdot b) = r_d(r_d(a) \cdot r_d(b))$
- $r_d(a^n) = r_d(r_d(a)^n)$

3.2.1. Codificación en base d

Sea $d \in \mathbb{N}$ con $d \geq 2$. Todo número $a \in \mathbb{N}$ admite un desarrollo en base d de la forma:

$$a = r_n \cdot d^n + r_{n-1} \cdot d^{n-1} + \cdots + r_1 \cdot d^1 + r_0$$

con $0 < r_i < d$ para todo $0 \leq i \leq n$ y $r_n \neq 0$ si $a \neq 0$

Propiedades

- El número más grande de tamaño n en base d es el número $d^n - 1$.
- Se pueden escribir d^n números usando n símbolos en base d .
- El tamaño (cantidad de dígitos) en base d de un número $a \in \mathbb{N}$ es $\lceil \log_d(a) \rceil + 1$

3.3. Relación de congruencia

Sean $a, b \in \mathbb{Z}$, decimos que a es **congruente a b módulo d** si $d|(b - a)$. y notamos $a \equiv b \pmod{d}$ ó $a \equiv b \pmod{d}$.

$a \equiv b \pmod{d}$ es una relación de equivalencia que parte a los números enteros de la siguiente manera:

$$\bar{a} = \{b \in \mathbb{Z} : r_d(b) = r_d(a)\}$$

Es decir, que la clase equivalencia está formada por todos los elementos de los enteros cuyo resto sea el mismo que el resto de a .

Propiedades

- $r_d(a) = 0 \iff d|a \iff a \equiv 0 \pmod{d}$
- $(\forall a \in \mathbb{Z}) a \equiv r_d(a) \pmod{d}$
- $a \equiv r \pmod{d}$ con $0 < r < |d| \rightarrow r = r_d(a)$
- $r_1 \equiv r_2 \pmod{d}$ con $0 < r_1, r_2 < |d| \rightarrow r_1 = r_2$
- $a \equiv b \pmod{d} \iff r_d(a) = r_d(b)$
- $(\forall a \in \mathbb{Z}, d \in \mathbb{N}) a \equiv a \pmod{d}$
- $a \equiv b \pmod{d} \rightarrow b \equiv a \pmod{d}$
- $a \equiv b \pmod{d} \wedge c \equiv e \pmod{d} \rightarrow a + c \equiv e + b \pmod{d} \wedge a \cdot c \equiv b \cdot e \pmod{d}$
- Sea $c \in \mathbb{N}$, $a \equiv b \pmod{d} \iff ac \equiv bc \pmod{dc}$
- Dado $d \in \mathbb{Z}$, la relación $a \equiv b \pmod{d}$ define d clases de equivalencias distintas.
- $a \equiv b \pmod{d} \rightarrow b \equiv a \pmod{d}$
- $a \equiv b \pmod{d} \text{ y } b \equiv c \pmod{d} \rightarrow a \equiv c \pmod{d}$
- $a \equiv b \pmod{d} \rightarrow a + c \equiv b + c \pmod{d}$ para todo $c \in \mathbb{Z}$
- $a \equiv b \pmod{d} \iff ac \equiv bc \pmod{d}$ para todo $c \in \mathbb{Z}$
- $a \equiv b \pmod{d} \rightarrow a^n \equiv b^n \pmod{d}$ para todo $n \in \mathbb{N}$
- $a \equiv a + dq \pmod{d}$ para todo $q \in \mathbb{Z}$

3.3.1. Criterios de divisibilidad

Sea $a = r_1 r_2 r_3 \dots r_n$ un desarrollo decimal de a , entonces:

- $3|a \iff 3|(r_1 + r_2 + \dots + r_n)$
- $11|a \iff 11|((-1)^n r_n + (-1)^{n-1} r_{n-1} + \dots + r_0)$

3.4. Máximo común divisor (MCD)

Sean $a, b \in \mathbb{Z}$ no nulos, definimos el conjunto de **divisores comunes** como el conjunto elementos que dividen a a y a b al mismo tiempo:

$$DivCom(\{a, b\}) = \{d \in \mathbb{Z} : d|a \wedge d|b\}$$

Y el **máximo común divisor** entre a y b , que se nota $(a : b)$, es el mayor de los divisores comunes entre a y b . Es decir $(a : b)$

$$(a : b) = c / c \in DivCom(\{a, b\}) \wedge (\forall d \in DivCom(\{a, b\})) d \leq c$$

Propiedades

- $(a : b) = (b : a)$ para todo $a, b \in \mathbb{Z}$ no nulos
- Si $c|a$ y $c|b \rightarrow c|(a : b)$
- $(a : b) = (|a| : |b|)$
- $(a : b)$ es único
- $(a : 1) = 1$ para todo $a \in \mathbb{Z}$
- $(\forall a, b \in \mathbb{Z}) (b|a \rightarrow (a : b) = |b|)$
- $(a : 0) = |a|$ para todo $a \in (\mathbb{Z} - \{0\})$
- Si p es un primo positivo, entonces, para todo $a \in \mathbb{Z}$ vale:

$$(a : p) = \begin{cases} p & \text{si } p|a \\ 1 & \text{sino} \end{cases}$$

- Sean $a, b \in \mathbb{Z}$ no nulos y sea $k \in \mathbb{Z} \rightarrow \text{DivCom}(\{a, b\}) = \text{DivCom}(\{a, a - kb\})$
- Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Si $a = bq + r$ con $q, r \in \mathbb{Z} \rightarrow (a : b) = (b : r)$

3.5. Algoritmo de euclides

El algoritmo de euclides hace uso de estas propiedades para calcular el MCD. Y propone lo siguiente:

Sean $a, b \in \mathbb{Z}$ no nulos, existe $l \in \mathbb{N}_0$ tal que en una sucesión de $l + 1$ divisiones se llega por primera vez al resto nulo $r_{l+1} = 0$. Entonces $(a : b) = r_l$, el último resto no nulo.

$$\begin{aligned} a &= k_1 b + r_1 \\ b &= k_2 r_1 + r_2 \\ &\vdots \\ r_{l-2} &= k_l r_{l-1} + r_l \\ r_{l-1} &= k_{l+1} r_l + r_{l+1} \end{aligned}$$

Propiedades/Consecuencias:

- $(a^m - 1 : a^n - 1) = a^{(m:n)} - 1$
- Sean $a, b \in \mathbb{Z}$ no nulos $\rightarrow \exists t, s \in \mathbb{Z} / (a : b) = at + bs$
- Sean $a, b \in \mathbb{Z}$ no nulos y $c \in \mathbb{Z}$, existen $s', t' \in \mathbb{Z}$ tal que $c = s'a + t'b$ si y solo si $(a : b) | c$
- $(a : b)$ es el número natural más chico que se puede escribir como combinación entera de a y b
- $d | a$ y $d | b \iff d | (a : b)$
- Sean $a, b, k \in \mathbb{Z}$ no nulos, entonces $(ka : kb) = |k|(a : b)$
- Sean $a, b \in \mathbb{Z}$ y $d \in \mathbb{N}$, son equivalentes:
 - $d | a, d | b$ y si $c | a$ y $c | b$ entonces $c \leq d$
 - $d | a, d | b \rightarrow \exists s, t \in \mathbb{Z} / d = sa + tb$
 - $d | a, d | b$ y si $c | a$ y $c | b$ entonces $c | d$

3.5.1. Números coprimos

Si $(a : b) = 1$ entonces se dice que a y b son **coprimos** y se nota $a \perp b$.

Propiedades

- Si $d = (a : b) \rightarrow \frac{a}{d}$ y $\frac{b}{d}$ son enteros y son coprimos.
- $a \perp b \iff \exists s, t \in \mathbb{Z} / 1 = sa + tb$
- $d | a$ y $d | b$ y $\frac{a}{d} \perp \frac{b}{d}$ entonces $d = (a : b)$
- $c | a$ y $d | a$ y $c \perp d \iff cd | a$
- Sea p primo, si $p | ab \rightarrow p | a$ ó $p | b$
- $d | ab$ y $d \perp a \rightarrow d | b$
- $a \perp b$ y $a \perp c \iff a \perp bc$
- Sean $a, b \in \mathbb{Z}$ no nulos, entonces $\frac{a}{(a:b)} \perp \frac{b}{(a:b)}$

- Sea $a, b \in \mathbb{Z}$ y $m_1, m_2 \in \mathbb{N}$ tal que $m_1 \perp m_2$, entonces $a \equiv b \pmod{m_1}$ y $a \equiv b \pmod{m_2} \iff a \equiv b \pmod{m_1 m_2}$
- $(a : b) = 1 \rightarrow (a^n : b^n) = 1$ ■ $(a : b) = d \rightarrow (a^n : b^n) = d^n$
- Sea p un número primo y $a \in \mathbb{Z}$ entonces $\text{Div}_+(p) = \{1, p\}$ y por lo tanto $\text{DivCom}_+(\{p, a\}) \subset \{1, p\}$
- Si p y q son números primos, entonces $(p : q) = 1$.

3.6. Factorización

Sea p un número primo y $a_1 \cdot a_2 \cdot \dots \cdot a_n \in \mathbb{Z}$ con $n \geq 2$, tal que $p | a_1 \cdot a_2 \cdot \dots \cdot a_n$ entonces $p | a_i$ para algún $0 \leq i \leq n$

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$, entonces a se escribe en forma única (**factoriza**) como producto de números primos, es decir:

$$\forall a \in \mathbb{Z} / a \neq 0, \pm 1, \exists r \in \mathbb{N} \text{ tal que existen } p_1, \dots, p_r \text{ primos distintos y } m_1, \dots, m_r \text{ números naturales tales que } a = \pm p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}$$

Propiedades

- Sean $a, b \in \mathbb{Z}$ no nulos de la forma $a = \pm p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ y $b = \pm p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, entonces:
 - $a \cdot b = p_1^{m_1+n_1} p_2^{m_2+n_2} \dots p_r^{m_r+n_r}$
 - $a^k = p_1^{km_1} p_2^{km_2} \dots p_r^{km_r}$
 - $(a : b) = p_1^{\min\{m_1, n_1\}} \dots p_r^{\min\{m_r, n_r\}}$
- Dado p primo, $p | a \iff p$ aparece en la factorización en primos de a .
- Cualquiera sea $a \in \mathbb{Z}$, a es divisible por un número finito de primos distintos.
- Sea $a \in \mathbb{Z}$ y $a = \pm p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ la factorización en primos de a , entonces:
 - $d | a \iff d = \pm p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$ con $0 \leq n_1 \leq m_1, \dots, 0 \leq n_r \leq m_r$
 - $|\text{Div}_+(a)| = \prod_{i=1}^r m_i$ y $|\text{Div}(a)| = 2 * |\text{Div}_+(a)|$
- $d | a \iff d^n | a^n$
- Sean $a, b \in \mathbb{Z}$ no nulos de la forma $a = \pm p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ y $b = \pm q_1^{n_1} q_2^{n_2} \dots q_r^{n_r}$, entonces $(a : b) = 1 \iff p_i \neq q_j \forall i, j$
- $(a : b) = 1 \iff (a^n : b^m) = 1 \forall m, n \in \mathbb{N}$
- $(a^n : b^n) = (a : b)^n \forall n \in \mathbb{N}$

3.7. Mínimo Común Múltiplo (MCM)

Sean $a, b \in \mathbb{Z}$ no nulos, el **mínimo común múltiplo** entre a y b ($[a : b]$) es el menor número natural que es múltiplo de a y de b .

Propiedades

- Sean $a, b \in \mathbb{Z}$ no nulos de la forma $a = \pm p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ y $b = \pm p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, entonces:

$$[a : b] = p_1^{\max\{m_1, n_1\}} \dots p_r^{\max\{m_r, n_r\}}$$

- $a|m$ y $b|m \iff [a : b]|m$
- $|a \cdot b| = (a : b)[a : b]$
- Si $a|b \rightarrow [a : b] = |b|$
- Si $(a : b) = 1 \rightarrow [a : b] = |a \cdot b|$

3.8. Ecuaciones lineales diofánticas

Las **ecuaciones diofánticas** son las ecuaciones lineales de la forma $aX + bY = c$ con $a, b, c \in \mathbb{Z}$, a, b no ambos nulos de las cuales se buscan los pares (X, Y) de soluciones enteras.

Si $a = 0$ ó $b = 0$, el problema se vuelve un problema de divisibilidad. $aX + 0Y = c$ tiene solución entera $\iff a|c$ y, en ese caso, las soluciones son todos los pares $(\frac{c}{a}, j)$ con $j \in \mathbb{Z}$.

Propiedades

- Sean $a, b, c \in \mathbb{Z}$ no nulos, la ecuación diofántica $aX + bY = c$ admite soluciones enteras si y solo si $(a : b)|c$.
- Sean $a, b \in \mathbb{Z}$ no nulos y coprimos, entonces la ecuación diofántica $aX + bY = c$ tiene soluciones enteras para todo $c \in \mathbb{Z}$

Sean $aX + bY = c$ y $a'X + b'Y = c'$ dos ecuaciones diofánticas, se dicen **equivalentes** si tienen exactamente las mismas soluciones. Y notamos

$$ax + by = c \rightsquigarrow a'X + b'Y = c'$$

Propiedades

- Sean $a, b, c \in \mathbb{Z}$ no nulos tales que $(a : b)|c$, entonces:

$$ax + by = c \rightsquigarrow \frac{a}{(a : b)}X + \frac{b}{(a : b)}Y = \frac{c}{(a : b)}$$

- Sean $a, b \in \mathbb{Z}$ no nulos, el conjunto S_0 de soluciones de la ecuación diofántica $aX + bY = c$ es:
 - $S_0 = \emptyset$ si $(a : b) \nmid c$
 - $S = \{(x, y) : x = x_0 + b'k, y = y_0 + a'k\}$ donde $a' = \frac{a}{(a:b)}$ y $b' = \frac{b}{(a:b)}$

3.9. Ecuaciones lineales de congruencia

Dado $m \in \mathbb{N}$ se puede aplicar el análisis realizado para las ecuaciones diofánticas a las ecuaciones de la forma $aX \equiv c \pmod{m}$ para $a, c \in \mathbb{Z}$.

Propiedades

- $aX \equiv c \pmod{m} \iff a'X \equiv c' \pmod{m'}$ si tienen exactamente las mismas soluciones.
- Sea $m \in \mathbb{N}$, dados $a, c \in \mathbb{Z}$, la ecuación de congruencia $aX \equiv c \pmod{m}$ tiene soluciones si y solo si $(a : m) | c$. Además, si ese es el caso, vale que

$$aX \equiv c \pmod{m} \iff \frac{a}{(a : m)}X \equiv \frac{c}{(a : m)} \pmod{\frac{m}{(a : m)}}$$

- Sean $m \in \mathbb{N}$, $a, c, d \in \mathbb{Z}$, entonces

$$(da)X \equiv dc \pmod{(dm)} \iff a \equiv c \pmod{m}$$

- Sean $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ tal que $a \perp m$, entonces la ecuación de congruencia $aX \equiv c \pmod{m}$ tiene soluciones enteras cualquiera sea $c \in \mathbb{Z}$
- El conjunto S de soluciones enteras de la ecuación de congruencia $aX \equiv c \pmod{m}$ es:
 - $S = \emptyset$ cuando $(a : m) \nmid c$
 - $S = \{x \in \mathbb{Z} : x \equiv x_0 \pmod{m'}\}$ donde $x_0 \in \mathbb{Z}$ es una solución particular cualquiera de la ecuación y $m' = \frac{m}{(a : m)}$

3.10. Sistemas equivalentes

Sean $m_1, \dots, m_n \in \mathbb{N}$ coprimos dos a dos, entonces:

$$\begin{cases} x \equiv c \pmod{m_1} \\ x \equiv c \pmod{m_2} \\ \vdots \\ x \equiv c \pmod{m_n} \end{cases} \iff x \equiv c \pmod{m_1 m_2 \dots m_n}$$

Sean $m, m' \in \mathbb{N}$ tales que $m' | m$, entonces para todo $c, c' \in \mathbb{Z}$ vale:

- Si $c \not\equiv c' \pmod{m}$, entonces el siguiente sistema es incompatible (no tiene soluciones enteras):

$$\begin{cases} x \equiv c' \pmod{m'} \\ x \equiv c \pmod{m} \end{cases}$$

- Si $c \equiv c' \pmod{m}$ entonces:

$$\begin{cases} x \equiv c' \pmod{m'} \\ x \equiv c \pmod{m} \end{cases} \iff X \equiv c \pmod{m}$$

3.11. Teorema chino del resto

Sean $m_1, \dots, m_n \in \mathbb{N}$ coprimos dos a dos, entonces para todo $c_1, \dots, c_n \in \mathbb{Z}$, el sistema:

$$\begin{cases} x \equiv c \pmod{m_1} \\ x \equiv c \pmod{m_2} \\ \vdots \\ x \equiv c \pmod{m_n} \end{cases}$$

tiene soluciones enteras $S = \{x \in \mathbb{Z} : x \equiv x_0 \pmod{m_1 m_2 \dots m_n}\}$

3.12. Pequeño teorema de fermat

Sea p un primo positivo, entonces $\forall a \in \mathbb{Z}$:

- $a^p \equiv a \pmod{p}$
- $p \nmid a \rightarrow a^n \equiv a^{r_{p-1}(n)} \pmod{p}$

Consecuencias/Propiedades

- Sea p un primo positivo, entonces $\forall a \in \mathbb{Z}$ tal que $p \nmid a$ y $n \in \mathbb{N}$ se tiene que $n \equiv r \pmod{p-1} \rightarrow a^n \equiv a^r \pmod{p}$.
- Sean p y q dos primos distintos y $a \in \mathbb{Z}$ coprimo con $p \cdot q$, entonces $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$ y por lo tanto, para todo $m \in \mathbb{N}$ vale:

$$m \equiv r \pmod{(p-1)(q-1)} \rightarrow a^m \equiv a^r \pmod{pq}$$

3.12.1. Teorema de Euler

Sea $m = p_1^{r_1} \dots p_s^{r_s}$ la factorización en primos de m , entonces definimos $\varphi(m) = \varphi(p_1^{r_1}) \dots \varphi(p_s^{r_s})$ y si p es un primo, $\varphi(p) = p - 1$.

Propiedades: Sea $m, a \in \mathbb{Z}$ tal que $(m : a) = 1$ y p un primo, entonces

- $a^{\varphi(m)} \equiv 1 \pmod{m}$
- $\varphi(a \cdot m) = \varphi(a)\varphi(m)$
- $\varphi(p^r) = p^{r-1}(p-1)$

3.13. Anillos y cuerpos

Sea $m \in \mathbb{N}$, consideremos en \mathbb{Z} la relación de congruencia módulo m . Entonces:

1. Sea $0 \leq r \leq m$, la clase de equivalencia \bar{r} de r es $\bar{r} = \{a \in \mathbb{Z} : a \equiv r \pmod{m}\}$ y $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \dots \cup \bar{r-1}$ es la partición de \mathbb{Z} asociada esta relación de equivalencia.
2. Notamos $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{r-1}\}$ y si $+$ y \cdot son las operaciones definidas por $\bar{r}_1 + \bar{r}_2 = \overline{r_1 + r_2}$ y $\bar{r}_1 \cdot \bar{r}_2 = \overline{r_1 \cdot r_2}$ entonces $\mathbb{Z}/m\mathbb{Z}$ es un **anillo conmutativo**

Propiedad:

- Sean $m \in \mathbb{N}$ y $a \in \mathbb{Z}$, entonces la ecuación de congruencia $aX \equiv c \pmod{m}$ tiene solución si y solo si $(a : m) = 1$ y, en este caso, la solución x_0 es única y $1 \leq x_0 < m$.
- Sea p un primo positivo y sea $a \in \mathbb{N}$ tal que $p \nmid a$, entonces la ecuación de congruencia $aX \equiv 1 \pmod{p}$ tiene solución única x_0 con $1 \leq x_0 \leq p$.

3.13.1. Elementos inversibles

El elemento \bar{r} es inversible en $\mathbb{Z}/m\mathbb{Z}$ si y solo si existe $\bar{x} \in \mathbb{Z}/m\mathbb{Z}$ tal que $r \cdot x = 1$.

Propiedad:

- En los enteros, los únicos elementos que tienen inverso multiplicativo son el -1 y el 1 .
- Sea $m \in \mathbb{Z}$ y $r \in \mathbb{Z}/m\mathbb{Z}$, entonces \bar{r} es inversible en $\mathbb{Z}/m\mathbb{Z}$ si y solo si $(m : r) = 1$.
- Sea p un primo positivo, entonces $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un **cuerpo**, es decir, además de ser un anillo conmutativo, satisface que todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ es inversible.

4. Polinomios

4.1. Números complejos

$(\mathbb{C}, +, \cdot)$ es un cuerpo en el que no se puede definir una relación \geq .

Dado $z \in \mathbb{C}$, la forma $z = a + bi$ con $a, b \in \mathbb{R}$ se llama la **forma binomial** de z , su **parte real** es $\operatorname{Re}(z) = a$ y su **parte imaginaria** es $\operatorname{Im}(z) = b$. Su **conjugado** $\bar{z} = a - bi \in \mathbb{C}$ y su **módulo** es $|z| = \sqrt{a^2 + b^2}$

Propiedades

- $|z| = 0 \iff z = 0$
- $|z + w| \leq |z| + |w|$
- $z \cdot \bar{z} = |z|^2$
- $\bar{z} \cdot \bar{w} = \overline{z \cdot w}$
- $z^{-1} = \frac{\bar{z}}{|z|^2}$
- $|z \cdot w| = |z||w|$
- $\overline{\bar{z}} = z$
- $z = \bar{z} \iff z \in \mathbb{R}$
- $z + \bar{z} = 2\operatorname{Re}(z)$
- $z - \bar{z} = 2i\operatorname{Im}(z)$
- Si $z \neq 0$, $|z^{-1}| = |z|^{-1}$
- Si $z \neq 0$, $|z^k| = |z|^k$ para todo $k \in \mathbb{Z}$
- $|\operatorname{Re}(z)| \leq |z|$
- $|\operatorname{Im}(z)| \leq |z|$
- $\overline{z + w} = \bar{z} + \bar{w}$
- $\bar{z}^{-1} = \overline{z^{-1}}$
- $||z| - |w|| \leq |z - w|$
- Sea $z \in \mathbb{C}$, entonces $\exists w \in \mathbb{C}$ tal que $w^2 = (-w)^2 = z$. Y si $z \neq 0$ entonces z tiene dos raíces cuadradas distintas que son w y $-w$.

La **forma trigonométrica** de z es $z = r(\cos(\theta) + i\operatorname{sen}(\theta))$ donde $r = |z|$ y θ es tal que $\cos(\theta) = \frac{\operatorname{Re}(z)}{|z|}$ y $\operatorname{sen}(\theta) = \frac{\operatorname{Im}(z)}{|z|}$.

Si elegimos θ con $0 \leq \theta < 2\pi$, entonces θ está determinado de forma única y se denomina **argumento** de z ($\arg(z)$).

- **Formula de euler:** $e^{i\theta} = \cos(\theta) + i\operatorname{sen}(\theta) \quad \forall \theta \in \mathbb{R}$
- Sea $z = r(\cos(\theta) + i\operatorname{sen}(\theta)) = re^{i\theta}$ con $r \in \mathbb{R}_{\geq 0}$ y $\theta \in \mathbb{R}$:
 - $\bar{z} = r(\cos(-\theta) + i\operatorname{sen}(-\theta)) = re^{-i\theta}$
 - $z^{-1} = r^{-1}(\cos(-\theta) + i\operatorname{sen}(-\theta)) = r^{-1}e^{-i\theta}$
- Sea $z = r(\cos(\theta) + i\operatorname{sen}(\theta)) = re^{i\theta}$ y $w = s(\cos(\psi) + i\operatorname{sen}(\psi)) = se^{i\psi}$ con $r, s \in \mathbb{R}_{\geq 0}$ y $\psi, \theta \in \mathbb{R}$:
 - $z \cdot w = rs(\cos(\theta + \psi) + i\operatorname{sen}(\theta + \psi)) = rse^{i(\theta + \psi)}$
 - $\arg(z + w) = \arg(z) + \arg(w) - 2k\pi$ con k elegido de tal modo que $0 \leq \arg(z) + \arg(w) - 2k\pi < 2\pi$
 - $\frac{z}{w} = \frac{r}{s}(\cos(\theta - \psi) + i\operatorname{sen}(\theta - \psi)) = \frac{r}{s}e^{i(\theta - \psi)}$
 - $z^n = r^n(\cos(n\theta) + i\operatorname{sen}(n\theta)) = r^ne^{in\theta}$

- $\arg(z^n) = n\arg(z) - 2k\pi$ con k elegido de tal modo que $0 \leq n\arg(z) - 2k\pi \leq 2\pi$
- $\arg(z^{-1}) = -\arg(z) + 2k\pi$
- $\arg(z + w) = \arg(z) + \arg(w) - 2k\pi$

Otra forma de escribir $z = a + bi$ es en forma de tuplas: $z = (a, b)$

- $(a, b) + (c, d) = (a + c, b + d)$
- $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$

4.2. Raíces n -ésimas

Sea $z \in \mathbb{C}$, hallar las **raíces n -ésimas** de z consiste en determinar los $w \in \mathbb{C}$ que cumplen $w^n = z$.

Sea $n \in \mathbb{N}$ y sea $z = se^{\psi i} \in \mathbb{C}$ con $s \in \mathbb{R}_{\geq 0}$ y $0 \leq \psi \leq 2\pi$, entonces z tiene n raíces n -ésimas w_0, \dots, w_{n-1} donde:

$$w_k = s^{\frac{1}{n}} e^{\theta_k i} \text{ donde } \theta_k = \frac{\psi + 2k\pi}{n} \text{ para } 0 \leq k \leq n-1$$

4.2.1. Raíces de la unidad

Cuando $z = 1$, el polinomio $x^n - z$ cumple que todas sus raíces w_0, \dots, w_n satisfacen $w^l = 1$ para $0 \leq l \leq n-1$. Estas raíces se denominan **raíces n -ésimas de la unidad** y cumplen que

$$w_k = e^{\frac{2k\pi}{n} i} \text{ con } 0 \leq k \leq n-1$$

Sea $n \in \mathbb{N}$, el conjunto G_n es el **conjunto de raíces n -ésimas de la unidad**, es decir:

$$G_n = \{w \in \mathbb{C} : w^n = 1\} = \{w_k = e^{\frac{2k\pi}{n} i} : 0 \leq k \leq n-1\}$$

Propiedades Sea $n \in \mathbb{N}$:

- $w \in G_n \iff w^n = 1$
- (G_n, \cdot) es un grupo abeliano, es decir que $\forall n \in \mathbb{N}$:
 - $\forall w, z \in G_n$ se tiene que $w \cdot z \in G_n$
 - $1 \in G_n$
 - $\forall w \in G_n, \exists w^{-1} \in G_n$
- $w \in G_n \rightarrow |w| = 1$
- $\forall w \in G_n, w^{-1} = \bar{w} \in G_n$
- $-1 \in G_n \iff n$ es par
- Sea $m \in \mathbb{Z}, n|m \rightarrow w^m = 1$
- Sea $m, m' \in \mathbb{Z}, m \equiv m' \pmod{n} \rightarrow w^m = w^{m'}$
- Existe $w \in G_n$ tal que $G_n = \{w^0, w^1, \dots, w^{n-1}\}$
- $\forall w \in G_n, w^{-1} = \bar{w} = w^{n-1}$
- Sea $m \in \mathbb{N}, G_n \cap G_m = G_{(n:m)}$
- Sea $m \in \mathbb{N}, n|m \iff G_n \subset G_m$
- Si $z \in G_n, \bar{z}^k = z^{-k} = z^{n-k}$

4.2.2. Raíces primitivas

Sea $n \in \mathbb{N}$, se dice que $w \in \mathbb{C}$ es una **raíz n -ésima primitiva de la unidad** si $G_n = \{w^k : 0 \leq k \leq n-1\}$

Propiedades Sea $n \in \mathbb{N}$ y $w \in \mathbb{C}$:

- w es una raíz n -ésima primitiva de la unidad si y solo si vale que $\forall m \in \mathbb{Z}, w^m = 1 \iff n|m$.
- Si w es una raíz primitiva de la unidad, entonces w^k es una raíz primitiva de la unidad si y solo si $(n:k) = 1$
- Sea $w_k = e^{\frac{2k\pi}{n}i}$ con $0 \leq k \leq n-1$, entonces w_k es una raíz primitiva de la unidad si y solo si $(n:k) = 1$.
- Sea p un primo, entonces cualquiera sea $k, 1 \leq k \leq p-1$, se tiene que $e^{\frac{2k\pi}{p}i}$ es raíz p -ésima primitiva de la unidad. Es decir que $\forall w \in G_p, w \neq 1$ se tiene que w es una raíz p -ésima primitiva de la unidad.

4.3. Polinomios

Sea K un cuerpo, se dice que f es un **polinomio con coeficientes en K** si f es de la forma:

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{i=0}^n a_i X^i$$

para algún $n \in \mathbb{N}_0$, donde X es una indeterminada sobre K y $a_i \in K$ para $0 \leq i \leq n$. Los elementos a_i se llaman los **coeficientes** de f .

Dos polinomios son **iguales** si y solo si coinciden todos sus coeficientes, es decir, si $f = \sum_{i=0}^n a_i X^i$ y $g = \sum_{i=0}^n b_i X^i$, entonces $f = g \iff a_i = b_i, 0 \leq i \leq n$.

El conjunto de todos los polinomios f con coeficientes en K se nota $K[X]$

Si f no es el polinomio nulo ($f \neq 0$), entonces se puede escribir para algún $n \in \mathbb{N}_0$, de la forma $f = \sum_{i=0}^n a_i X^i$ con $a_n \neq 0$.

En ese caso, n es el **grado** de f y se nota $\text{gr}(f)$ y a_n es el **coeficiente principal** de f .

El polinomio nulo no tiene grado. Cuando el coeficiente principal de f es igual a 1, entonces se dice que el polinomio es **mónico**.

Operaciones : Sean $f = \sum_{i=0}^n a_i X^i$ y $g = \sum_{i=0}^n b_i X^i$ polinomios en $K[X]$:

- La **suma** se define como:

$$f + g = \sum_{i=0}^n (a_i + b_i) X^i$$

- La **multiplicación** como:

$$f \cdot g = \sum_{k=0}^{n+m} c_k X^k \text{ donde } c_k = \sum_{i+j=k} a_i b_j$$

Propiedades: Sea K un cuerpo y sean $f, g \in K[X]$ no nulos, entonces:

- Si $f + g \neq 0$, entonces $\text{gr}(f + g) \leq \max\{\text{gr}(f), \text{gr}(g)\}$
- $\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g)$
- $\text{cp}(f \cdot g) = \text{cp}(f) \cdot \text{cp}(g)$

Sea K un cuerpo, entonces $(K[X], +, \cdot)$ es un anillo conmutativo y vale que:

$$\forall f, g \in K[X], f \cdot g = 0 \rightarrow f = 0 \text{ ó } g = 0$$

$f \in K[X]$ es inversible si y solo si $f \in K^\times$, o sea que los elementos inversibles de $K[X]$ son los polinomios de grado 0.

4.3.1. Divisibilidad

Sean $f, g \in K[X]$ con $g \neq 0$, se dice que g **divide a** f , y se nota $g|f$, si existe un polinomio $q \in K[X]$ tal que $f = q \cdot g$

Propiedades

- Todo polinomio $g \neq 0$ satisface que $g|0$
- Si $f|g$ y $g \neq 0$, entonces $\text{gr}(f) \leq \text{gr}(g)$
- $g|f \iff cg|f, \forall c \in K^\times$
- $g|f$ y $f|g \iff f = cg$ para algún $c \in K^\times$
- $f|g$ y $\text{gr}(f) = \text{gr}(g) \rightarrow f = k \cdot g$ para algún $k \in K$
- Para todo $f \in K[X]$, $f \notin K$ se tiene $c|f$ y $cf|f, \forall c \in K^\times$.

La **divisibilidad** de los polinomios cumple exactamente las mismas propiedades que la divisibilidad de los números enteros.

4.3.2. Reducibilidad

Sea $f \in K[X]$, se dice que f es **irreducible** en $K[X]$ cuando $f \notin K$ y los únicos divisores de f son de la forma $g = c$ ó $g = cf$ para algún $c \in K^\times$. O sea que f tiene únicamente dos divisores mónicos (distintos), que son 1 y $f/\text{cp}(f)$.

Y se dice que f es reducible en $K[X]$ cuando $f \notin K$ y f tiene algún divisor $g \in K[X]$ con $g \neq c$ y $g \neq cf, \forall c \in K^\times$, es decir, f tiene algún divisor $g \in K[X]$ (no nulo por definición) con $0 \leq \text{gr}(g) \leq \text{gr}(f)$.

4.3.3. Algoritmo de la división

Dados $f, g \in K[X]$ no nulos, existen únicos $q, r \in K[X]$ que satisfacen:

$$f = q \cdot g + r \text{ con } r = 0 \text{ ó } \text{gr}(r) < \text{gr}(g)$$

Se dice que q es el **cociente** y r es el **resto** de la división de f por g , que notaremos $r_g(f)$.

4.3.4. Máximo Común Divisor (MCD)

Sean $f, g \in K[X]$ no ambos nulos. El máximo común divisor entre f y g , que se nota $(f : g)$, es el polinomio mónico de mayor grado que divide simultáneamente a f y a g .

Propiedades: Sean $f, g \in K[X]$,

- $(f : 0) = \frac{f}{\text{cp}(f)}$
- Sea g no nulo. Si $f = q \cdot g + r$ para $q, r \in K[X]$, entonces $(f : g) = (g : r)$.
- Sea $c \in K^\times$, $(c : g) = 1$
- Si $g|f$, entonces $(f : g) = \frac{g}{\text{cp}(g)}$
- Por el algoritmo de la división de euclides existen $s, t \in K[X]$ tal que $(f : g) = sf + tg$
- Si ni f ni g son nulos. El MCD entre f y g es el único polinomio mónico $h \in K[X]$ que satisface simultáneamente que $h|f$ y $h|g$.
- Si $\bar{h} \in K[X]$ satisface que $\bar{h}|g$ y $\bar{h}|f \rightarrow \bar{h}|h$

4.3.5. Polinomios coprimos

Sean $f, g \in K[X]$ no ambos nulos, se dice que f y g son **coprimos** si satisfacen $(f : g) = 1$.

Propiedades :

- Si g y h son coprimos, entonces $g|f \wedge h|f \iff gh|f$
- Si g y h son coprimos, entonces $g|hf \iff g|h$

Sea $f \in K[X]$ un polinomio irreducible en $K[X]$, entonces:

- $\forall g \in K[X]$, $(f : g) = \frac{f}{\text{cp}(f)}$ si $f|g$ y $(f : g) = 1$ si $f \nmid g$.
- $\forall g \in K[X]$, $f|gh \rightarrow f|g$ ó $f|h$.

4.3.6. Reducibilidad de un polinomio

Sea K un cuerpo y sea $f \in K[X]$ un polinomio no constante, entonces existen únicos polinomios irreducibles mónicos g_1, \dots, g_r tales que:

$$f = cg_1^{m_1} \dots g_r^{m_r} \text{ donde } c \in K - \{0\} \text{ y } m_1, \dots, m_r \in \mathbb{N}$$

Sea $f = a_n X^n + \dots + a_1 X + a_0 \in K[X]$ un polinomio, entonces f define en forma natural una función $f : K \rightarrow K$, $f(x) = a_n x^n + \dots + a_1 x + a_0$ que se llama **función de evaluación**.

Propiedades:

- $(f + g)(x) = f(x) + g(x)$
- $(f \cdot g)(x) = f(x) \cdot g(x)$
- Si $f = gq + r$ con $q, g, r \in K[X]$, entonces $f(x) = g(x)q(x) + r(x)$

4.3.7. Raíces de un polinomio

Sea $f \in K[X]$ y $x \in K$, si $f(x) = 0$ se dice que x es una **raíz** de f en K .

$$x \text{ es raíz de } f \iff f(x) = 0 \iff (X - x) \mid f \iff f = (X - x)q \text{ para algún } q \in K[X]$$

Propiedades:

- Si $f \neq 0$, $X - x$ es un factor irreducible (mónico) en la descomposición en irreducibles de $f \in K[X]$.
- Si $g \mid f$ en $K[X]$, sea $x \in K$ una raíz de $g \rightarrow x$ es raíz de f .
- $f(x) = 0$ y $g(x) = 0 \iff (f : g)(x) = 0$

4.3.8. Polinomios cuadráticos

Sea K un cuerpo y sea $f = aX^2 + bX + c \in K[X]$, con $a \neq 0$, un polinomio cuadrático. Entonces se define el **discriminante** de f como $\Delta = b^2 - 4ac$.

Propiedades: Sea f un polinomio cuadrático en $K[X]$,

- f es reducible en $K[X]$ si y solo si f tiene una raíz en K
- Si existe $w^2 = \Delta$, entonces f tiene al menos una raíz en K .
- Si $2 \neq 0$ en K , f es reducible en $K[X] \iff$ existe $w^2 = \Delta$ y, en ese caso, las raíces de f en K son

$$x_{\pm} = \frac{-b \pm w}{2a}$$

y $f = a(X - x_+)(X - x_-)$ es la factorización de f en $K[X]$.

4.3.9. Multiplicad de raíces

Sean $f \in K[X]$ no nulo y sea $m \in \mathbb{N}_0$, se dice que $x \in K$ es una raíz de multiplicidad m de f si $(X - x)^m \mid f$ y $(X - x)^{m+1} \nmid f$. Y notamos $\text{mult}(x, f) = m$

Propiedades:

- $\text{mult}(x, f) \leq \text{gr}(f)$
- $\text{mult}(x, f) = 0 \iff x$ no es raíz de f .

4.3.10. Derivadas

Sea $f = a_n X^n + \dots + a_0 \in K[X]$, definimos su **derivada** como:

$$f' = na_n X^{n-1} + a_1 \in K[X]$$

Propiedades:

- $(f + g)' = f' + g'$
- $(g \circ f)' = (g' \circ f) \cdot f'$
- $f'' = (f')'$ y $f^{(m)} = (f^{(m-1)})'$
- Sea $f \in K[X]$ y sea $x \in K$,
 - x es raíz múltiple de f si y solo si $f(x) = 0$ y $f'(x) = 0$.
 - x es raíz simple de f si y solo si $f(x) = 0$ y $f'(x) \neq 0$

- Sea $K = \mathbb{Q}, \mathbb{R}$ ó \mathbb{C} y $x \in K$ entonces:

- $\text{mult}(x, f) = m \iff f(x) = 0 \text{ y } \text{mult}(x, f') = m - 1$
-

$$\text{mult}(x, f) = m \iff \begin{cases} f(x) = 0 \\ f'(x) = 0 \\ \vdots \\ f^{(m-1)}(x) = 0 \\ f^{(m)}(x) \neq 0 \end{cases}$$

- Sean $x_1, \dots, x_r \in K$ raíces distintas de f tales que $\text{mult}(x_1, f) = m_1, \dots, \text{mult}(x_r, f) = m_r$, entonces $(X - x_1)^{m_1} \dots (X - x_r)^{m_r} | f$.
- Sea K un cuerpo y sea $f \in K[x]$ un polinomio no nulo de grado n , entonces f tiene a lo sumo n raíces en K contadas con multiplicidad.

4.3.11. Polinomios en \mathbb{C}

Sea $f \in \mathbb{C}[X]$ un polinomio no constante, entonces $\exists z \in \mathbb{C} / f(z) = 0$ y si $\text{gr}(f) = n$, entonces f tiene exactamente n raíces irreducibles contadas con multiplicidad en \mathbb{C} .

Propiedades : Sea $f \in \mathbb{C}[X]$,

- f es irreducible en $\mathbb{C}[X]$ si y solo si $\text{gr}(f) = 1$.
- La factorización en irreducibles de f en $\mathbb{C}[X]$ es de la forma:

$$f = c(x - z_1)^{m_1} \dots (x - z_r)^{m_r} \text{ donde } z_1, \dots, z_r \in \mathbb{C} \text{ son distintos, } m_1, \dots, m_r \in \mathbb{N} \text{ y } c \in \mathbb{C}^\times$$

No existe ninguna formula que describa las raíces complejas de un polinomio general cualquiera $f \in \mathbb{C}[X]$ de grado mayor igual a 5 a partir de sus coeficientes, de las operaciones elementales $+$, $-$, \cdot , $/$ y extracciones de raíces n -ésimas.

4.4. Polinomios en \mathbb{R}

Propiedades: Sea $f \in \mathbb{R}[X]$

- Si f es de grado impar, entonces f tiene al menos una raíz en \mathbb{R} .
- Sea $z \in \mathbb{C} - \mathbb{R}$, entonces:
 - $f(z) = 0 \iff f(\bar{z}) = 0$
 - $\forall m \in \mathbb{N}, \text{mult}(z, f) = m \iff \text{mult}(\bar{z}, f) = m$
 - $(X - z)(X - \bar{z})$ es un polinomio irreducible en $\mathbb{R}[X]$
 - $f(z) = 0 \rightarrow (X - z)(X - \bar{z})|f$ en $\mathbb{R}[X]$
 - $\text{mult}(z, f) = m \rightarrow ((X - z)(X - \bar{z}))^m|f$ en $\mathbb{R}[X]$
- Los polinomios irreducibles en $\mathbb{R}[X]$ son exactamente los siguientes: los de grado 1 y los de grado dos con discriminante negativo.
- Sea $f \in \mathbb{R}[X] - \mathbb{R}$ entonces, la factorización en irreducibles de $f \in \mathbb{R}[X]$ es de la forma:

$$f = c(X - x_1)^{m_1} \dots (X - x_r)^{m_r} (x^2 + b_1x + c_1)^{n_1} \dots (x^2 + b_sx + c_s)^{n_s}$$

donde $c \in \mathbb{R}^\times$, $r, s \in \mathbb{N}_0$, $m_i, n_j \in \mathbb{N} \forall 1 \leq i \leq r, 1 \leq j \leq s$, $x_1, \dots, x_r \in \mathbb{R}$, $b_i, c_i \in \mathbb{R}$ y $\Delta_j = b_j^2 - 4c_j < 0$.

- Sea $f = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ con $a_n, a_0 \neq 0$, si $\frac{\alpha}{\beta} \in \mathbb{Q}$ es una raíz racional de f , con α y β coprimos, entonces $\alpha|a_0$ y $\beta|a_n$.

4.4.1. Lema de Gauss (Algoritmo)

1. Construir el conjunto de divisores positivos y negativos de a_0 (\mathcal{N})
2. Construir el conjunto de divisores positivos y negativos de a_n (\mathcal{D})
3. Las raíces del polinomio f se encuentran en el conjunto de todas las fracciones coprimas α/β , eligiendo α en \mathcal{N} y β en \mathcal{D} .

Sea $m \in \mathbb{Q}$ tal $\sqrt{m} \notin \mathbb{Q}$, y sean $a, b \in \mathbb{Q}$, con $b \neq 0$. Sea $f \in \mathbb{Q}[X]$, entonces:

- $g := (X - (a + b\sqrt{m}))(X - (a - b\sqrt{m}))$
- $f(a + b\sqrt{m}) = 0 \rightarrow g|f$ en $\mathbb{Q}[X]$
- $f(a + b\sqrt{m}) = 0 \iff f(a - b\sqrt{m}) = 0$
- $\forall m \in \mathbb{N}, \text{mult}(a + b\sqrt{m}, f) = m \iff \text{mult}(a - b\sqrt{m}, f) = m$