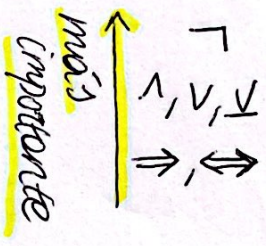
Lógica

Operadores lógicos

$\vee$: "o", "disyunción"
$\wedge$: "y", "conjunción"
$\Leftrightarrow$: "equivalencia", "si y solo si"
$\Rightarrow$: "implica", "si p entonces q"

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \veebar q$
V	V	V	V	V	V	F
V	F	F	V	F	F	V
F	V	F	V	V	F	V
F	F	F	F	V	V	F



Tautologías básicas

$p \vee V \Leftrightarrow V$; $p \wedge F \Leftrightarrow F$ — Dominancia
$p \wedge V \Leftrightarrow p$; $p \vee F \Leftrightarrow p$ — Identidad
$p \vee p \Leftrightarrow p$; $p \wedge p \Leftrightarrow p$ — Idempotencia
$p \vee \neg p \Leftrightarrow V$ — Tercio excluso
$p \wedge \neg p \Leftrightarrow F$ — Consistencia
$p \Rightarrow p \vee q$; $p \wedge q \Rightarrow p$ — Relajación

$\neg(\neg p) \Leftrightarrow p$ — Doble negación
$p \vee (p \wedge q) \Leftrightarrow p$; $p \wedge (p \vee q) \Leftrightarrow p$ — Absorción
$[p \Rightarrow q] \Leftrightarrow [\neg p \vee q]$ — Caracterización implica
$[p \Leftrightarrow q] \Leftrightarrow [(p \Rightarrow q) \wedge (q \Rightarrow p)]$ — Caracterización equivalencia
$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$ — Transitividad implica
$[(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)] \Rightarrow (p \Leftrightarrow r)$ — Transitividad equivalencia

Conmutatividad del $\wedge, \vee, \veebar, \Leftrightarrow$
$p \vee q \Leftrightarrow q \vee p$

Asociatividad del $\vee, \wedge, \veebar$
$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$

Distributividad del $\wedge$ respecto al $\vee$
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
$(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$

Distributividad del $\vee$ respecto el $\wedge$
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
$(p \wedge q) \vee r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$

Leyes de Morgan
$\overline{(p \vee q)} \Leftrightarrow \neg p \wedge \neg q$
$\overline{(p \wedge q)} \Leftrightarrow \neg p \vee \neg q$

Extras
$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ — Contrarecíproca
$p \wedge (p \Rightarrow q) \Rightarrow q$ — Modus ponens
$[(p \Rightarrow q) \Leftrightarrow V] \Leftrightarrow [p \wedge \neg q \Rightarrow F]$ — Absurdo

Técnicas demostración

Verificación exploratoria
└ Asumir que algo es V o F

Demostración simbólica
└ Simplificación de 1 lado

Contrarecíproca
└ Equivalente demostrar $p \Rightarrow q$ a $\bar{q} \Rightarrow \bar{p}$

Reducción al absurdo
└ cambiar $\Rightarrow$ por $\wedge$ y poner lo 2do negativo

Función proposicional o predicado $P(x, y, z)$
Expresión depende de variables, al ser reemplazadas x elementos del conjunto de referencia E, hacen a P proposición pos a V o F.

Cuantificadores

Universal ($\forall$) "un gran $\wedge$" $(\forall x \in E, P(x))$
↳ para todo

Existencial ($\exists$) "un gran $\vee$" $(\exists x \in E, P(x))$
↳ existe al menos un

negación →
$(\exists x \in E, \overline{P(x)})$
$(\forall x \in E, \overline{P(x)})$

$\exists!$ $(\exists! x \in E, P(x))$
↳ existe un único

Principio Inducción

Sea $P(n)$ un predicado, entonces

$$(\forall n \geq n_0, P(n)) \iff (P(n_0) \wedge (\forall n > n_0, P(n_0) \wedge P(n_0+1) \wedge \dots \wedge P(n-1) \Rightarrow P(n))$$

$P(n-1)$ ← o $P(n+1)$

CASO BASE — Hipotesis Inductiva — Paso inductivo

¡Ejercicios!
1. "todo"
2. CB → n_0
3. Hipotesis inductiva: $P(n_0) \wedge P(n_0+1) \wedge \dots \wedge P(n-1)$ ← o $(n+1)$
4. Luego, resolver y reemplazar por hipotesis inductiva (con el $n-1$ o $n+1$)

Conjuntos

se denotan con mayusculas, sus elementos con minusculas

Conjunto vacío $\emptyset$: $\forall x \in E, x \in \emptyset \iff F$

Inclusión $\subseteq$: $A \subseteq B \iff (\forall x \in E, x \in A \Rightarrow x \in B)$

Igualdad $=$: $A = B \iff (\forall x \in E, x \in A \iff x \in B)$

$A \cup B \iff (\forall x \in E, x \in A \cup B \iff x \in A \vee x \in B)$

$A \cap B \iff (\forall x \in E, x \in A \cap B \iff x \in A \wedge x \in B)$

$A^c \to \bar{A} \iff (\forall x \in E, x \in A^c \iff x \notin A)$

$A \setminus B \iff (\forall x \in E, x \in A \setminus B \iff x \in A \wedge x \notin B)$

$A \triangle B \iff (\forall x \in E, x \in A \triangle B \iff x \in A \veebar x \in B)$

Propiedades

Transitividad de $\subseteq$
$A \subseteq B \wedge B \subseteq C \iff A \subseteq C$

Antisimetría de $\subseteq$
$A \subseteq B \wedge B \subseteq A \iff A = B$

Leyes de Morgan
$(A \cap B)^c = A^c \cup B^c$
$(A \cup B)^c = A^c \cap B^c$

Doble complemento
$(A^c)^c = A$

Idempotencia
$A \cap A = A \quad A \cup A = A$

Conmutatividad
$A \cap B = B \cap A \quad A \cup B = B \cup A \quad A \triangle B = B \triangle A$

Asociatividad
$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$
$A \triangle (B \triangle C) = (A \triangle B) \triangle C$

—o—

- $A \cap \bar{A} = \emptyset \quad A \cup \bar{A} = E$
- $A \cup \emptyset = A \quad A \cap \emptyset = \emptyset$
- $A \cap E = A \quad A \cup E = E$

- $A \subseteq A \cup B$
- $B \subseteq A \cup B$
- $A \cap B \subseteq A$
- $A \cap B \subseteq B$
- $A \subseteq C \wedge B \subseteq C \Rightarrow A \cup B \subseteq C$
- $C \subseteq A \wedge C \subseteq B \Rightarrow C \subseteq A \cap B$

Conjuntos

Par ordenado: 2 elementos a y b en E y F → 2-tupla de a y b $(a,b)=\{a,\{a,b\}\}$

Producto cartesiano: $A\subseteq E$ con $B\subseteq F \to A\times B$ $[\forall a\in E, \forall b\in F, (a,b)\in A\times B \Leftrightarrow a\in A \wedge b\in B]$

↳ para desarrollar ejercicios, llevarlos a la definición

Conjunto potencia (partes de...) Conjunto de los subconjuntos de A → $\mathcal{P}(A): X\in\mathcal{P}(A)\Leftrightarrow X\subseteq A$

Partición conjuntos $\mathcal{C}\subseteq\mathcal{P}(A)$ → $\forall C\in\mathcal{C}, C\neq\emptyset$

→ (No tiene elementos en común) $\forall C, C'\in\mathcal{C}, C\neq C' \Rightarrow C\cap C'=\emptyset$

→ $\mathcal{C}$ cubre todo A

Cuantificadores sobre conjuntos
- $\forall x\in A, P(x) \Leftrightarrow (\forall x\in A, x\in A \Rightarrow P(x))$
- $\exists x\in A, P(x) \Leftrightarrow (\exists x\in A, x\in A \wedge P(x))$

Funciones

$f:A\to B$
- $\forall a\in A, \exists! b\in B,$
- $G\subseteq A\times B, \to G_f=\{(a), f(a)) / a\in A\}$

G: Grafo
A: Dom(f)
B: codominio(f)

→ $f(a)=b$

Igualdad de funciones: $Dom(f)=Dom(g) \wedge Cod(f)=Cod(g) \wedge \forall x\in Dom(f), f(x)=g(x)$

grafos iguales

Conjunto funciones: Todas las funciones de A en B → $B^A=\{f:A\to B \mid f \text{ función}\}$

*Identidad de un conjunto A: $id_A: A\to A$; $id_A(x)=x$ para cada $x\in A$

Inyectividad: $\forall x_1, x_2\in A \quad f(x_1)=f(x_2)\Rightarrow x_1=x_2$
$\forall x_1, x_2\in A \quad x_1\neq x_2 \Rightarrow f(x_1)\neq f(x_2)$
↳ para ejercicios, reemplazar con incognitas x e y, e igualar para comprobar punto 1

Epiyectividad: $\forall y\in B, \exists x\in A, y=f(x)$
↳ en hoja aparte despejar y como el calculo inverso y luego escribirlo "mágicamente"

Biyectividad: $Iny \wedge Epiy$
↳ id_A es biyectiva!

Imagenes y Preimagenes

$f: A \to B$ función $f(a) = b$ → b es la imagen de a por f
→ a es la preimagen de b por f

Conjunto imagen

$A' \subseteq A$:

- $f(A') = \{f(x) \in B \mid x \in A'\}$
- $\forall y \in B, (y \in f(A') \Leftrightarrow \exists x \in A', f(x) = y)$
- $f(A')$ es subconjunto de B (todas las imágenes de los elementos de A')

Propiedades:

- $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$
- $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
- $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

Conjunto preimagen

$B' \subseteq B$:

- $f^{-1}(B') = \{x \in A : f(x) \in B'\}$
- $\forall x \in A, (x \in f^{-1}(B') \Leftrightarrow f(x) \in B')$
- $f^{-1}(B')$ es subconjunto de A (todas las preimagenes de los elementos de B')

Propiedades

- $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$
- $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
- $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

—o—

Propiedades globales

- $f(f^{-1}(B')) = B' \cap f(A)$
- $A' \subseteq f^{-1}(f(A'))$
- ~~$f(f^{-1}(B')) \subseteq B$~~

- f inyectiva $\Leftrightarrow \forall y \in B,\ f^{-1}(\{y\}) = \emptyset \vee (\exists! x \in A, f^{-1}(\{y\}) = \{x\})$
- f epiyectiva $\Leftrightarrow \forall y \in B,\ f^{-1}(\{y\}) \neq \emptyset$
- f biyectiva $\Leftrightarrow \forall y \in B, \exists! x \in A, f^{-1}(\{y\}) = \{x\} \vee \forall B' \subseteq B, f^{-1}(B') = \{B'\}$

Relaciones

$(A, B, \mathcal{R})$ $\mathcal{R} \subseteq A \times B$ • A dominio relación ∧ B codominio relación

- $(a,b) \in A \times B \to a \mathcal{R} b$ cuando $(a,b) \in \mathcal{R}$
  $\to a \not\mathcal{R} b$ cuando $(a,b) \notin \mathcal{R}$
- $\mathcal{R}$ relación en $A \times B$
- $\mathcal{R}$ relación en $A \times A$ = $\mathcal{R}$ relación en A

Propiedades $\mathcal{R}$ en A

- Refleja: $\forall x \in A, x\mathcal{R}x$
- Simétrica: $\forall x,y \in A, x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- Antisimétrica: $\forall x,y \in A, x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x=y$
- Transitiva: $\forall x,y,z \in A, x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$

Tipos Relaciones

Orden: Refleja, Transitiva, Antisimetrica

- $x\mathcal{R}y$: x precede a y
- orden total: si son comparables $(x\mathcal{R}y \vee y\mathcal{R}x)$
  orden parcial: si no son comparables

Equivalencia: Refleja, Transitiva, Simetrica

- Clase equivalencia $[a]_{\mathcal{R}} = \{x \in A \mid a\mathcal{R}x\} \subseteq A$
  - $\forall a \in A, [a]_{\mathcal{R}} \neq \emptyset$
    - $a\mathcal{R}b$
    - $b \in [a]_{\mathcal{R}}$
    - $[b]_{\mathcal{R}} \subseteq [a]_{\mathcal{R}}$
    - $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$
    - $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset$
  - Conjunto cociente: Conjunto clases de equivalencia
    - $A/\mathcal{R} = \{[a]_{\mathcal{R}} \mid a \in A\}$
      - conjunto $A/\mathcal{R}$ es partición de A

*Divisibilidad

- $a|b$ si existe $c \in \mathbb{Z}$ tal que $b = ca$

$$a \equiv_n b \Leftrightarrow \frac{a-b}{n}$$

Sumatorias

Propiedades:

- $\sum_{i=k}^{m} \lambda a_i = \lambda \sum_{i=k}^{m} a_i$
- $\sum_{i=k}^{m} (a_i \pm b_i) = \sum_{i=k}^{m} a_i \pm \sum_{i=k}^{m} b_i$
- $\sum_{i=k}^{m} a_i = \sum_{i=k}^{p} a_i + \sum_{i=p+1}^{m} a_i$
- $\sum_{i=k}^{m+p} a_i = \sum_{j=k-p}^{m} a_{j+p}$
- $\sum_{i=k}^{m} (a_{i+1} - a_i) = a_{m+1} - a_k$ (telescopica)
- $\sum_{k=m}^{m} 1 = n - m + 1$

Formulas:

- $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
- $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$
- $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$
- $\sum_{i=1}^{n} a = na$
- $\sum_{j=1}^{n} a^j = \frac{1-a^{n+1}}{1-a}$
- $\sum_{j=0}^{n} a^j = \frac{a^{n+1}-a}{a-1}$
- $\sum_{i=1}^{n} \frac{1}{a^i} = \frac{a^n - 1}{a^{n+1} - a^n}$
- $\sum_{k=1}^{n} ak = a \sum_{k=1}^{n} k$

Sumatorias dobles

$\sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}$ / $\sum_{j=1}^{n} \sum_{i=1}^{j} a_{ij} \neq \sum_{i=1}^{j} \sum_{j=1}^{n} a_{ij}$

En general para no intercambiables:

$\sum_{j=1}^{n} \sum_{i=j}^{n} a_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{i} a_{ij}$

* Usar fracciones parciales ayuda: $\frac{1}{(x)(y)} = \frac{A}{x} + \frac{B}{y}$ y resolver

Cardinalidad

Finita A es conjunto finito ssi con $n \in \mathbb{N}$ existe $f: A \to [1..n]$ biyectiva

↳ $f[1..n]$ biy ssi, $a_1 \dots a_n \in A$ son distintos entre si

↳ $a_1 \dots a_m$ y $b_1 \dots b_n$ son enumeraciones de A ssi $m=n$

↳ $f: A \to [1..n]$ y $g: A \to [1..m]$ biyectivas ssi $n=m$

Cardinal finito: $n \in \mathbb{N}$ enumeración $a_1 \dots a_n$ es cardinal de A, denotado $|A|$

Propiedades/formulas:

- Sean A y B finito: → $|\emptyset| = 0 \Rightarrow |A| = 0 \Leftrightarrow A = \emptyset$
  → $|\{a\}| = 1 \Rightarrow |\{\emptyset\}| = 1$
  → $A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$
  → $A \subseteq B \wedge |A| = |B| \Leftrightarrow A = B$
  → $A \subseteq B \Rightarrow |B \setminus A| = |B| - |A|$
  → $|A \cup B| = |A| + |B| - |A \cap B|$
  → $|B \setminus A| = |B| - |A \cap B|$
  → $|A \times B| = |A| \cdot |B|$
  → $|B^A| = \underbrace{B \times \dots \times B}_{A \text{ veces}} = |B|^{|A|}$
- $\exists f: A \to B$ biy $\Leftrightarrow$ B es finito $\wedge |A| = |B|$
- Sea B finito. $A \subseteq B \Rightarrow$ A es finito y $|A| \leq |B|$
- Sean A y B finitos con $|A| = |B|$ y $f: A \to B$ es equivalente decir que → f es iny → f es epiy → f es biy
- A y B conjuntos donde B es finito → A es finito y $|A| \leq |B|$ ssi $f: A \to B$ iny
  → A es finito y $|A| = |B|$ ssi $f: A \to B$ biy
- Conjuntos $A_1, \dots A_n$ son disjuntos pares se tiene: $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$

* Sin, $k \in \mathbb{N}, k \leq n, |A| = A$ y $|B| = n$ → Hay n^k funciones de A en B, esto es, $|B^A| = n^k$ *
→ Hay $n!/(n-k)!$ funciones iny de A en B
→ Si $n=k$, hay $n!$ funciones biy de A en B, y ninguna si $n \neq k$

Coeficientes binomiales $n, k \in \mathbb{N}, k \geq 0 \to \binom{n}{k} = n^\circ$ conjuntos de tamaño k en un conjunto de n elementos

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

Propiedades
- $\binom{n}{k} = 0$ si $k > n$
- $\binom{n}{0} = \binom{n}{n} = 1$
- $\binom{n}{1} = \binom{n}{n-1} = n$
- $\binom{n}{k} = \binom{n}{n-k}$
- $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$, si $k \neq 0$
- $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$ triangulo Pascal ↑
- $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

Binomio Newton
$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

Cardinalidad

Infinita: Son aquellos que no son finitos lol

Propiedades

- $\varphi: A \to B$ biyectiva $\Leftrightarrow |A| = |B|$
- $|A| \leq |A|$
- $A \subseteq B$ entonces $|A| \leq |B|$
- $|A| \leq |B| \wedge |B| \leq |C| \Rightarrow |A| \leq |C|$
- $|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$
- $f: A \to B$ función $\to |f(A)| \leq |A|$
- A infinito y B finito: $|A \cup B| = |A \setminus B| = |A|$
- $|\mathbb{N}|$ es el menor cardinal infinito $\to |\mathbb{N}| \leq |A|$

Numerables: Cualquier conjunto A tq $|A| = |\mathbb{N}|$
- ↳ $\mathbb{Z}, \mathbb{Q}, \mathbb{N} \times \mathbb{N}$ son numerables
- ↳ A y B numerables → A∪B es numerable
- ↳ Todo infinito con $|A| \leq |\mathbb{N}|$ es numerable

→ Para comprobar que es numerable
1. Crear función $\varphi: \mathbb{N} \to A$. $\varphi: A \to \mathbb{N}$ y demostrar su biyectividad
2. Dem que es infinito y que $A \subseteq B$ con B numerable
   ↳ $|\mathbb{N}| \leq |A| \wedge |A| \leq |\mathbb{N}| \Rightarrow |A| = |\mathbb{N}|$

Estructuras Algebraicas

***LCI**: Ley de composición interna es una función $*$ $A \times A \to A$, $(x, y) \to x * y$

$*$ es una lci definida sobre A, $(A, *)$ es una estructura algebraica. Y si Δ tb cumple con eso se denomina $(A, *, \Delta)$

Definiciones importantes:

- Asociatividad: $*$ es asociativa si $\forall x, y, z \in A$, $(x * y) * z = x * (y * z)$
- Neutro: $e \in A$ es neutro para $*$ si $\forall x \in A$, $e * x = x * e = x$
- Inverso: x tiene inverso si existe $y \in A$ tq $x * y = y * x = e$ *(ambos son inversos entre sí)*
- Conmutatividad: $*$ es conmutativa si $\forall x, y \in A$, $x * y = y * x$
- Absorbente: $a \in A$ es absorbente si $\forall x \in A$, $x * a = a * x = a$
- Idempotente: $a \in A$ será idempotente $a * a = a$
- Cancelable: $a \in A$ es cancelable si $\forall y, z \in A$ $a * y = a * z \Rightarrow y = z$
  $y * a = z * a \Rightarrow y = z$

- $(A,*,\Delta)$ ea, Δ distribuye con respecto a $*$ si $\forall x,y,z \in A$ $\quad x\Delta(y*z) = (x\Delta y)*(x\Delta z)$
  $\quad (y*z)\Delta x = (y\Delta x)*(z\Delta x)$

Proposiciones:

- $(A,*)$ ea con $a \in A$ es cancelable si las funciones $I_a(x) = a*x$ y $D_a(x) = x*a$ son inyectivas
- $(A,*)$ posee un único elemento neutro
- $(A,*)$ tiene neutro e y $*$ es asociativa → tiene inversos únicas x^{-1}
  - → $x \in A$ tiene inverso, x^{-1} también, $(x^{-1})^{-1} = x$
  - → $x, y \in A$ poseen inverso, $x*y$ también, $(x*y)^{-1} = y^{-1} * x^{-1}$
  - → Si $x \in A$ posee inverso, x es cancelable

* Para $n \in \mathbb{N}$ y $\neq 0$ se define $\mathbb{Z}_n = \mathbb{Z}/\equiv_n$

$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ $\quad$ $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

$([a],[b]) \to [a+b]$ $\quad$ $([a],[b]) \to [a \cdot b]$

son LCI

Homomorfismos:

$(A,*)$ y (B,Δ) ea, una función $f: A \to B$ es homomorfismo de $(A,*)$ en (B,Δ) si

$$\forall x,y \in A,\ f(x*y) = f(x)\Delta f(y)$$

- Monomorfismo: f inyectiva
- Epimorfismo: f epiyectiva → Si $(A,*)$ es asociativa, (B,Δ) también
  - → Si $(A,*)$ es conmutativa, (B,Δ) también
  - → e neutro en $(A,*)$, $f(e)$ neutro en (B,Δ)
  - → $a \in A$ tiene inverso b para $(A,*)$, $f(a)$ tiene inverso $f(b)$ para (B,Δ)
- Isomorfismo: f biyectiva $\{ (A,*) \cong (B,\Delta) \to f^{-1}$ es isomorfismo de (B,Δ) en $(A,*)$
  - → es relación de equivalencia
- Endomorfismo $(A,*) = (B,\Delta)$
- Automorfismo $(A,*) = (B,\Delta)$ $\wedge$ f biyectiva

Proposiciones:

Sea f homomorfismo de $(A,*)$ en (B,Δ) con neutros e_A y e_B

1. ① $e_B \in f(A)$ entonces $e_B = f(e_A)$
   ② $e_B \in f(A)$ y $a \in A$ tiene inverso b para $(A,*)$ entonces $f(a)$ tiene inverso $f(b)$ para (B,Δ)
   ③ $g: B \to C$ homomorfismo de (B,Δ) en $(C,\cdot)$, entonces $g \circ f: A \to C$ es homo de $(A,*)$ en $(C,\cdot)$

Estructuras en conjuntos funciones

- $B^A = \{ f: A \to B, f$ función $\}$. Si $(B,*)$ es ea. $(B^A,*)$ es ea
- $f,g \in B^A$, se define $f*g$ función. $f(x)*g(x) \in B$, la función $f*g \in B^A$, por lo que $(B^A,*)$ es ea
- Si $(B,*)$ es asociativa o conmutativa, entonces $(B^A,*)$ también
- Si $(B,*)$ tiene neutro e, entonces $f \in B^A$ dado por $f(x) = e$ (con $x \in B$) es neutro de $(B^A,*)$

Estructura en productos cartesianos

$(A_1, *_1)$ y $(A_2, *_2)$ son ea, definimos $\otimes$ en $A_1 \times A_2$ como $(a_1, a_2) \otimes (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$

- $(A_i, *_i)$ es asociativa o conmutativa (para $i=1,2$) entonces $(A_1 \times A_2, \otimes)$ tb
- Si e_i es neutro para $(A_i, *_i)$ (para $i=1,2$) entonces (e_1, e_2) es neutro de $(A_1 \times A_2, \otimes)$
- Si a_i tiene inverso b_i en $(A_i, *_i)$ (para $i=1,2$) entonces (a_1, a_2) tiene inversos (b_1, b_2) en $(A_1 \times A_2, \otimes)$

Grupos: $(G, *)$ es grupo ssi $*$ es asociativo, admite neutro en G y todo elemento $x \in G$ posee inverso x^{-1}
si además es conmutativo, es grupo abeliano.

Si $(G, *)$ es grupo:

- Inverso de cada elemento es único
- $\forall x \in G, (x^{-1})^{-1} = x$
- $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1}$
- Todo elemento $x \in G$ es cancelable
- $\forall a, b \in G$, $a * x_1 = b$ tienen soluciones únicas $x_1 = a^{-1} * b$
  $x_2 * a = b$ $\quad x_2 = b * a^{-1}$
- Funciones $I_a(x) = a * x$, $D_a(x) = x * a$ son biyectivas (de G a G)
- Si (K, Δ) es ea y $f: G \to K$ es homomorfismo, $(f(G), \Delta)$ es grupo
  Sea $e_K = f(e_G)$ el neutro del grupo $(f(G), \Delta)$. Entonces f iny ssi $f^{-1}(\{e_K\}) = \{e_G\}$
- $(G, *)$ es grupo $\wedge$ $A \neq \emptyset$, (G^A, α) es grupo. Lo mismo con abeliano
- $(G_1, *_1)$ $\wedge$ $(G_2, *_2)$ son grupos, entonces $(G_1 \times G_2, \otimes)$ es grupo. " " " "

Subgrupos: $(G, *)$ grupo y $H \subseteq G$, H es subgrupo de G si $(H, *)$ es grupo

Proposiciones:

- neutros e inversos son iguales $\Rightarrow e = e_H \wedge x^{-1} = \tilde{x}$
- $(G, *)$ grupo y (K, Δ) ea y $f: G \to K$ homomorfismo, si H subgrupo de $(G, *)$, $f(H)$ es subgrupo de $(f(G), \Delta)$

Caracterización de subgrupos: Sea $H \neq \emptyset$, entonces
$(H, *)$ es subgrupo de $(G, *) \Leftrightarrow \forall x, y \in H, x * y^{-1} \in H$

Traslaciones de subgrupo (por izq): H subgrupo de $(G, *)$. Una traslación de H en $a \in G$ es el conjunto $a * H = \{a * h : h \in H\}$

Estructuras Algebraicas

Anillos: $(A,+,\cdot)$ es anillo si:

- $(A,+)$ es grupo abeliano (neutro ant 0)
- $\cdot$ asociativa
- $\exists!$ neutro $\in A\setminus\{0\}$ c/r a $\cdot$ (neutro ant 1)
- $\cdot$ distribuye c/r a $+$

* Si además, $\cdot$ es conmutativo, el anillo es conmutativo.

Propiedades: $(A,+,\cdot)$ anillo, $\forall x,y \in A$:

- $0\cdot x = x\cdot 0 = 0$
- $-(x\cdot y) = (-x)\cdot y = x\cdot(-y)$
- $(-x)\cdot(-y) = x\cdot y$
- $-x = (-1)\cdot x = x\cdot(-1)$

* **Convenciones**
  - → Inverso de $a\in A$ c/r a $+$: $-a$
  - → $a-b$ si $a,b\in A$: $a+(-b)$
  - → $x\in A$, inverso para $\cdot$: x^{-1}

Homomorfismo de anillos: $(A,+_A,\cdot_A)$ y $(B,+_B,\cdot_B)$ anillos. es una función $f:A\to B$ es homomorfismo si

$\forall x,y\in A,\ f(x+_A y) = f(x)+_B f(y);\ f(x\cdot_A y) = f(x)\cdot_B f(y);\ f(1_A) = 1_B$

Operaciones iteradas: $(A,+,\cdot)$ anillo, $a\in A$, $n\in\mathbb{N}$

- $a^0 = 1 \wedge a^{n+1} = a^n\cdot a$
- Si posee inverso $a^{-1} \Rightarrow a^{-n} = (a^{-1})^n$
- $0\cdot a = 0$; $(n+1)a = na + a \wedge (-n)\cdot a = n\cdot(-a)$

→ $\forall k,l\in\mathbb{Z}, \forall a,b\in A$; $k(a+b) = ka+kb$, $(k+l)a = ka+la$ y $(ka)(lb) = (kl)(ab)$

→ $\forall x\in A, \forall n\in\mathbb{N}$; $x^{n+1} - 1_A = (x-1)\sum_{k=0}^{n} x^k$

→ $\forall x,y\in A, \forall n\in\mathbb{N}$, anillo conmutativo; $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$

Divisores de cero: $(A,+,\cdot)$ anillo, $a\in A$ es div de cero si
- $a\neq 0$
- $\exists b\in A\setminus\{0\}, a\cdot b = 0 \vee b\cdot a = 0$

* a es cancelable en $(A,\cdot) \Leftrightarrow$ a no es div de cero

→ Si anillo no tiene divisores de cero, se le llama **Dominio de integridad**

Cuerpos: $(K,+,\cdot)$ es cuerpo si:
- $(K,+,\cdot)$ es anillo conmutativo
- $\forall x\in K\setminus\{0\}$, es invertible para $\cdot$

→ Equivalentemente:
- $(K,+)$ es grupo abeliano
- $(K\setminus\{0\},\cdot)$ es grupo abeliano
- $\cdot$ distribuye c/r a $+$

* **Proposiciones**
  - → $(K,+,\cdot)$ cuerpo, entonces K es dominio integridad
  - → Si $(A,+,\cdot)$ es dominio de integridad, con $|A|$ finito, entonces es cuerpo

Complejos

$\mathbb{C} = \{a+bi, a,b \in \mathbb{R}\} \supseteq \mathbb{R}$

- (a,b) dnt $a+bi$
- $(a,-b)$ dnt $a-bi$ / $a+(-b)i$
- $a \in \mathbb{R}$ represent $a+0i$
- $(0,b)$ dnt bi
- $(0,1)$ dnt i

Forma cartesiana: $z = a+bi$, $w = c+id$

- Parte real $Re(z)=a$ ∧ Parte imaginaria: $Im(z)=b$
- Suma: $z+w = (a+c)+i(b+d)$
- Multiplicación: $z \cdot w = (ac-bd)+i(ad+bc)$
  - $(\mathbb{C}, +, \cdot)$ es cuerpo → neutro aditivo $0+0i=0$ ∧ neutro multi.: $1+0i=1$
    → inverso aditivo $-a-bi$ ∧ inverso mult. $\frac{-a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$

Propiedades: $z, w \in \mathbb{C}, \alpha \in \mathbb{R}$

- $Re(z+w) = Re(z)+Re(w)$
- $Im(z+w) = Im(z)+Im(w)$

$Re: \mathbb{C} \to \mathbb{C}$ ∧ $Im: \mathbb{C} \to \mathbb{C}$ son homomorfismos

- $Re(\alpha z) = \alpha Re(z)$ ∧ $Im(\alpha z) = \alpha Im(z)$
- $z = w \Leftrightarrow Re(z) = Re(w)$ ∧ $Im(z) = Im(w)$

Modulo: Distancia de $z = a+bi$ al origen 0

$|z| = \sqrt{a^2+b^2}$

Conjugado: $a-bi$ es conjugado de $a+bi$

$\overline{a+bi} = a-bi$

Propiedades: $z \in \mathbb{C}$ con $z = a+bi$

- $|z| \geq 0 \to |z|=0 \Leftrightarrow z=0$
- $|z| \geq |a|$ ∧ $|z| \geq |b|$ $(|z| \geq |Re(z)|$ ∧ $|z| \geq |Im(z)|)$
- $|z \cdot w| = |z| \cdot |w|$, para $w \in \mathbb{C}$
- $|z^k| = |z|^k$
- $|z+w| \leq |z| + |w|$

Propiedades:

- $\overline{\overline{z}} = z$
- $z \in \mathbb{R} \Leftrightarrow \overline{z} = z$
- $\overline{z \pm w} = \overline{z} \pm \overline{w}$
- $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$
- $Re(\overline{z}) = Re(z)$ ∧ $Im(\overline{z}) = -Im(z)$
- $Re(z) = \frac{1}{2}(z+\overline{z})$ ∧ $Im(z) = \frac{1}{2i}(z-\overline{z})$
- $|\overline{z}| = z$
- $|z|^2 = z \cdot \overline{z}$
- $z^{-1} = \overline{z}/|z|^2$ ∧ $|\overline{z/w}| = \overline{z}/\overline{w}$

Argumento: Ángulo formado entre OX y segmento une z con Origen $Arg(z)$

Propiedades:

$z = w \Leftrightarrow |z| = |w|$ ∧ $arg(z) = arg(w)$

$arg(zw) = arg(z) + arg(w)$

$arg(z^k) = k\, arg(z)$

$arg(\overline{z}) = 2\pi - arg(z)$

Forma polar: $z = re^{i\,arg(z)}$; $e^{i\theta} = \cos\theta + i\,sen\theta$

- $z \cdot w = |z| \cdot |w| e^{i(arg(z)) + arg(w)}$
- $(e^{i\theta})^k = e^{i\theta k}$
- $\overline{z} = |z| e^{i(2\pi - arg(z))} = |z| e^{-i\,arg(z)}$
- $z^{-1} = \frac{1}{|z|} e^{-i\,arg(z)}$
- $e^{i\theta} = e^{-i\theta}$
- $e^{i\theta} \cdot e^{i\varphi} = e^{i(\theta+\varphi)}$
- $e^{i\theta} = e^{i(\theta+2k\pi)}$ $\forall k \in \mathbb{Z}$

Operaciones en forma polar: $z = \rho e^{i\theta}$, $z' = \rho' e^{i\theta'}$

- $|z| = \rho$
- $|\bar{z}| = \rho e^{-i\theta}$
- $z^{-1} = \frac{1}{z} = \frac{1}{\rho} e^{i\theta} = \frac{\bar{z}}{|z|^2}$
- $z \cdot z' = \rho \cdot \rho' e^{(\theta+\theta')}$

Raíces de un complejo: $w \in \mathbb{C} \setminus \{0\}$ y $n \geq 2$. z es raíz n-ésima de w si $z^n = w$

- Si $w = 1$, las soluciones se llaman raíces n-ésimas de la unidad
- Sea $w = r_0 e^{i\theta_0} \in \mathbb{C} \setminus \{0\}$. $z^n = w$ tiene n soluciones, $(w_0 \dots w_{n-1}) \rightarrow z_k = \sqrt[n]{r_0} \cdot e^{\frac{i\theta_0}{n}} \cdot w_k$, $k \in \{0, \dots n-1\}$
- $\sum_{k=0}^{n-1} w_k = 0$

Polinomios

$(\mathbb{K},+,\cdot)$ cuerpo en $\mathbb{R}$ o $\mathbb{C}$

Definiciones básicas:

- Un polinomio es una función de $\mathbb{K}$ en $\mathbb{K}$: $P:\mathbb{K}\to\mathbb{K}$, $x\to P(x)=\sum_{k=0}^{n} p_k x^k$
- $P\in\mathbb{K}^{\mathbb{K}}$ se dice polinomio a coeficientes en $\mathbb{K}$ si $\exists d\in\mathbb{N}$, $p_1\dots p_d\in\mathbb{K}$ tq $P(x)=p_0+p_1x+\dots p_dx^d$
- Conjunto de polinomios a coeficientes en $\mathbb{K}$ en la variable x se denota $\mathbb{K}[x]$
- P es polinomio constante si $\exists r\in\mathbb{K}$ tq $P(x)=r$, $\forall x\in\mathbb{K}$
- P polinomio nulo: $P\equiv 0$

Igualdad de polinomios: $P=Q$:

$$P(x)=Q(x)\Leftrightarrow (n=m \text{ y } \forall k\in[0\dots n], p_k=q_k)$$

Grado del polinomio:

Exponente más alto con coeficiente no nulo. $P(x)=p_0+p_1x+\dots p_dx^d$, $gr(P)=d$, si $p_d\neq 0$

→ Si $P=Q$, $gr(P)=gr(Q)$

→ $P\equiv 0$ ⇒ grado $(P)=-\infty$, se tiene $\begin{cases}-\infty+n=n+(-\infty)=-\infty\\ n>-\infty\\ (-\infty)+(\infty)=-\infty\end{cases}$

→ Polinomio constante $\Leftrightarrow gr(P)\leq 0$

Polinomio mónico: $n=gr(P)$ se tiene que $p_n=1$ (el coef de la potencia de x mas grande)

Suma: $(P+Q)(x)=(p_0+q_0)+(p_1+q_1)x+\dots=\sum_{k=0}^{\max\{gr(P),gr(Q)\}}(p_k+Q_k)x^k$

→ $gr(P+Q)\leq \max\{gr(P),gr(Q)\}$

→ $P+Q\in\mathbb{K}[x]$

Multiplicación: $(P\cdot Q)(x)=\sum_{k=0}^{n+m}\left(\sum_{i=0}^{k}p_i\,q_{k-i}\right)x^k=\sum_{k=0}^{n+m}\left(\sum_{i=0}^{k}p_{k-i}\,q_i\right)x^k$

→ $gr(P\cdot Q)=gr(P)+gr(Q)$

→ $P\cdot Q\in\mathbb{K}[x]$

¡OJO! $(\mathbb{K}[x],+,\cdot)$ es un anillo conmutativo, sin divisores de 0 (es dominio de la integridad)

↳ pero NO es cuerpo, únicos polinomios con inversos los de grado 0 (constantes no nulos)

División: $P, D \in \mathbb{K}[x]$, $D \neq 0$:

$\exists! Q, R$ tq $P = Q \cdot D + R \rightarrow gr(R) < gr(D)$

- división con resto de P por D
- polinomio Q se llame cociente
- " R se llame resto

→ Cuando $R=0$ diremos que D divide a P, denotado $D \mid P$

→ $P \in \mathbb{K}[x]$ y $c \in \mathbb{K}$, el resto de dividir P por $x-c$ es $P(c)$

♥ Se divide $P(x) : Q(x)$ así:

"¿Por qué multiplicar el término de mayor exponente de $Q(x)$, para tener el término de mayor exponente de $P(x)$? Luego, multiplicar ese número por $Q(x)$ y restarle el resultado a $P(x)$. Se repite el procedimiento las veces que se pueda."

Raíz: $\alpha \in \mathbb{K}$ se dice raíz de $P \in \mathbb{K}[x]$ si $P(\alpha) = 0$

- $\alpha \in \mathbb{K}$ es raíz de $P \Leftrightarrow (x-\alpha) P$
- Decimos que $\alpha \in \mathbb{K}$ raíz de P es multiplicidad de m si: $(x-\alpha)^m \mid P$, $(x-\alpha)^m \nmid P$
- $P, Q \in \mathbb{K}[x]$ se tiene → $Q \mid P$ y $\alpha \in \mathbb{K}$ es raíz de P, pero no de $Q \Leftrightarrow \exists d \in \mathbb{K}[x], P(x) = Q(x) \cdot D(x)$ y raíz de D
  - → $\alpha_1, \dots \alpha_k$ son raíces distintas de $P \Rightarrow (x-\alpha_1) \dots (x-\alpha_k) \mid P$
  - → grado $(P) = n \geq 0 \Rightarrow P$ posee a lo más n raíces distintas
  - → grado (P), grado $(Q) \leq n$, se tiene $\exists a_1, \dots a_{n+1} \in \mathbb{K}$ distintos entre sí y tq $P(a_i) = Q(a_i)$, $\forall i \in 1, \dots n+1 \Rightarrow P = Q$

Teorema Fundamental del Algebra

Si $P \in \mathbb{C}[x]$ es tq grado $(P) \geq 1$, entonces $\exists \alpha \in \mathbb{C}$ raíz de P

Facto en $\mathbb{C}$:

- $P \in \mathbb{C}[x]$ grado $(P) = n \geq 1 \Rightarrow \exists \lambda \in \mathbb{C}, \exists a_1, \dots a_n \in \mathbb{C}$ tq, $P(x) = \lambda (x-a_1)(x-a_2) \dots (x-a_n)$ donde $\lambda = P_n$

→ Sea $P \in \mathbb{C}[x]$ tq todos sus coeficientes están en $\mathbb{R}$. Si $z \in \mathbb{C}$ es una raíz de P, $\bar{z}$ también es raíz de P

Facto en $\mathbb{R}$

- $P \in \mathbb{R}[x]$, grado $(P) = n \geq 1$ entonces $P(x) = \lambda (x-\beta_1)(x-\beta_2) \dots (x-\beta_k)(x^2+p_1 x+q_1) \dots (x^2+p_m x+q_m)$, donde
  - donde $\beta_1, \dots \beta_n \in \mathbb{R}$, $p_1 \dots p_m \in \mathbb{R}$, $n = k+2$, $\lambda = P_0$

Criterio de raíces racionales:

- Sea P un polinomio a coeficiente enteros grado $(P) = d$, $P_0 \neq 0$
  - → $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ son coprimos y $\frac{a}{b}$ raíz de $P \Rightarrow a \mid P_0$ y $b \mid P_d$