MA1101-2 Introducción al Álgebra
Profesor : Mauricio Telias H.
Auxiliar : Arturo Merino F.

"Resumen" Examen

- Una proposición lógica es un enunciado que toma un valor de verdad V o F.
- Los conectivos lógicos son operaciones entre proposiciones y permiten construir nuevas proposiciones a partir de proposiciones ya conocidas.
- Las tablas de verdad de las proposiciones básicas son:

p	$\overline{p}$
V	F
F	V

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

- Los conectivos $\vee$ y $\wedge$ son asociativos, conmutativos y distribuyen uno con respecto a otro.
- Otras proposiciones conocidas son:
  1. $(p \implies q) \equiv (\overline{p} \vee q)$
  2. $(p \iff q) \equiv [(p \implies q) \wedge (q \implies p)]$
  3. $(p \veebar q) \equiv \overline{(p \iff q)}$
- Se dirá que una proposición es una tautología si su valor de verdad es siempre V, en cambio si es siempre F diremos que es una contradicción.
- Algunas tautologías útiles son:
  1. $\overline{(p \vee q)} \iff (\overline{p} \wedge \overline{q})$
  2. $\overline{(p \wedge q)} \iff (\overline{p} \vee \overline{q})$
  3. $(p \implies q) \iff (\overline{q} \implies \overline{p})$
  4. $[(p \implies q) \wedge (q \implies r)] \implies (p \implies r)$
- Una función proposicional es una expresión $p(x)$, tal que al reemplazar x en la función esta se transforma en una propocisión $p(x)$.
- Un cuantificador nos proporciona información sobre los objetos a evaluar en la función proposicional. Los clásicos cuantificadores son :
  1. Cuantificador Universal ($\forall$), se lee "para todo".
  2. Cuantificador Existencial ($\exists$), se lee "existe".
  3. Cuantificador de Existencia y Unicidad ($\exists!$), se lee "existe un único".
- Las negaciones clásicas con cuantificadores son:
  1. $\overline{[\forall x, p(x)]} \iff [\exists x, \overline{p(x)}]$
  2. $\overline{[\exists x, p(x)]} \iff [\forall x, \overline{p(x)}]$
  3. $\overline{[\exists! x, p(x)]} \iff$ $[\forall x, p(x)] \vee [\exists x, y, p(x) \wedge p(y) \wedge x \neq y]$
- La proposición $x \in A$ se lee x pertenece al conjunto A.
- A partir de un conjunto universo $\mathcal{U}$ y una proposición lógica $p(x)$, podemos definir el conjunto A de quienes satisfacen la proposición lógica como:

$$(\forall x)[(x \in A) \iff (x \in \mathcal{U} \wedge p(x))]$$

  O de manera abreviada:

$$A = \{x \in \mathcal{U} : p(x)\}$$

- Se define el conjunto vacío como:

$$\emptyset = \{x \in \mathcal{U} : x \neq x\} = \{\}$$

- Diremos que A es subconjunto de B si:

$$(A \subseteq B) \iff [(x \in A) \implies (x \in B)]$$

  De similar manera:

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

- Sean A y B dos subconjuntos de $\mathcal{U}$. Definimos las siguientes operaciones entre conjuntos :
  1. $A \cup B = \{x : x \in A \vee x \in B\}$
  2. $A \cap B = \{x : x \in A \wedge x \in B\}$
  3. $A^c = \{x : x \notin A\}$
  4. $A \setminus B = A \cap B^c$
  5. $A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
- La unión e intersección satisfacen las leyes de conmutatividad, asociatividad, distributividad y de Morgan.
- Definimos el conjunto de las partes de un conjunto A como la familia de todos los subconjuntos de A.

$$\mathcal{P}(A) = 2^A = \{X \subseteq A\}$$

- Sea $a \in A$ y $b \in B$, definimos el par ordenado (a, b) como:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

- La igualdad de pares ordenados es por coordenadas, es decir:

$$(a, b) = (c, d) \iff (a = c \wedge b = d)$$

- Definimos el producto entre A y B como:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

- Llamaremos función de A en B a cualquier $f \subseteq A \times B$ tal que:
$$(\forall a \in A)(\exists! b \in B) \quad (a,b) \in f$$
Si f es una función de A en B lo anotaremos como $f : A \to B$, de igual manera si $(a,b) \in f$ lo anotaremos $f(a) = b$.

- Si $f : A \to B$ al conjunto A lo llamaremos dominio de f y a B lo llamaremos el recorrido de f.

- Si $f : A \to B$ y $g : C \to D$ entonces:
$$f = g \iff \left[\begin{array}{c} \mathrm{Dom}(f) = \mathrm{Dom}(g) \\ \wedge \\ \mathrm{Rec}(f) = \mathrm{Rec}(g) \\ \wedge \\ (\forall x \in \mathrm{Dom}(f))(f(x) = g(x)) \end{array}\right]$$

- Sea $f : A \to B$. Diremos que f es inyectiva si $\forall x, y$ verifica:
$$x \neq y \implies f(x) \neq f(y)$$
O de manera equivalente:
$$f(x) = f(y) \implies x = y$$

- Sea $f : A \to B$ diremos que f es sobreyectiva (o epiyectiva) si verifica:
$$[\forall y \in B][\exists x \in A][y = f(x)]$$

- Diremos que una función es biyectiva si es sobreyectiva e inyectiva.

- Sea f biyectiva. Definimos f^{-1} como:
$$[\forall x \in A][\forall y \in B][f(x) = y \iff f^{-1}(y) = x]$$

- Sea $f : A \to B$ y $X \subseteq A$, definimos:
$$f(X) = \{b \in B : \exists x \in X, f(x) = b\}$$

- Sea $f : A \to B$ y $X \subseteq B$, definimos:
$$f^{-1}(X) = \{a \in A : f(a) \in X\}$$

- Sea $f : A \to B$ y $g : B \to C$ definimos la función composición $(g \circ f) : A \to C$ como:
$$(g \circ f)(a) = g(f(a))$$

- Sea $f : A \to B$, $g : B \to C$ y $h : C \to D$, entonces:
  1. $h \circ (g \circ f) = (h \circ g) \circ f$
  2. $I_B \circ f = f \circ I_A = f$, donde I_X es la función identidad del conjunto X.
  3. Si f es biyectiva, entonces $f \circ f^{-1} = I_B$ y $f^{-1} \circ f = I_A$.

- Sea $f : A \to B$ y $g : B \to C$, entonces:
  1. Si f y g son inyectivas, entonces $(g \circ f)$ es inyectiva.
  2. Si f y g son sobreyectivas, entonces $(g \circ f)$ es sobreyectiva.
  3. Si f y g son biyectiva, entonces $(g \circ f)$ es biyectiva.
  4. Si $(g \circ f)$ es inyectiva, entonces f es inyectiva.
  5. Si $(g \circ f)$ es sobreyectiva, entonces g es sobreyectiva.

- Sea $f : A \to B$ biyectiva y sea $g : B \to A$
  1. Si $g \circ f = I_A$, entonces $g = f^{-1}$
  2. Si $f \circ g = I_B$, entonces $g = f^{-1}$.

- Sean $f : A \to B$ y $g : B \to A$ tales que:
$$g \circ f = I_A \qquad f \circ g = I_B$$
Entonces f y g son biyectivas y $f^{-1} = g$.

- Sea $f : A \to B$, $g : B \to A$ biyectivas, entonces:
$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

- Dados dos conjuntos no-vacíos A y B, diremos que $\mathcal{R}$ es una relación en $A \times B$ si $\mathcal{R} \subseteq A \times B$. Denotaremos $a\mathcal{R}b$ cuando $(a,b) \in \mathcal{R}$. Si $A = B$ simplemente diremos que $\mathcal{R}$ es una relación en A.

- Sea $\mathcal{R}$ un relación en A, diremos que $\mathcal{R}$ es:
  1. **Refleja** si y sólo si:
  $$(\forall x \in A)(x\mathcal{R}x)$$
  2. **Simétrica** si y sólo si:
  $$(\forall x, y \in A)(x\mathcal{R}y \implies y\mathcal{R}x)$$
  3. **Antisimétrica** si y sólo si:
  $$(\forall x, y \in A)([x\mathcal{R}y \wedge y\mathcal{R}x] \implies x = y)$$
  4. **Transitiva** si y sólo si:
  $$(\forall x, y, z \in A)([x\mathcal{R}y \wedge y\mathcal{R}z] \implies x\mathcal{R}z)$$

- Sea $\mathcal{R}$ una relación en A, diremos que $\mathcal{R}$ es un orden en A si es una relación refleja, antisimétrica y transtiva. Si además $\mathcal{R}$ verifica la propiedad:
$$(\forall a, b \in A)(a\mathcal{R}b \vee b\mathcal{R}a)$$
lo llamaremos orden total.

- Sea $\mathcal{R}$ una relación en A, diremos que $\mathcal{R}$ es una relación de equivalencia si es refleja, simétrica y transitiva.
- Sea $\mathcal{R}$ una relación de equivalencia en A. Para todo $a \in A$ definimos la clase de equivalencia de a como:

$$[a]_{\mathcal{R}} = \{x \in A : a\mathcal{R}x\}$$

Y construiremos el conjunto cuociente como:

$$A/\mathcal{R} = \{X \subseteq A : \exists x \in A, X = [x]_{\mathcal{R}}\}$$

Es decir el conjunto de las clases de equivalencias.

- Sean $x, y \in A$ y $\mathcal{R}$ una relación de equivalencia en A, entonces:
  1. $[x]_{\mathcal{R}} \neq \emptyset$.
  2. $x\mathcal{R}y \iff [x]_{\mathcal{R}} = [y]_{\mathcal{R}}$.
  3. $\overline{(x\mathcal{R}y)} \iff [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \emptyset$
- Sea P una familia de conjuntos. Diremos que P es una partición de X si satisface:
  - $\emptyset \notin P$.
  - $\bigcup_{A \in P} A = \{x : (\exists A \in P)[x \in A]\} = X$.
  - Si $A, B \in P$ y $A \neq B$, entonces $A \cap B = \emptyset$.
- Sea P una partición de X. La siguiente es una relación de equivalencia sobre X:

$$x \sim y \iff \exists A \in P \text{ tal que } x, y \in A$$

- Si $\mathcal{R}$ es una relación de equivalencia en A, entonces $A/\mathcal{R}$ es una partición de A.
- Sean $a, b \in \mathbb{Z}$. Existe un único par $q, r \in \mathbb{Z}$ tal que:

$$a = qb + r \quad \wedge \quad 0 \leq r < |b|$$

- Sea $p \in \mathbb{N}$, $p \geq 2$. Definimos la relación de equivalencia módulo p como:

$$x \equiv_p y \iff [\exists k \in \mathbb{Z}][(x - y) = kp]$$

Esta relación es de equivalencia y además:

$$\mathbb{Z}/\equiv_p = \{[0]_{\equiv_p}, [1]_{\equiv_p}, \ldots, [p-1]_{\equiv_p}\}$$

A este último conjunto se le suele denotar por Z_p.

- Consideremos una proposición:

$$(\forall n \in \mathbb{N}, n \geq n_0)p(n)$$

Entonces esto es equivalente a:

$$p(n_0) \wedge [(\forall n \geq n_0)p(n) \implies p(n+1)]$$

y también es equivalente a:

$$p(n_0) \wedge [(\forall n \geq n_0)(p(n_0) \wedge \cdots \wedge p(n-1)) \implies p(n)]$$

- Sea $a_0, a_1, \ldots, a_n$ una secuencia de números reales, definimos su suma desde m hasta M como:

$$\sum_{k=m}^{M} a_k = a_m + a_{m+1} + \cdots + a_{M-1} + a_M$$

- Las sumas verifican las siguientes propiedades:
  1. $\sum_{k=m}^{M} 1 = M - m + 1$
  2. $\sum_{k=m}^{M} \lambda a_k = \lambda \sum_{k=m}^{M} a_k$
  3. $\sum_{k=m}^{M} (a_k + b_k) = \sum_{k=m}^{M} a_k + \sum_{k=m}^{M} b_k$
  4. $\sum_{k=m}^{M} a_k = \sum_{k=m+s}^{M+s} a_{k-s}$
  5. $\sum_{k=m}^{M} a_k = \sum_{k=m}^{l} a_k + \sum_{k=l+1}^{M} a_k$
  6. $\sum_{k=m}^{M} a_k - a_{k+1} = a_m - a_{M+1}$
- Suma aritmética:

$$\sum_{k=0}^{n} (A + kd) = A(n+1) + d\frac{n(n+1)}{2}$$

- Suma geométrica: (si $r \neq 1$)

$$\sum_{k=0}^{n} r^k = \frac{r^{n+1} - 1}{r - 1} \qquad \sum_{k=1}^{n} r^k = \frac{r^{n+1} - r}{r - 1}$$

- Suma de cuadrados:

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

- Suma de cubos:

$$\sum_{k=0}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2 = \left(\sum_{k=0}^{n} k\right)^2$$

- Definimos el factorial de n por la siguiente recurrencia:

$$n! = n(n-1)! \quad 0! = 1$$

De manera más informal:

$$n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$$

También puede ser definido como las manera de permutar un conjunto de n elementos.

- Definimos el número binomial $\binom{n}{k}$ como el número de subconjuntos de tamaño k que posee un conjunto de tamaño n. Si $k \leq n$, entonces:

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

- Identidad de Pascal:

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

- Teorema del Binomio: Sean $x, y \in \mathbb{R}$, $n \in \mathbb{N}$. Entonces:

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

- Si tenemos una suma doble cuyos limites inferiores y superiores no dependen de los indices. Entonces:

$$\sum_{k=0}^{n}\sum_{j=0}^{m} a_{kj} = \sum_{j=0}^{m}\sum_{k=0}^{n} a_{kj}$$

- Desde ahora consideraremos A y B conjuntos.
- Diremos que A y B tienen el mismo cardinal si existe $f : A \to B$ biyectiva. En tal caso diremos que $|A| = |B|$.
- Si existe $f : A \to B$ inyectiva, diremos que $|A| \leq |B|$.
- Si existe $f : A \to B$ inyectiva, pero no existe $g : A \to B$ biyectiva, diremos que $|A| < |B|$.
- Tenemos las siguientes propiedades del cardinal:
  1. $|A| \leq |A|$.
  2. Si $A \subseteq B$, entonces $|A| \leq |B|$.
  3. Si $|A| \leq |B|$ y $|B| \leq |C|$, entonces $|A| \leq |C|$.
- **Teo. de Cantor-Bernstein-Schröder:** Si $|A| \leq |B|$ y $|B| \leq |A|$, entonces $|A| = |B|$.
- Sea $n \in \mathbb{N}$ Definimos:

$$\mathbb{N}_n = \{x \in \mathbb{N} : 1 \leq x \leq n\}$$

  Se tienen las siguiente propiedades sobre $\mathbb{N}_n$
  1. $|\mathbb{N}_k| < |\mathbb{N}_{k+1}|$
  2. $m \leq n \iff |\mathbb{N}_m| \leq |\mathbb{N}_n|$

  Esto justifica escribir $|\mathbb{N}_k| = k$.
- Diremos que un conjunto A es finito si y sólo si:

$$\exists k \in \mathbb{N} \text{ tal que } |A| = |\mathbb{N}_k|$$

  En caso contrario diremos que A es infinito.
- $\mathbb{N}$ es infinito y si un conjunto A es tal que $|A| = |\mathbb{N}|$ lo llamaremos numerable, si se verifica $|A| \leq |\mathbb{N}|$ diremos que es a lo más numerable.
- $\mathbb{Z}$ y $\mathbb{Q}$ son numerables.
- A es un conjunto infinito si y sólo si $|\mathbb{N}| \leq |A|$.
- Sea A un conjunto infinito tal que $|A| \leq |\mathbb{N}|$. Entonces $|A| = |\mathbb{N}|$.
- Sea $(A_n)_{n\in\mathbb{N}} = A_0, A_1, A_2, \ldots, A_n, \ldots$ una colección numerable de conjuntos definimos su unión como:

$$\bigcup_{k\in\mathbb{N}} A_k = \{x : (\exists k \in \mathbb{N}), x \in A_k\}$$

- Sean A, B conjuntos numerables, entonces $A \times B$ es numerable.
- Sean $(A_k)_{k=0}^{n} = A_0, A_1, \ldots, A_n$ conjuntos numerables. Entonces:

$$\prod_{k=0}^{n} A_k = A_0 \times \ldots \times A_n \text{ es numerable.}$$

- Sea $(A_n)_{n\in\mathbb{N}}$ colección numerable de conjuntos numerables. Entonces:

$$\bigcup_{k\in\mathbb{N}} A_k \text{ es numerable.}$$

- Sea $(A_n)_{n\in\mathbb{N}}$ colección a lo más numerable de conjuntos a lo más numerables. Entonces:

$$\bigcup_{k\in\mathbb{N}} A_k \text{ es a lo más numerable.}$$

- Sea A un conjunto infinito, y sea $x \in A$. Entonces $|A| = |A \setminus \{x\}|$.
- Un conjunto A se dirá *no numerable* si $|\mathbb{N}| < |A|$.
- $\mathbb{R}$ es no numerable.
- Dado A un conjunto no vacío. Diremos que $*$ es una *ley de composición interna* (u operación binaria) si $*$ es una función

$$\begin{array}{rcl} * : A \times A & \to & A \\ (x, y) & \mapsto & x * y \end{array}$$

- Si $*$ es una l.c.i. definida en el conjunto A, al par $(A, *)$ le llamaremos estructura algebraica. Si el conjunto A tiene definida una segunda operación $\triangle$, denotaremos por $(A, *, \triangle)$ a la estructura algebraica que considera ambas l.c.i. en A.

- Sea $(A, *)$ una estructura algebraica.
  1. Diremos que es **asociativa** si
  $$\forall x, y, z \in A \quad (x * y) * z = x * (y * z)$$
  2. Sea $e \in A$. Diremos que e es un **neutro** para $*$ si
  $$\forall x \in A \quad e * x = x * e = x$$
  3. Si $e \in A$ es el neutro para $*$, diremos que $x \in A$ es **invertible** si:
  $$\exists y \in A \quad y * x = x * y = x$$
  4. Sea $a \in A$. Diremos que a es **absorbente** si:
  $$\forall x \in A \quad x * a = a * x = a$$
  5. Sea $a \in A$. Diremos que a es **idempotente** si:
  $$a * a = a$$
- Sea $(A, *, \triangle)$ una estructura algebraica. Diremos que $\triangle$ **distribuye** con respecto a $*$ si
$$\forall x, y, z \in A \quad x \triangle (y * z) = (x \triangle y) * (x \triangle z)$$
$$\forall x, y, z \in A \quad (y * z) \triangle x = (y \triangle x) * (z \triangle x)$$
- Una estructura algebraica $(A, *)$ tiene a lo más un elemento neutro.
- En una estructura algebraica $(A, *)$ con neutro y asociativa los inversos son únicos. En este caso si $x \in A$ posee inverso, lo podemos denotar sin ambigüedad como x^{-1}.
- Sea $(A, *)$ una estructura con neutro y asociativa.
  1. Si $x \in A$ es invertible, entonces $(x^{-1})^{-1} = x$.
  2. Si $x, y \in A$ son invertibles, entonces $(x * y)^{-1} = y^{-1} * x^{-1}$.
  3. Si $x \in A$ es invertible, entonces es cancelable. Es decir $\forall y, z \in A$
  $$x * y = x * z \implies y = z$$
  $$y * x = z * x \implies y = z$$
- Si $(G, *)$ es una estructura algebraica asociativa, con neutro y tal que todo elemento es invertible, entonces diremos que $(G, *)$ es un grupo. Si ademas la operación $*$ es conmutativa, diremos que es un grupo abeliano.
- Sea $(G, *)$ un grupo, entonces:
  1. El inverso de cada elemento es único.
  2. $(\forall x \in G)$, $(x^{-1})^{-1} = x$.
  3. $(\forall x, y \in G)$, $(x * y)^{-1} = y^{-1} * x^{-1}$.
  4. Todo elemento $x \in G$ es cancelable.
  5. Para todo $a, b \in G$, las ecuaciones:
  $$a * x_1 = b$$
  $$x_2 * a = b$$
  tienen solución única. Ellas son $x_1 = a^{-1} * b$ y $x_2 = b * a^{-1}$.
  6. El único elemento idempotente de G es su neutro.
- Sea $(G, *)$ un grupo, y sea $H \subseteq G$. Diremos que H es subgrupo de G si $(H, *)$ también es grupo.
- **Caracterización de Subgrupo:** Sea $H \neq \emptyset$, entonces:
$$(H, *) \text{ subgrupo de } (G, *) \Leftrightarrow (\forall x, y \in H)\, x * y^{-1} \in H$$
- $(\mathbf{Z}_n, +_n)$ es un grupo abeliano.
- **Teorema de Lagrange:** Sea $(G, *)$ un grupo finito y $(H, *)$ un subgrupo de $(G, *)$. Entonces $|H|$ divide a $|G|$.
- Sea $(G, *)$ un grupo. A $|G|$ le llamaremos el orden del grupo.
- Sean $(A, *)$ y $(B, \triangle)$ dos estructuras. Diremos que $f : A \to B$ es un morfismo si $\forall x, y \in A$ verifica:
$$f(x * y) = f(x) \triangle f(y)$$
- Si f es un morfismo biyectivo, le llamaremos isomorfismo.
- Sean $(A, *)$ y $(B, \triangle)$ dos estructuras tales que existe $f : A \to B$ isomorfismo, diremos entonces que $(A, *)$ es isomorfo a $(B, \triangle)$ y lo denotaremos por $(A, *) \cong (B, \triangle)$.
- $(\mathbb{R}^+, \cdot) \cong (\mathbb{R}, +)$.
- Sean $(A, *)$ y $(B, \triangle)$ y $f : A \to B$ un morfismo sobreyectivo (a veces llamado *epimorfismo*), entonces:
  1. Si $*$ es asociativa, entonces $\triangle$ también.
  2. Si $*$ es conmutativa, entonces $\triangle$ también.
  3. Si $*$ tiene neutro, entonces $\triangle$ también. Más aun si e es el neutro para $*$, entonces $f(e)$ es el neutro para $\triangle$.
  4. Si $(A, *)$ es asociativa con neutro y $a \in A$ es invertible, entonces $f(a)$ es invertible y $f(a)^{-1} = f(a^{-1})$.
- Si $f : G \to H$ es un morfismo y tanto $(G, *)$ como $(H, *)$ son grupos, entonces:

1. $f(e_G) = e_H$.
2. $f(a^{-1}) = f(a)^{-1}$

- La composición de morfismos es morfismo.
- Si $f : A \to B$ es un isomorfismo, entonces $f^{-1} : B \to A$ también.
- $\cong$ es una relación de equivalencia.
- A una estructura $(A, +, \cdot)$ le llamaremos anillo si satisface:
  1. $(A, +)$ es un grupo abeliano.
  2. $\cdot$ es asociativa.
  3. $\cdot$ distribuye con respecto a $+$.
- Sea $(A, +, \cdot)$ un anillo, tenemos la siguiente notación:
  1. Al neutro de $(A, +)$ se le suele denotar por 0, mientras que el inverso de x para $+$ se denota por $-x$.
  2. Si $(A, \cdot)$ tiene neutro a dicho neutro le llamaremos 1, más aún diremos que $(A, +, \cdot)$ es un anillo con unidad. Si $x \in A$ posee inverso para $\cdot$ lo denotaremos por x^{-1}.
  3. Si $\cdot$ es conmutativa, diremos que $(A, +, \cdot)$ es un anillo conmutativo.
- $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad.
- Si $(A, +, \cdot)$ es un anillo con unidad y $|A| \geq 2$, entonces $0 \neq 1$.
- Sea $(A, +, \cdot)$ un anillo, entonces:
  1. 0 es absorbente.
  2. $(\forall x, y \in A)$, $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$.
  3. $(\forall x, y \in A)$, $(-x) \cdot (-y) = x \cdot y$.
  4. Si A tiene unidad:

$$(\forall x \in A) \ -x = (-1) \cdot x = x \cdot (-1)$$

- $(\mathbf{Z}_n, +_n, \cdot_n)$ es un anillo conmutativo con unidad.
- Sea $(A, +, \cdot)$ un anillo. Si $x, y \in A \setminus \{0\}$ son tales que $x \cdot y = 0$, diremos que x e y son divisores del 0.
- Sea $(A, +, \cdot)$ un anillo y $a \in A \setminus \{0\}$, luego:

$$a \text{ es divisor del } 0 \iff a \text{ no es cancelable}$$

- Sea $(\mathbb{K}, +, \cdot)$ un anillo conmutativo con unidad tal que todo $x \in \mathbb{K} \setminus \{0\}$ es invertible, diremos que $(\mathbb{K}, +, \cdot)$ es un cuerpo.
- De manera equivalente $(\mathbb{K}+, \cdot)$ es un cuerpo si y sólo si:
  1. $(\mathbb{K}, +)$ es un grupo abeliano.
  2. $(\mathbb{K} \setminus \{0\}, \cdot)$ es un grupo abeliano.
  3. $\cdot$ distribuye con respecto a $+$.
- $(\mathbb{R}, +, \cdot)$ y $(\mathbb{Q}, +, \cdot)$ son cuerpos.
- Un cuerpo no tiene divisores del 0.
- Sea $(A, +, \cdot)$ un anillo conmutativo con unidad tal que $|A|$ es finito. Entonces $(A, +, \cdot)$ no tiene divisores del cero si y sólo si $(A, +, \cdot)$ es un cuerpo.
- $(\mathbf{Z}_n, +, \cdot)$ es un cuerpo $\iff$ n es un primo.
- Sea $\mathbb{C} = \mathbb{R}^2$ dotado de las siguientes operaciones:

$$\begin{aligned} z + w &= (z_1 + w_1, z_2 + w_2) \\ z \cdot w &= (z_1 w_1 - z_2 w_2, z_1 w_2 + w_1 z_2) \end{aligned}$$

- $(\mathbb{C}, +, \cdot)$ es un cuerpo.
- Sea $R = \{(z_1, 0) \in \mathbb{C} : z_1 \in \mathbb{R}\} \subseteq \mathbb{C}$, entonces $(R, +, \cdot) \cong (\mathbb{R}, +, \cdot)$.
- Usualmente anotaremos los $(a, b) \in \mathbb{C}$ como $a + bi$. Donde además $i^2 = -1$.
- Sea $z = a + bi \in \mathbb{C}$. Definimos la parte real y la parte imaginaria respectivamente como:

$$\mathbb{R}\mathrm{e}(z) = a \qquad \mathbb{I}\mathrm{m}(z) = b$$

- Sean $z, z_1, z_2 \in \mathbb{C}$ y $\lambda \in \mathbb{R}$, entonces:
  1. $\mathbb{R}\mathrm{e}(z_1 + z_2) = \mathbb{R}\mathrm{e}(z_1) + \mathbb{R}\mathrm{e}(z_2)$.
  2. $\mathbb{I}\mathrm{m}(z_1 + z_2) = \mathbb{I}\mathrm{m}(z_1) + \mathbb{I}\mathrm{m}(z_2)$.
  3. $\mathbb{R}\mathrm{e}(\lambda z) = \lambda \mathbb{R}\mathrm{e}(z)$.
  4. $\mathbb{I}\mathrm{m}(\lambda z) = \lambda \mathbb{I}\mathrm{m}(z)$.
  5. $z_1 = z_2 \Leftrightarrow [\mathbb{R}\mathrm{e}(z_1) = \mathbb{R}\mathrm{e}(z_2) \ \wedge \ \mathbb{I}\mathrm{m}(z_1) = \mathbb{I}\mathrm{m}(z_2)]$
- Sea $z = a + bi \in \mathbb{C}$. Definimos el conjugado de z como:

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

- Sean $z, w \in \mathbb{C}$. Entonces:
  1. $\overline{z + w} = \overline{z} + \overline{w}$ y $\overline{z - w} = \overline{z} - \overline{w}$.
  2. $\overline{zw} = \overline{z} \cdot \overline{w}$. Si $w \neq 0$ $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.
  3. Si $\lambda \in \mathbb{R}$, entonces $\overline{\lambda z} = \lambda \overline{z}$.
  4. $\overline{\overline{z}} = z$.
  5. $\mathbb{R}\mathrm{e}(z) = \mathbb{R}\mathrm{e}(\overline{z})$ y $\mathbb{I}\mathrm{m}(z) = -\mathbb{I}\mathrm{m}(\overline{z})$.
  6. $\mathbb{R}\mathrm{e}(z) = \frac{1}{2}(z + \overline{z})$ y $\mathbb{I}\mathrm{m}(z) = \frac{1}{2i}(z - \overline{z})$
  7. $z \in \mathbb{R} \iff z = \overline{z}$.

- Sea $z = a + bi$. Definimos el módulo como:

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

- Sean $z, w \in \mathbb{C}$. Entonces:

1. $|z| = |\overline{z}|$ y $z = 0 \iff |z| = 0$.
2. $|\mathbb{R}\text{e}(z)| \leq |z|$ y $|\mathbb{I}\text{m}(z)| \leq |z|$.
3. $|zw| = |z||w|$ y $|z + w| \leq |z| + |w|$.
4. Si $z \neq 0$, entonces $z^{-1} = \frac{\overline{z}}{|z|^2}$.
5. Si $w \neq 0$, entonces $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$.

- Sea $\theta \in \mathbb{R}$. Definimos $e^{i\theta}$ como:

$$e^{i\theta} = \cos(\theta) + i\sin(\theta)$$

- Sea $\theta, \varphi \in \mathbb{R}$, entonces:

1. $|e^{i\theta}| = 1$.
2. $\overline{e^{i\theta}} = (e^{i\theta})^{-1} = e^{-i\theta}$.
3. $e^{i\theta}e^{i\varphi} = e^{i(\theta+\varphi)}$.
4. $(e^{i\theta})^n = e^{ni\theta} = \cos(n\theta) + i\sin(n\theta)$

- $\arg(z)$ es el ángulo de z con el eje real. Se acostumbra a escoger un ángulo en el rango $(-\pi, \pi]$.

- **Forma Polar:** $z = |z|e^{i\arg(z)}$.

- Si $e^{i\theta} = e^{i\varphi}$, entonces existe algún $k \in \mathbb{Z}$ tal que $\theta = \varphi + 2k\pi$.

- Sea $z \in \mathbb{C}$ y $n \geq 2$. Diremos que z es una raiz n-ésima de la unidad si $z^n = 1$.

- Las raices n-ésimas de la unidad son de la forma $e^{i\frac{2k\pi}{n}}$ con $k \in \{0, \ldots, n-1\}$.

- Sea $z, w \in \mathbb{C}$ y $n \geq 2$. Diremos que z es una raiz n-ésima de w si $z^n = w$.

- Las raices n-ésimas de $z = Re^{i\theta} \in \mathbb{C}$ son de la forma $\sqrt[n]{R}e^{i\frac{\theta+2k\pi}{n}}$ con $k \in \{0, \ldots, n-1\}$.

- Sea $n \geq 2$. La suma de las n raíces n-ésimas de la unidad vale 0.

- Consideraremos a $(\mathbb{K}, +, \cdot)$ como el cuerpo $\mathbb{R}$ o $\mathbb{C}$. Un polinomio es una función $p : \mathbb{K} \to \mathbb{K}$ de la forma:

$$p(x) = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + \ldots + a_n x^n$$

donde $a_0, a_1, \ldots, a_n$ son constantes en $\mathbb{K}$ a las que llamaremos coeficientes.

- Al conjunto de polinomios con coeficientes en $\mathbb{K}$ se le denota $\mathbb{K}[x]$.

- Sean $p, q \in \mathbb{K}[x]$.

$$p = q \iff \text{Los coeficientes de } p \text{ y } q \text{ son iguales.}$$

- Sea $p \in \mathbb{K}[x]$. Definimos $\text{gr}(p)$ (el grado) como el k más grande tal que $a_k \neq 0$. Si $p \equiv 0$, diremos que $\text{gr}(p) = -\infty$.

- Diremos que $p \in \mathbb{K}[x]$ es mónico si el coeficiente asociado a $x^{\text{gr}(p)}$ es 1.

- Sea $p(x) = \sum_{k=0}^{n} a_k x^k$ y $q(x) = \sum_{k=0}^{n} b_k x^k$ definimos:

1. $(p+q)(x) = \sum_{k=0}^{n} (a_k + b_k)x^k$
2. $(pq)(x) = \sum_{k=0}^{2n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$

Estas operaciones verifican:

1. $\text{gr}(p+q) \leq \text{máx}\{\text{gr}(p), \text{gr}(q)\}$.
2. $\text{gr}(pq) = \text{gr}(p) + \text{gr}(q)$.

- $(\mathbb{K}[x], +, \cdot)$ es un anillo conmutativo con unidad, que no posee divisores del 0.

- En $(\mathbb{K}[x], +, \cdot)$, los únicos elementos con inverso para $\cdot$ son los polinomios de grado 0.

- Sean $p, d \in \mathbb{K}[x]$ con $d \neq 0$. Entonces existe un único par $q, r \in \mathbb{K}[x]$ tal que:

1. $p = qd + r$.
2. $\text{gr}(r) < \text{gr}(d)$.

A r lo llamaremos resto. Si $r \equiv 0$, diremos que d divide a p y lo denotaremos por $d|p$.

- **Teorema del Resto:** Sea $p \in \mathbb{K}[x]$ y $c \in \mathbb{K}$. El resto de dividir p por el polinomio $(x - c)$ es $p(c)$.

- Diremos que $c \in \mathbb{K}$ es una raíz de $p \in \mathbb{K}[x]$ si $p(c) = 0$.

- Si $c_1, c_2, \ldots, c_k$ son raíces distintas de p, entonces:

$$(x - c_1)(x - c_2)\ldots(x - c_k)|p(x)$$

- Sea $n \geq 1$. Si $p \in \mathbb{K}[x]$ es tal que $\text{gr}(p) = n$, entonces p posee a lo más n raíces distintas.

- Sea $n \geq 1$ y $p, q \in \mathbb{K}[x]$ tales que $\text{gr}(p) \leq n$ y $\text{gr}(q) \leq n$. Si p y q coinciden en $n + 1$ puntos distintos, entonces son iguales.

- **Teorema Fundamental del Álgebra:**
  Sea $p \in \mathbb{C}[x]$ tal que $\text{gr}(p) = n \geq 1$. Entonces p posee al menos una raíz en $\mathbb{C}$.

- Sea $p \in \mathbb{C}[x]$ tal que $\text{gr}(p) = n \geq 1$. Entonces existen $\alpha, c_1, \ldots c_m \in \mathbb{C}$ y $l_1, \cdots l_m \in \mathbb{N}$ tales que:

$$p(x) = \alpha(x - c_1)^{l_1} \ldots (x - c_m)^{l_m}$$

- Sea $p \in \mathbb{C}[x]$ con coeficientes en $\mathbb{R}$ y sea $z \in \mathbb{C}$ una raiz de p. Entonces $\overline{z}$ es una raiz de p.

- Sea $p \in \mathbb{R}[x]$, tal que $\text{gr}(p) = n \geq 1$. Entonces existen valores $\alpha, c_1, \ldots, c_m, a_1, b_1, \ldots, a_s, b_s \in \mathbb{R}$ tales que:

$$p \equiv \alpha(x-c_1)\ldots(x-c_m)(x^2+a_1x+b_1)\ldots(x^2+a_sx+b_s)$$

- **Teorema de la Raíz Racional:** Sea $p \in \mathbb{R}[x]$, con coeficientes en $\mathbb{Z}$. Si r y s son primos relativos tal que $\frac{r}{s}$ es una raíz de p, entonces:

$$r|a_0 \quad \wedge \quad s|a_n$$

- Sea $p \in \mathbb{R}[x]$ mónico con coeficientes en $\mathbb{Z}$. Entonces toda raíz racional de p es entera y divide a a_0.

- El algoritmo de Ruffini permite dividir un polinomio p por $x - c$.