

MATEMÁTICA BASICA

*José Darío Sánchez Hernández
Bogotá –Colombia. julio- 2009
danojuanos@hotmail.com
danojuanos@tutopia.com
danojuanos@yahoo.com*

Algunos de mis apreciados visitantes me proponían un material elemental dirigido a estudiantes un poco más neófitos, pero conservando el espíritu inicial que me he propuesto desde la iniciación de mi trabajo en el ciberespacio. Es ésta la razón para colocar un cursillo que sea como una invitación al aprendizaje de la matemática avanzada en el campo virtual.

CONTENIDO

§1. Fundamentos de Lógica.....	2
§2. Conjuntos.....	8
2.1 Clases de conjuntos.....	9
2.2 Proposiciones condicionales y cuantificadores.....	12
§3. Métodos de una demostración.....	16
§4. Parejas ordenadas y producto cartesiano.....	20
§5. Relaciones y funciones.....	23
§6. Clases de funciones.....	27
6.3 Función inversa.....	28
6.6 Algunas propiedades de las funciones.....	29
§7. Leyes de composición interna (operaciones).....	32
7.2 Clases de leyes de composición.....	34
§8. Concepto de Grupo.....	37
§9. Los números reales.....	40
9.3 Métodos geométricos y expansión decimal.....	42
9.4 Propiedades algebraicas.....	42
9.5 Propiedades de orden.....	46
9.6 Propiedades de completitud.....	49
§10. Los números naturales.....	52
§11. Los números enteros.....	54
§12. Números racionales.....	57

12.6 Construcción de los elementos racionales.....	58
§13. Acotación. Terminación. Extremación.....	61
13.5 Principio de buena ordenación.....	64
13.6 Divisibilidad.....	66
13.7 El algoritmo de Euclides.....	69
§14. Teorema fundamental de la aritmética.....	73
§15. Congruencias.....	75
§16. Clases Residuales.....	79
§17. Números complejos.....	83
17.2 Valor absoluto de un número complejo.....	85
17.3 Imposibilidad de ordenar los números complejos.....	88
17.4 Exponenciales complejas.....	89
17.5 Argumento de un número complejo.....	90
17.6 Potencias enteras y raíces de números complejos.....	92
17.7 Logaritmos complejos.....	92
17.8 Potencias complejas.....	93
Bibliografía.....	97

§ 1. FUNDAMENTOS DE LÓGICA

1.1 Los vocablos *verdadero* y *falso* son fundamentales en el estudio de la matemática, se consideran completamente conocidos y se aceptan *sin definir*, es decir se admiten intuitivamente como ideas iniciales y se notan

$$V \quad , \quad F$$

1.2 Las oraciones en las cuales se pueden establecer uno de los vocablos verdadero o falso se denominan *proposiciones* o afirmaciones. Son frecuentemente notadas por letras minúsculas p, q, r, s, \dots

EJEMPLOS. Las frases: ¿Cómo estas?, ¿Cuál es tu nombre?, que la suerte te acompañe; no son proposiciones

Bolívar es un hombre muy conocido, Bogotá es la capital de Bolivia, Venezuela es la patria del Libertador; son proposiciones.

Toda proposición suele ir acompañada de una tabla

p
V
F

llamada tabla de verdad y que indica las posibilidades de que la proposición p sea verdadera o falsa

1.3 Negar una proposición es el procedimiento, mediante el cual una proposición que es verdadera se convierte en falsa y recíprocamente si es falsa se convierte en verdadera.

Se usa en estos casos p para la proposición y $\neg p$ para su negación

p	$\neg p$
V	F
F	V

1.4 PROPOSICIONES COMPUESTAS. Una propiedad fundamental de las proposiciones se encuentra en el hecho de poderlas componer para obtener nuevas *oraciones* las cuales son nuevamente proposiciones llamadas proposiciones compuestas y están caracterizadas por tablas llamadas tradicionalmente *tablas de verdad*.

1.4.1 CONJUNCIÓN: Dadas dos proposiciones p y q la proposición compuesta $p \wedge q$ (p y q) es llamada *conjunción* y está definida por la siguiente tabla

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

es decir su tabla depende estrechamente de los valores de verdad de las proposiciones componentes.

EJEMPLO. Hoy es lunes y estamos a 28 de febrero de 1936.

Esta es una conjunción y es una proposición falsa por que estar a 28 de febrero de 1936 es una proposición falsa.

1.4.2. DISYUNCIÓN: Sean p y q dos proposiciones, la proposición $p \vee q$ (léase p o q) es una proposición compuesta llamada *disyunción* y está definida mediante la tabla

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

EJEMPLO. Colombia es una nación de América del sur o estamos a 9 de abril de 1948.

Esta proposición es una disyunción la cual es claramente una proposición verdadera, por que es verdad que Colombia es una nación de América del sur.

Se sigue entonces que la veracidad o falsedad de la disyunción o de la conjunción depende de la verdad o falsedad de las proposiciones componentes.

Hay una variación de la disyunción que se presenta en proposiciones como "el papa Juan Pablo II está vivo o el papa Juan Pablo II está muerto" esta es llamada el *o exclusivo* o *el aut* y está definida por la siguiente tabla

p	q	$p \underline{\vee} q$
V	V	F
V	F	V
F	V	V
F	F	F

1.4.3 IMPLICACIÓN: Sean p y q dos proposiciones, la proposición $p \Rightarrow q$ es llamada *implicación*, la cual se lee de una de las formas siguientes

p implica q
 si p entonces q
 p sólo si q
 p es una condición suficiente para q
 q es una condición necesaria para p

y es una proposición compuesta definida por la tabla

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

EJEMPLO. Si no me da pereza, entonces estudio geometría

Es de notar que la mayoría de los enunciados de la matemática están en forma de implicación, de donde su importancia.

EJEMPLO. Si a, b y c son las longitudes de los lados de un triángulo rectángulo entonces $c^2 = a^2 + b^2$.

1.4.4 EQUIVALENCIA: Sean p y q dos proposiciones, la proposición $p \Leftrightarrow q$ es llamada *equivalencia*, la cual se lee de una de las siguientes maneras

p es equivalente a q
 p si y sólo si q
 p es una condición necesaria y suficiente para q

es una proposición compuesta definida mediante la siguiente tabla

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

EJEMPLO. Sean a y b números enteros entonces se tiene $a \leq b$ si y sólo si $b - a$ es un número natural.

Los símbolos $\neg, \wedge, \vee, \underline{\vee}, \Rightarrow, \Leftrightarrow$ son referidos como los ***conectivos proposicionales***.

En adelante, además de p, q, r, s, \dots , usaremos p_1, p_2, p_3, \dots como símbolos para designar proposiciones y nos referiremos a ellos como los ***símbolos proposicionales***. Tenemos tantos símbolos proposicionales como números naturales, disponemos de una buena cantidad de ellos, suficientes para representar cualquier proposición que tengamos en la memoria; seguramente una persona no alcanza en toda su vida a fijar en su mente más proposiciones que números. Así, podemos considerar que cada símbolo proposicional representa una única proposición simple.

A cualquier combinación de símbolos proposicionales, se le determina *fórmula*, y aquellas para las cuales se les puede construir su tabla de verdad son frecuentemente llamadas *fórmulas bien formadas* (*f.b.f.*).

Las reglas que gobiernan las fórmulas bien formadas son:

- (1) Los símbolos proposicionales son fórmulas bien formadas
- (2) Si α es una fórmula bien formada, entonces su negación ($\neg\alpha$) es una fórmula bien formada.
- (3) Si α y β son fórmulas bien formadas entonces también lo son $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \underline{\vee} \beta)$, $(\alpha \Rightarrow \beta)$ y $(\alpha \Leftrightarrow \beta)$
- (4) Una expresión es una fórmula bien formada si y sólo si el que lo sea se sigue de aplicar (1), (2) y (3).

La regla (4) significa que las únicas fórmulas bien formadas son las que se pueden construir combinando (1), (2), (3) un número finito de veces.

Como una fórmula bien formada se ha obtenido a partir de finitos símbolos proposicionales y por aplicación de (1), (2) y (3) finitas veces, siempre es posible construir su tabla de verdad: se dan a los símbolos proposicionales que aparecen en la fórmula bien formada los valores V, F combinándolos adecuadamente para obtener todos los casos posibles y luego se van construyendo paso a paso las tablas de verdad de las fórmulas bien formadas que se han ido formando hasta llegar a la de la fórmula bien formada dada inicialmente (Nótese que si aparecen n símbolos proposicionales en una fórmula bien formada, su tabla de verdad tendrá 2^n filas, correspondientes a las 2^n formas posibles de combinar V y F)

Unos ejemplos aclararán lo dicho: Construir la tabla de verdad de $p \vee \neg p$, $(p \vee q) \wedge \neg p$, y $[p \wedge (p \Rightarrow q)] \Rightarrow q$:

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

p	q	$p \vee q$	$\neg p$	$(p \vee q) \wedge (\neg p)$
V	V	V	F	F
V	F	V	F	F
F	V	V	V	V
F	F	F	V	F

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$[p \wedge (p \Rightarrow q)] \Rightarrow q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

Observando las tablas de verdad anteriores, vemos que existen fórmulas bien formadas como $p \vee \neg p$, $[p \wedge (p \Rightarrow q)] \Rightarrow q$, tales que en su tabla de verdad únicamente aparece el valor V , sin importar la verdad o falsedad de sus proposiciones componentes; estas fórmulas se llaman **tautologías**. Son las fórmulas bien formadas más importantes, debido a que corresponden a proposiciones compuestas que intuitivamente son *siempre* verdaderas, independientemente de la veracidad de sus proposiciones componentes.

1.5 NEGACIÓN: Es de utilidad conocer la negación de los conectivos proposicionales y está dado por las siguientes tautologías:

$$\begin{aligned} \neg(p \vee q) &\Leftrightarrow (\neg p) \wedge (\neg q) \\ \neg(p \wedge q) &\Leftrightarrow (\neg p) \vee (\neg q) \\ \neg(p \Rightarrow q) &\Leftrightarrow p \wedge (\neg q) \\ \neg(p \Leftrightarrow q) &\Leftrightarrow \left\{ \begin{array}{l} (\neg p) \Leftrightarrow q \\ p \Leftrightarrow (\neg q) \end{array} \right\} \Leftrightarrow [(p \wedge \neg q) \vee (\neg p \wedge q)] \end{aligned}$$

1.6 EJERCICIOS.

1. Negar las siguientes proposiciones

- (a) Si el sol sale esta tarde, entonces voy a jugar
- (b) Estudiaré sólo si llueve
- (c) Comeré frutas si y solamente si es una pera o una manzana

2. Haga los cuadros de verdad para cada una de las proposiciones siguientes y concluya si son tautologías o no

- (a) $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
- (b) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
- (c) $(p \Rightarrow q) \Leftrightarrow (\neg p) \vee q$
- (d) $(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$
- (e) $\neg(\neg p) \Leftrightarrow p$
- (f) $p \wedge p \Leftrightarrow p$
- (g) $p \vee p \Leftrightarrow p$

3. De cada una de las expresiones siguientes, diga si es una *f.b.f.* o no; dé las razones de sus respuestas:

- (a) $(\neg p \Rightarrow \neg q) \Rightarrow \neg(p \vee q)$
- (b) $p \Rightarrow \underline{\vee} \neg r \wedge q$
- (c) $(p_1 \wedge p_2) \wedge p_3 \Leftrightarrow (\neg p_4 \vee p_3)$
- (d) $((p_1 \Rightarrow (\neg p_2)) \wedge p_1) \Rightarrow \neg p_2$
- (e) $p \wedge q \vee p \wedge r$
- (f) $(\neg \vee p) \Rightarrow (q \wedge r)$
- (g) $\neg(p \wedge q) \Rightarrow ((\neg p) \wedge (\neg q))$.

4. Use las tablas de verdad para probar que $(p \wedge \neg p) \Rightarrow q$ es una tautología.

5. Sea α, β fórmulas bien formadas. Se dice que " α implica tautológicamente a β " si $\alpha \Rightarrow \beta$ es una tautología. Se dice que " α es tautológicamente equivalente a β " si α implica tautológicamente a β y β implica tautológicamente a α , o lo que es igual, si $\alpha \Leftrightarrow \beta$ es una tautología. Halle cuatro ejemplos de implicaciones tautológicas y cuatro de equivalencias tautológicas

6. Una **contradicción** es una *f.b.f* compuesta que siempre es falsa, independientemente de la veracidad de las proposiciones componentes. Dar cinco ejemplos de contradicciones, demostrando que lo son mediante tablas de verdad, si es el caso.

7. Dadas las proposiciones p : Hace frío, y q : Está de noche, y suponiendo que la primera es verdadera en este momento y la segunda falsa, escriba en términos de p, q y los conectivos, las proposiciones siguientes, y halle sus valores de verdad:

- (a) No está de noche o no hace frío.
- (b) Hace frío o no está de noche.
- (c) Ni está de noche ni hace frío
- (d) Está de noche pero no hace frío.

§2. CONJUNTOS

Otra idea fundamental en el estudio de la matemática, es la de *conjunto* y la tomamos sin definir como materia prima. Intuitivamente es una colección de objetos llamados *elementos*, esta idea la vemos por ejemplo en un panal de abejas, en un rebaño de ovejas, en una planta de crianza de truchas, son ejemplos de conjuntos.

El hecho de *pertenecer* a un conjunto es otro concepto primitivo y que se toma como materia prima.

Notacionalmente los conjuntos suelen indicarse por letras del alfabeto en mayúscula y los elementos que los componen serán indicados por letras minúsculas en este caso se dice que los conjuntos están dados por *extensión*.

Cuando se dan las propiedades que definen a los elementos se dice que el conjunto se da por *comprensión*, es cuando se usan los corchetes y las palabras "conjunto de elementos tales que".

Si denotamos por $p(x)$ a una condición redactada en términos de la letra x , el conjunto determinado por ella se escribe

$$\{x/p(x)\} \quad \text{ó} \quad \{x : p(x)\}$$

A la condición le llamaremos muchas veces una *proposición condicional*. Usaremos también la palabra *colección* como sinónimo de conjunto. La fórmula " $a \in M$ " es utilizada para indicar " a es elemento del conjunto M " y suele leerse " a pertenece a M ".

2.1 CLASES DE CONJUNTOS. Los conjuntos se clasifican según el número de elementos que ellos tienen, así se tendrán conjuntos finitos y conjuntos infinitos.

El conjunto *universal* o referencial es un conjunto variable y es el más grande conjunto que se considere en un determinado problema, por ejemplo hablando de números el universo podría ser el conjunto de los números reales o el de los números complejos dependiendo de la teoría, si es real o si es compleja.

El conjunto *vacío* es un conjunto que carece completamente de elementos, se nota por la letra griega Φ ó $\{\}$.

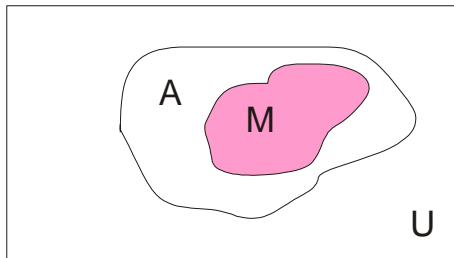
Algunos conjuntos frecuentemente usados y utilizados son:

$$\begin{aligned} \mathbb{N} &= \{0, 1, 2, \dots\} && \text{números naturales} \\ \mathbb{Z} &= \{\dots, -1, 0, 1, 2, \dots\} && \text{números enteros} \\ \mathbb{Q} &= \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\} \right\} && \text{números racionales} \\ \mathbb{R} &&& \text{el conjunto de los números reales} \\ \mathbb{C} &&& \text{el conjunto de los números complejos} \end{aligned}$$

2.1.2 DEFINICIÓN. Sea A un conjunto de un universo dado, un subconjunto M de A , notado $M \subseteq A$, está definido por la proposición condicional

$$\text{si } x \in M \text{ entonces } x \in A$$

Esta idea puede visualizarse por medio de un diagrama llamado diagrama de Venn



$$A \subseteq M \Leftrightarrow (x \in A \Rightarrow x \in M)$$

Decir que un elemento x no está en A se denota por la proposición compuesta

$$x \notin A \Leftrightarrow \neg(x \in A)$$

2.1.3 DEFINICIÓN. Un conjunto A se dice igual a un conjunto B si la siguiente proposición es verdadera

$$A \subseteq B \wedge B \subseteq A$$

o sea

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

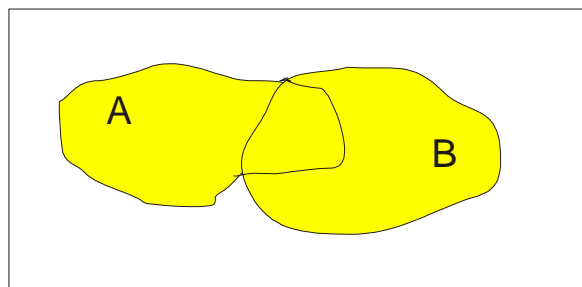
2.1.4 PROPOSICIÓN. Sea A un conjunto arbitrario de un universo dado U entonces $\Phi \subseteq A$.

DEMOSTRACIÓN. La proposición condicional $x \in \Phi \Rightarrow x \in A$ es siempre verdadera, pues $x \in \Phi$ es falsa

2.1.5 DEFINICIÓN. Sean A y B conjuntos de un universo dado. La *reunión* de A con B , notada $A \cup B$, está definida por la proposición compuesta

$$x \in A \cup B \Rightarrow x \in A \vee x \in B$$

es decir, es el conjunto de los elementos que están en A o están en B . Si hacemos uso de diagrama de Venn tenemos

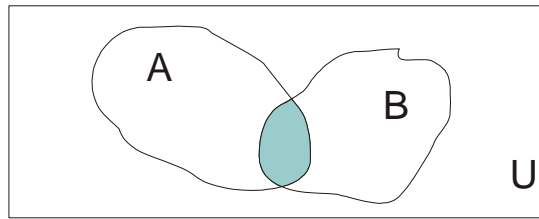


$$A \cup B = \{x/x \in A \vee x \in B\}$$

2.1.6 DEFINICIÓN. Sean A y B conjuntos de un universo dado, la intersección de A con B , notado $A \cap B$, está definida por la siguiente proposición

$$x \in A \cap B \Leftrightarrow (x \in A \wedge x \in B)$$

es decir, el conjunto de los elementos comunes a A y B ; en diagrama de Venn se tiene



$$A \cap B = \{x/x \in A \wedge x \in B\}$$

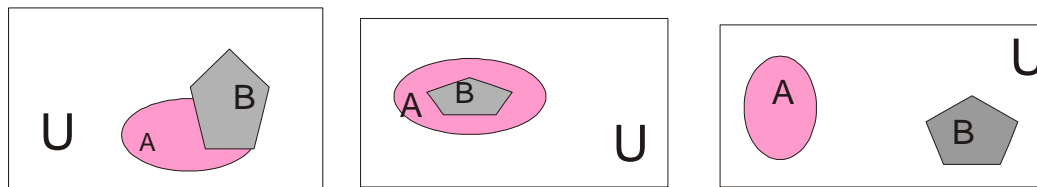
- 2.1.7 PROPOSICIÓN.** (a) $A = B$ implica $A \cap B = A \cup B = A = B$
 (b) Si $A \subseteq B$ entonces $A \cup B = B$ y $A \cap B = A$
 (c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
 (d) $A \cup \Phi = A$
 (e) $A \cup B = B \cup A$
 (f) $A \cap B = B \cap A$

La demostración se propone como ejercicio.

2.1.8 DEFINICIÓN. Sean A y B conjuntos de un universo dado, la diferencia de A con B es notada $A - B$ y está definida por la siguiente proposición

$$x \in A - B \Leftrightarrow x \in A \wedge x \notin B$$

con diagrama de Venn sería:



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

2.1.9 DEFINICIÓN. Sean A y B conjuntos de un universo dado U y tal que $A \subseteq B$ entonces el complemento de A con respecto a B es definido por

$$C_B A = B - A$$

Cuando B es el universo U se dice simplemente el complemento de A notado $C_U A$ ó $C A$ y está definido por la proposición

$$x \in C A \Leftrightarrow x \notin A$$

2.1.10 PROPOSICIÓN. Sean A y B conjuntos de un universo U , entonces

(i) $C(A \cup B) = (C A) \cap (C B)$

$$(ii) \mathbf{C}(A \cap B) = (\mathbf{C}A) \cup (\mathbf{C}B)$$

$$(iii) (\mathbf{C}A) \cap A = \Phi$$

$$(iv) (\mathbf{C}A) \cup A = U$$

$$(v) \mathbf{C}(U) = \Phi$$

$$(vi) \mathbf{C}(\Phi) = U$$

DEMOSTRACIÓN. Se hacen en forma directa usando las definiciones y la fórmulas bien formadas dadas en la sección anterior así:

$$\begin{aligned} (i) \quad x \in \mathbf{C}(A \cup B) &\Leftrightarrow x \notin (A \cup B) \Leftrightarrow \neg(x \in A \cup B) \\ &\Leftrightarrow \neg(x \in A \vee x \in B) \Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) \\ &\Leftrightarrow x \notin A \wedge x \notin B \Leftrightarrow x \in \mathbf{C}A \wedge x \in \mathbf{C}B \Leftrightarrow x \in (\mathbf{C}A) \cap (\mathbf{C}B) \end{aligned}$$

Siguiendo el mismo orden de ideas se demuestran las restantes afirmaciones.

2.2 PROPOSICIONES CONDICIONALES Y CUANTIFICADORES

2.2.1 DEFINICIÓN. Sea A un conjunto de un universo dado, una *variable* de A es un símbolo que representa a cualquier elemento de A y una *constante* en A es un símbolo que representa exactamente un elemento de A bien determinado.

2.2.2 DEFINICIÓN. Una proposición condicional es una sucesión de símbolos envolviendo variables y que se convierten en proposición al reemplazar estas variables en un universo conveniente y notan

$$p_x / x \in U, \quad p_y / y \in U \dots$$

siempre y cuando x ó y sean las variables.

EJEMPLOS. (1) $p_x : x + 1 = 0$ es una sucesión de símbolos

$(p_x : x + 1 = 0)(x \in \mathbb{Z})$ es la proposición condicional

(2) $p_x : x^2 + 1 + 2x = 0$ es una sucesión de símbolos

$(p_x : x^2 + 1 + 2x = 0)(x \in \mathfrak{R})$ es la proposición condicional

(3) $p_x : x^2 - 1 = (x + 1)(x - 1)$ es una sucesión de símbolos

$(p_x : x^2 - 1 = (x + 1)(x - 1))(x \in \mathfrak{R})$ es la proposición condicional

2.2.3 DEFINICIÓN. Se llama *conjunto solución* de una proposición condicional al subconjunto del universo dado, donde la proposición condicional es verdadera.

Sea $(p_x)(x \in U)$ y P su conjunto solución entonces

$$P = \{x \in U / p_x \text{ es verdadera}\}$$

2.2.4 PROPOSICIÓN. Sea $(p_x)(x \in U)$ una proposición condicional, si P es el conjunto solución de $(p_x)(x \in U)$ entonces

$$\{x \in U / p_x \text{ es falso}\} = \{x \in U / \neg(p_x) \text{ es verdad}\} = \mathbf{CP}$$

DEMOSTRACIÓN. Sea $a \in \{x / \neg(p_x)\} \Leftrightarrow \neg p_a$ es verdadero $\Leftrightarrow p_a$ es falso $\Leftrightarrow a \notin \{x / p_x\} = P \Leftrightarrow a \in \mathbf{CP}$.

□

2.2.5 PROPOSICIÓN. Sean $(p_x)(x \in U)$ y $(q_x)(x \in U)$ dos proposiciones condicionales con P y Q como conjuntos de soluciones entonces

$$\{x / p_x \wedge q_x\} = P \cap Q$$

DEMOSTRACIÓN. Sea $a \in \{x / p_x \wedge q_x\} \Leftrightarrow p_a \wedge q_a$ es verdadera $\Leftrightarrow p_a$ es verdadera y q_a es verdadera $\Leftrightarrow a \in P$ y $a \in Q \Leftrightarrow a \in P \cap Q$.

□

2.2.6 PROPOSICIÓN. Sean $(p_x)(x \in U)$ y $(q_x)(x \in U)$ dos proposiciones condicionales con P y Q como conjuntos de soluciones entonces

$$\{x \in U / p_x \vee q_x\} = P \cup Q$$

DEMOSTRACIÓN. Sea $a \in \{x \in U / p_x \vee q_x\} \Leftrightarrow p_a \vee q_a$ es verdadera $\Leftrightarrow p_a$ es verdadera, ó, q_a es verdadera $\Leftrightarrow a \in P \vee a \in Q \Leftrightarrow a \in P \cup Q$.

□

2.2.7 PROPOSICIÓN. Sean $(p_x)(x \in U)$ y $(q_x)(x \in U)$ dos proposiciones condicionales con P y Q como conjuntos de soluciones entonces

$$\{x \in U / p_x \Rightarrow q_x\} = (\mathbf{CP}) \cup Q$$

DEMOSTRACIÓN. Se sabe que $(p \Rightarrow q) \Leftrightarrow ((\neg p) \vee q)$ es una tautología por lo tanto

$$\{x \in U / p_x \Rightarrow q_x\} = \{x \in U / (\neg p_x) \vee q_x\} = (\mathbf{CP}) \cup Q.$$

□

2.2.8 PROPOSICIÓN. Sean $(p_x)(x \in U)$ y $(q_x)(x \in U)$ dos proposiciones condicionales con P y Q como conjuntos de soluciones entonces

$$\{x \in U / p_x \Leftrightarrow q_x\} = (P \cap Q) \cup (\mathbf{CP} \cap \mathbf{CQ})$$

DEMOSTRACIÓN. $\{x \in U / p_x \Leftrightarrow q_x\} = \{x \in U / (p_x \Rightarrow q_x) \wedge (q_x \Rightarrow p_x)\} =$

$$\begin{aligned}
&= \{x \in U / p_x \Rightarrow q_x\} \cap \{x \in U / q_x \Rightarrow p_x\} = (\mathbf{C}P \cup Q) \cap (\mathbf{C}Q \cup P) = \\
&= [(\mathbf{C}P \cup Q) \cap \mathbf{C}Q] \cup [(\mathbf{C}P \cup Q) \cap P] = \\
&= [(\mathbf{C}P \cap \mathbf{C}Q) \cup (Q \cap \mathbf{C}Q)] \cup [(\mathbf{C}P \cap P) \cup (Q \cap P)] \\
&= (P \cap Q) \cup (\mathbf{C}P \cap \mathbf{C}Q)
\end{aligned}$$

□

2.2.9 Un *cuantificador* es un símbolo que nos responde a la pregunta ¿Cuántos elementos del universo en consideración satisfacen a una proposición condicional?

Así los cuantificadores son de dos tipos: existencial y universal

El cuantificador *existencial* denotado con \exists y está definido así:

Sea $(p_x)(x \in U)$ una proposición condicional y $P \subseteq U$ su conjunto solución entonces

$$(\exists x \in U)(p_x) \Leftrightarrow P \neq \Phi$$

léase existe un x en U tal que p_x es verdadera y esto es equivalente a decir que el conjunto solución de p_x no es vacío.

El cuantificador *universal* notado \forall , está definido así: Sea $(p_x)(x \in U)$ una proposición condicional y sea $P \subseteq U$ es el conjunto solución de p_x entonces

$$(\forall x \in U)(p_x \text{ es verdadera}) \Leftrightarrow P = U$$

léase para todo x en U p_x es verdadera y esto es equivalente a decir el conjunto solución de p_x es igual al universo.

EJEMPLOS. (1) La proposición condicional $(x^2 + 1 = 0)(x \in \mathbb{C})$ tiene conjunto solución no vacío, entonces se puede usar el cuantificador así

$$(\exists x \in \mathbb{C})(x^2 + 1 = 0)$$

(2) $(x^2 - 1 = (x - 1)(x + 1))(x \in \mathbb{C})$ tiene por conjunto solución al conjunto \mathbb{C} entonces se puede usar el cuantificador así:

$$(\forall x \in \mathbb{C})(x^2 - 1 = (x - 1)(x + 1))$$

2.2.10 NEGACIÓN DE CUANTIFICADORES

PROPOSICIÓN. (1) $\neg(\exists x \in U)(p_x) \Leftrightarrow (\forall x \in U)(\neg p_x)$

$$(2) \neg(\forall x \in U)(p_x) \Leftrightarrow (\exists x \in U)(\neg p_x)$$

Veamos el caso (2): Sea P el conjunto solución de p_x entonces

$$\neg(\forall x \in U)(p_x) \Leftrightarrow \neg(P = U) \Leftrightarrow \neg(P = P \cup \mathbf{C}P) \Leftrightarrow \mathbf{C}P \neq \mathbf{C}(P \cup \mathbf{C}P) = \mathbf{C}P \cap \mathbf{C}(\mathbf{C}P)$$

$$\Leftrightarrow \mathbf{C}P \neq \Phi \Leftrightarrow (\exists x \in U)(\neg p_x)$$

EJEMPLO. Todos los hombres son buenos

Cuantificación: Sea $U = \{\text{Hombres del mundo}\}$

$$(\forall x \in U)(x \text{ es bueno})$$

Si queremos la negación tendríamos

$$(\exists x \in U)(x \text{ no es bueno})$$

En español sería: Hay hombres que son malos.

2.3 EJERCICIOS

(1) Tomando como referencial al conjunto de los números reales, hallar los conjuntos que definen las condiciones siguientes

$$(a) (x^2 - 8x + 15)(x + 1) = 0$$

$$(b) x^2 - 5x + 15 \geq 0$$

$$(c) x^2 < 2$$

(2) Resolver el ejercicio (1) tomando como referencial el conjunto \mathbb{Z} de los enteros.

(3) Resolver el ejercicio (1) considerando como referencial el conjunto $\{6, 7, 8, 9, \dots\}$ de todos los números naturales mayores o iguales a 6.

(4) En cada uno de los tres ejercicios anteriores, anteponer a cada condición un cuantificador adecuado para que se obtenga una proposición verdadera; dar las razones de sus respuestas.

(5) Escribir la negación de cada una de las proposiciones siguientes:

Todos los hombres son mortales.

$$(\forall x)(x + 0 = x)$$

$$(\exists x)(\forall y)(x + y > 0)$$

(6) Tomando como referencial al conjunto de los números reales, hallar una condición $p(x, y)$ en dos variables, tal que

$$(\exists x)(\forall y)(p(x, y)) \text{ sea falsa y}$$

$$(\forall y)(\exists x)(p(x, y)) \text{ sea verdadera}$$

(7) (a) Hallar todos los subconjuntos del conjunto $\{1, 2, 3\}$ o sea $P(\{1, 2, 3\})$

(b) Hallar todos los subconjuntos del conjunto $\{1, 2\}$ ($P(\{1, 2\})$)

(c) Hallar todos los subconjuntos del conjunto $\{1\}$ ($P(\{1\})$)

(d) Hallar todos los subconjuntos del conjunto Φ .

(e) ¿Podría usted adivinar una relación entre el número de elementos de un conjunto finito y el número de sus subconjuntos?

(8) Escribir la negación de cada una de las expresiones siguientes:

$$(\forall x)(p(x) \Rightarrow q(x))$$

$$(\forall x)p(x) \Rightarrow (q(x) \vee r(x))$$

$$(\exists x)(\forall z)(p(x, z) \wedge q(z))$$

(9) Sea S un referencial para una condición $p(x)$. Sea $A \subseteq S$. Definimos $(\forall x \in A)(p(x))$ como $(\forall x)(x \in A \Rightarrow p(x))$ es verdadera). Análogamente, definimos $(\exists x \in A)(p(x))$ como $(\exists x)(x \in A \wedge p(x))$ es verdadera).

Demuestre que

$$\neg(\forall x \in A)(p(x)) \Leftrightarrow (\exists x \in A)(\neg p(x))$$

y que

$$\neg(\exists x \in A)(p(x)) \Leftrightarrow (\forall x \in A)(\neg p(x))$$

(10) ¿Qué sentido tiene para usted expresiones como

$$(\forall x)(2 + 3 = 5), (\exists x)(2 \cdot 4 = 8) ?$$

¿Son éstas proposiciones? ¿Se podría suprimir el cuantificador?

(11) Dé justificaciones a las equivalencias siguientes:

$$(\forall x)(p \wedge q(x)) \Leftrightarrow (p \wedge (\forall x)q(x))$$

$$(\forall x)(p \vee q(x)) \Leftrightarrow p \vee (\forall x)(q(x))$$

$$(\exists x)(p \wedge q(x)) \Rightarrow p \wedge (\exists x)(q(x))$$

$$(\exists x)(p \vee q(x)) \Rightarrow p \vee (\exists x)(q(x))$$

Nota: p es una proposición en la cual no aparece x .

(12) Escriba en español correcto la negación de las frases siguientes:

(a) Si las Matemáticas son fáciles, aprobaré el curso

(b) Existe un número natural m tal que cualquiera sea el natural n , $m \leq n$

(c) Si el costo de vida continúa subiendo, algunos tendremos que dejar la "costumbre burguesa" de comer tres veces al día o trabajar por un cambio de estructuras.

(d) Todos tenemos problemas y algunos nos dejamos vencer por ellos.

(e) Todos los gatos son pardos o algunos estamos miopes.

(13) Diga, dando las razones de sus respuestas, cuáles de las afirmaciones siguientes son verdaderas y cuáles no:

(a) $\{1, 1, 2\} \subseteq \{1, 2\}$

(b) $\{1, 2, 2\} = \{2, 1\}$

(c) $a \in \{\{a\}\}$

(e) $A \subseteq \Phi \Rightarrow A = \Phi$.

§3. MÉTODOS DE UNA DEMOSTRACIÓN

Uno de los criterios de deducción más importantes y el cual es inherente al hombre, es el dado por la tautología

$$[p \wedge (p \Rightarrow q)] \Rightarrow q$$

llamada el *modus ponens* la cual afirma que con el conocimiento de p y $p \Rightarrow q$ se deduce la veracidad de q , es el razonamiento del hombre prehistórico cuando razonaba así:

Yo mato toro y, si yo mato toro entonces calmo hambre, entonces yo calmo hambre.

Este criterio es utilizado en la mayoría de las pruebas de la matemática aunque siempre está tácita su utilización. A continuación se darán unos métodos clásicos de demostración.

3.1 *Método trivial* ; se trata de estudiar la veracidad de la proposición $p \Rightarrow q$ estudiando la proposición p en si misma. Si p es falsa no importa que sea q , $p \Rightarrow q$ siempre es verdadera.

EJEMPLO. Estamos en el siglo XXII, entonces hoy es viernes, es una proposición compuesta verdadera por que la hipótesis es falsa.

3.2 Método vacío ; consiste en estudiar la veracidad de la proposición $p \Rightarrow q$ estudiando la proposición q en si misma, así si q es verdadera no importa cual sea el valor de verdad de p la proposición compuesta $p \Rightarrow q$ siempre es verdadera.

EJEMPLO. Si Julio César fue un gran guerrero, entonces Bogotá es la capital de Colombia. Esta proposición es verdadera

En álgebra, si $(\forall x \in \mathbb{Z})(x^2 + 2 = 1)$ entonces $2 = 1 + 1$, en una proposición verdadera.

3.3 Método indirecto ; se aplica en el estudio de la veracidad de la proposición $p \Rightarrow q$, procediendo de la siguiente forma

(i) Supóngase que q es falsa

(ii) Con este hecho y otros conocidos dentro de la teoría se demuestra que p es falsa.

Entonces se tiene que $p \Rightarrow q$ es verdadera. Este método también es conocido como el contrarrecíproco.

EJEMPLO. Si a^2 es par entonces a es par

PRUEBA: (i) Supongamos que a no es par

(ii) existe $m \in \mathbb{N}$ tal que $a = 2m + 1$

(iii) $a^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$

así, existe $k = 2m^2 + 2m \in \mathbb{N}$ tal que $a^2 = 2k + 1$ ó sea que a^2 no es par.

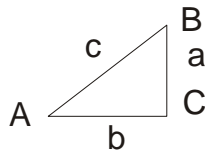
3.4 Método directo ; se trata de probar que la proposición $p \Rightarrow q$ es verdadera y se procede así;

(i) Se supone que p es verdadera

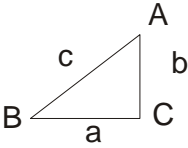
(ii) Con este hecho y otros bien conocidos de la teoría se demuestra que q es verdadera.

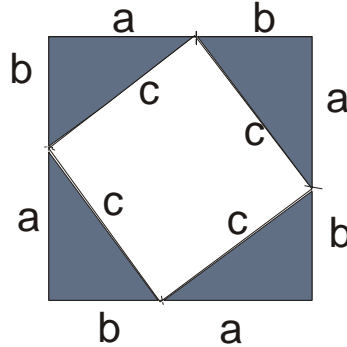
Así $p \Rightarrow q$ es verdadera.

EJEMPLO. Si $\triangle ABC$ es un triángulo rectángulo, entonces $a^2 + b = c^2$ donde a, b son las longitudes de los catetos y c es la longitud de la hipotenusa.



PRUEBA: (i) Supongamos que es un triángulo rectángulo

(ii) con el triángulo  construimos un cuadrado que tenga de lado $a + b$ así;



(iii) El área del cuadrado de lado $a + b$ será $(a + b)^2 = a^2 + 2ab + b^2$

pero sumando áreas tenemos que $(a + b)^2 = c^2 + 2ab$

así

$$a^2 + 2ab + b^2 = c^2 + 2ab$$

de donde tenemos

$$a^2 + b^2 = c^2$$

□

3.5 *Método de contradicción* (Absurdo). Sea τ una teoría y p una proposición de la teoría, de la cual se desea saber su veracidad. El método consiste en:

- (i) Construir una nueva teoría τ' obtenida adjuntado a τ la proposición $\neg p$
 - (ii) Se demuestra que la teoría τ' es contradictoria ó inconsistente, hallando en τ' una proposición q verdadera y $\neg q$ verdadera.
- Así tenemos que p es una proposición verdadera en τ .

EJEMPLO. No se puede dividir por cero

PRUEBA. (i) Sea τ la teoría de los números reales y p la proposición: no se puede dividir por cero.

(ii) Sea τ' la teoría de los números reales en los cuales se puede dividir por cero.

(iii) Consideremos en τ' la siguiente igualdad

$$a = b \quad a, b \in \mathbb{Z} - \{0\}$$

Se multiplica por a ambos miembros de la anterior igualdad obteniéndose

$$a^2 = ab$$

Agregue $-b^2$ a los dos lados de la igualdad

$$a^2 - b^2 = ab - b^2$$

Factorizando se tiene

$$(a - b)(a + b) = (a - b)b$$

Como en τ' se puede dividir por cero, entonces simplificamos por $(a - b)$, así se obtiene

$$a + b = b$$

Como $a = b$, se tiene

$$2a = a$$

Simplificando por a se llega a la proposición

$$2 = 1$$

Así en la teoría τ' se tendría simultáneamente

$$2 \neq 1 \text{ y } 2 = 1$$

obteniéndose que τ' es una teoría contradictoria, (es usual afirmar en estos casos que τ' es absurdo)

Luego no se puede dividir por cero.

3.6 Método del contra-ejemplo. Dada una proposición p la cual quiere ser probada, es decir, la cual se desea adjuntar como verdadera dentro de una teoría. El método consiste en hallar un ejemplo donde se diga lo contrario de la proposición deseada, así la proposición queda automáticamente falsa dentro de la teoría.

EJEMPLO. En la teoría de los números enteros si el cuadrado de un número entero es impar el número es primo.

PRUEBA. Se usa el método del contra-ejemplo, así $81 = 9^2$ es número impar sin embargo 9 no es número primo.

Así la proposición es falsa en la teoría de los números enteros.

3.7 EJERCICIOS.

(1) Puede suceder que $A \cap B = B$; dé un ejemplo en el cual se cumpla dicha igualdad. ¿Podría idear (demostrándolo) una condición necesaria y suficiente para que tal igualdad se cumpla?

(2) Se pide lo mismo que en el (1) pero con respecto a $A \cup B = A$.

(3) Demuestre que si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$ y que si $M \subseteq N$ entonces $P(M) \subseteq P(N)$

Aquí $P(M) = \{X/X \subseteq M\}$ el conjunto llamado partes de M .

(4) Pruebe que

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

y que

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

(5) Sea S un conjunto referencial y sean A, B subconjuntos de S : Demuestre que

$$A - B = A \cap (\mathbf{C}_S B).$$

(6) Puede suceder que $A - B = \Phi$; dé dos ejemplos en los cuales se cumpla dicha igualdad e idee (demostrándolo) una condición necesaria y suficiente para que tal igualdad se cumpla.

(7) Sean A_1, A_2, \dots, A_n conjuntos. Pruebe que si $(A_1 \subseteq A_2)$ y $(A_2 \subseteq A_3)$, y... y $(A_{n-1} \subseteq A_n)$ y $(A_n \subseteq A_1)$, entonces $A_1 = A_2 = \dots = A_n$.

(8) Sean P, Q subconjuntos de un conjunto referencial S . Demuestre que $P \subseteq Q$ si y sólo si $(\mathbf{C}_S Q) \subseteq (\mathbf{C}_S P)$.

(9) Pruebe que $(A - B) - C \subset A - (B - C)$, pero que en general no se tiene la contención en el sentido contrario. Demuestre además que

$$A - (B - C) \subset (A - B) \cup (A \cap C)$$

(10) Muestre que $A \cap (B - C) = (A \cap B) - (A \cap C)$
 $A \cup (B - C) = (A \cup B) - (C - A)$

Pero que en general la unión no es distributiva respecto de la diferencia.

(11) (a) Dé una justificación a la equivalencia

$$(\forall x)(p(x) \wedge q(x)) \Leftrightarrow [(\forall x)(p(x)) \wedge (\forall x)(q(x))]$$

(b) Úsela para demostrar que

$$(\exists x)(p(x) \vee q(x)) \Leftrightarrow (\exists x)(p(x)) \vee (\exists x)(q(x)).$$

Ayuda: niegue en los dos lados de la equivalencia anterior

(12) Análogamente al ejercicio anterior, justifique que

$$(\exists x)(p(x) \wedge q(x)) \Rightarrow [(\exists x)(p(x)) \wedge (\exists x)(q(x))].$$

(13) Halle un referencial y condiciones $p(x), q(x)$ adecuadas para hacer ver que en general $(\exists x)(p(x)) \wedge (\exists x)(q(x))$ no implica $(\exists x)(p(x) \wedge q(x))$.

(14) Si A es el conjunto de los enteros múltiplos de 6 y B el de los múltiplos de 10, halle $A \cup B$ y $A \cap B$.

(15) (a) ¿Podría hallar dos subconjuntos infinitos del conjunto B de los números naturales, que sean disyuntos?

(b) ¿Podría hallar siete subconjuntos infinitos de \mathbb{N} que sean disyuntos dos a dos?

(c) ¿Será posible hallar n (siendo n número natural mayor que 1) subconjuntos infinitos de \mathbb{N} que sean disyuntos dos a dos?

§4. PAREJAS ORDENADAS Y PRODUCTO CARTESIANO

4.1 DEFINICIÓN. Sean A y B dos conjuntos de un universo dado, una pareja ordenada (a, b) de un elemento de A y otro de B está definida por el siguiente conjunto

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

Si $a \neq b$ entonces $(a, b) \neq (b, a)$ ya que $\{\{a\}, \{a, b\}\} \neq \{\{b\}, \{a, b\}\}$ pues por hipótesis $a \neq b$.

4.2 PROPOSICIÓN. Si $(a, b) = (c, d)$, entonces $a = c$ y $b = d$

DEMOSTRACIÓN. Si $(a, b) = (c, d)$ entonces $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Para que se tenga la igualdad es natural que los conjuntos de un elemento sean iguales o sea

$$\{a\} = \{c\} \quad \text{y} \quad \{a, b\} = \{c, d\}$$

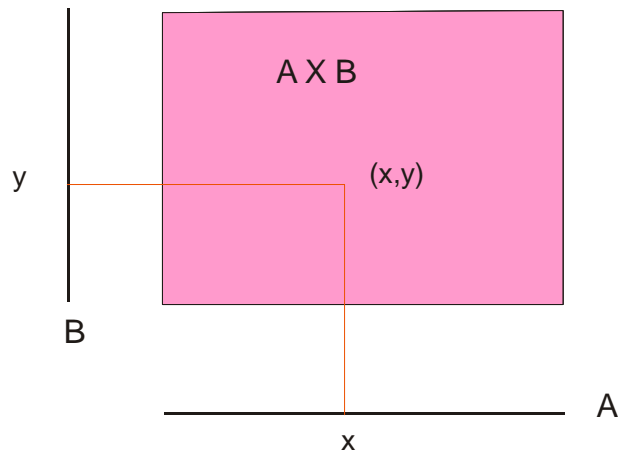
así del primero se tiene $a = c$ y del segundo $\{a, b\} = \{a, d\}$ se deduce que $b = d$.

□

4.3 DEFINICIÓN. Sean A y B dos conjuntos de un universo dado. Se define el producto cartesiano de A por B mediante la siguiente proposición

$$(x, y) \in A \times B \Leftrightarrow x \in A \wedge y \in B$$

es decir, es el conjunto de parejas ordenadas tales que la primera componente está en A y la segunda en B . Si hacemos uso de un diagrama de Venn, podríamos interpretarlo así



$$A \times B = \{(x, y) / x \in A \wedge y \in B\}$$

4.4 PROPOSICIÓN. Sean A, B y C conjuntos de un universo dado

$$(i) \quad A \times (B \cup C) = (A \times B) \cup (A \times C)$$

$$(ii) \quad A \times (B \cap C) = (A \times B) \cap (A \times C)$$

DEMOSTRACIÓN. (i) Sea $p \in A \times (B \cup C) \Leftrightarrow p = (x, y) : (x, y) \in A \times (B \cup C)$
 $\Leftrightarrow x \in A \wedge y \in B \cup C \Leftrightarrow x \in A \wedge (y \in B \vee y \in C) \Leftrightarrow (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C)$
 $\Leftrightarrow (x, y) \in A \times B \vee (x, y) \in A \times C \Leftrightarrow p \in A \times B \vee p \in A \times C$
 $\Leftrightarrow p \in (A \times B) \cup (A \times C)$

Análogamente se procede para (ii)

4.5 EJERCICIOS.

(1) Sean R, S, T conjuntos de un universo dado. Demostrar que $(R \cap S) \times T \subseteq R \times (T \cup S)$.

(2) En las hipótesis de (1) demuestre que $R \times (S \cup T) \subseteq (R \cup T) \times S$

(3) Negar las siguientes frases:

Si todos los animales tienen plumas, entonces algunos hombres tienen cuernos.

Algunos animales son mamíferos y todos tienen piel, es equivalente a decir que algunas aves tienen piel y todas son ovíparas.

Si todos los toreros son buenos, entonces algún toro Colombiano embiste.

(4) Cuantifique las siguientes frases:

Los habitantes europeos son todos industriales

En la Universidad Nacional unos estudiantes son físicos

Las medidas de los ángulos interiores de un triángulo siempre miden 180° .

(5) ¿Qué sentido tiene para usted, expresiones como $(\forall x)(2 + 3 = 5)$, $(\exists x)(2 \cdot 4 = 8)$? ¿Son estas proposiciones? ¿Se podría suprimir el cuantificador?

(6) Sean A, B y C conjuntos en un universo, muestre que

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

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

pero que en general la unión no es distributiva respecto de la diferencia.

(7) Definimos una nueva operación entre conjuntos llamada la *diferencia simétrica* así:

$$A \Delta B = \{x/x \in A \vee x \in B\}$$

(a) Usando una tautología apropiada pruebe la asociatividad de la diferencia simétrica: $(A \Delta B) \Delta C = A \Delta (B \Delta C)$

(b) Demuestre que $A \Delta B = (A - B) \cup (B - A)$

(c) Pruebe que la diferencia simétrica es conmutativa

(d) Pruebe que $A \Delta B = A \cup B - (A \cap B)$

(e) Usando diagrama de Venn y luego prescindiendo de ellos, halle $A \Delta \Phi$, $A \Delta A$ y $A \Delta B$ si $A \subseteq B$.

(8) ¿En qué caso $A \times B$ es igual a $B \times A$?

(9) Sea $A = \{2, 3\}$, $B = \{0, 1\}$ y $C = \{1\}$. Halle y represente gráficamente los siguientes conjuntos: $A \times B$, $B \times (A \cup C)$, $(A \times B) \cup (A \times C)$, $A \times (B \cup C)$, $(A \times C) \cap (A \times B)$, $A \times (B \cup C)$.

(10) ¿Qué es $[0] \times \{x, y\}$, donde x y y son números reales?

(11) Si A es un conjunto cualesquiera, ¿qué es $A \times \{ \}$?

Nota: Recuerde que $\{ \} = \Phi =$ conjunto vacío.

(12) (a) Represente gráficamente $[-2, 3] \times [-4, -1]$

(b) Idee una representación de $(-2, 3) \times [-3, -1]$

(c) ¿Cuál sería la gráfica de $\{2\} \times (1, +\infty)$?

(d) Idem. de $\mathbb{R} \times \{3\}$.

(13) Represente gráficamente:

(a) $(-\infty, 2] \times (1, +\infty)$

(d) $(1, 3] \times [-2, +\infty)$

(b) $[2, +\infty) \times (1, +\infty)$

(e) $(-\infty, 2] \times [-1, 3]$

(c) $[-2, 3] \times \mathbb{R}$

(f) $\mathbb{R} \times (-1, 3)$

(14) Demuestre que

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

y que

$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

§5. RELACIONES Y FUNCIONES

Sean A y B dos conjuntos de un universo dado, y consideremos su producto cartesiano $A \times B$. Todo subconjunto de $A \times B$ es llamado una relación de A en B . Puesto que $\Phi \subseteq A \times B$ entonces el vacío Φ es también una relación de A en B , lo mismo puede decirse de $A \times B$ que es una relación de A en B .

EJEMPLO. $A = \{a, b, c\}$, $B = \{1, 2, 3\}$

$$R_1 = \{(a, 1), (a, 2), (b, 2), (b, 3), (c, 1)\}$$

$$R_2 = \{(a, 1)\}, \quad R_3 = \{(a, 1), (a, 2), (a, 3)\}$$

son relaciones de A en B .

5.1 DEFINICIÓN. Sea R una relación de A en B , el conjunto

$$D_R = \{a \in A / (\exists b \in B)((a, b) \in R)\}$$

es llamado el *dominio* de la relación.

De otra manera el conjunto de todos los primeros elementos de las parejas que forman a R es llamado dominio de la relación.

5.2 DEFINICIÓN. Sea Λ una relación de A en B . El conjunto B es llamado *codominio* de la relación y el conjunto

$$Rec_\Lambda = \{b \in B / (\exists a \in A)((a, b) \in \Lambda)\}$$

es llamado el *recorrido* de la relación. Es decir el recorrido es el conjunto de todos los segundos elementos de las parejas ordenadas que forman la relación.

EJEMPLO. En el ejemplo anterior se tiene

$$Rec_{R_1} = \{1, 2, 3\}$$

$$D_{R_1} = \{a, b, c\}$$

$$Rec_{R_2} = \{1\}$$

$$D_{R_2} = \{a\}$$

$$Rec_{R_3} = \{1, 2, 3\} \quad D_{R_3} = \{a\}.$$

5.3 DEFINICIÓN. Sea R una relación de A en B se dice que R es una relación *funcional* (ó gráfica funcional) si

- (i) El dominio de R es A
- (ii) La siguiente proposición es siempre verdadera
 $(\forall x)(\forall y)(\forall z)((x, y) \in R \wedge (x, z) \in R \Rightarrow y = z).$

EJEMPLOS (1) $\{(x, y)/y = \sqrt{1 - x^2}\} \subseteq [-1, 1] \times \mathbb{R}$ es una relación funcional de $[-1, 1]$ en \mathbb{R} mientras que

$$G = \{(x, y)/x^2 + y^2 = 1\}$$

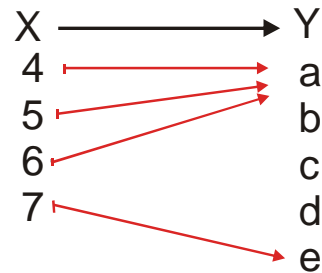
no lo es , ya que $(0, 1)$ y $(0, -1)$ son elementos de G y no se cumple la condición (ii) de la definición.

(2) Sean $X = \{4, 5, 6, 7\}$ y $Y = \{a, b, c, d, e\}$ $f = \{(4, a), (5, a), (6, a), (7, e)\}$ es una relación funcional, mientras que $F = \{(4, a), (5, b), (6, d)\}$ no lo es ya que $D_F \neq X$.

5.4 NOTACIÓN. Cuando f es una relación funcional, $(x, y) \in f$ se acostumbra escribir $y = f(x)$. También, " f es una función de X en Y " se escribe

$$f : X \longrightarrow Y \quad \text{ó} \quad X \xrightarrow{f} Y$$

La función f descrita en el ejemplo (2) se puede escribir entonces en la forma



Así, la condición (i) dada al comienzo significa: de todo elemento de X sale una flecha y la condición (ii) de ningún elemento de X salen dos o más flechas. Es de notar que a un elemento de Y pueden llegar varias flechas o ninguna.

5.5 DEFINICIÓN. Sea X un conjunto de un universo dado, se llama *diagonal* de X al conjunto

$$\Delta_X = \{(x, x)/x \in X\}$$

EJEMPLO. Si $X = \{a, b, c\}$ entonces $\Delta_X = \{(a, a), (b, b), (c, c)\}$

5.6 DEFINICIÓN. Sean X e Y conjuntos, sea $G \subseteq X \times Y$ una gráfica o relación. Se llama gráfica inversa de G al conjunto

$$G^{-1} = \{(x, y)/(y, x) \in G\} \subseteq Y \times X$$

5.7 DEFINICIÓN. Sean $G_1 \subseteq X \times Y$ y $G_2 \subseteq Y \times Z$. se llama gráfica compuesta por G_1 y G_2 y se nota $G_2 \circ G_1$ al conjunto

$$\{(x, z)/(\exists y \in Y)((x, y) \in G_1 \wedge (y, z) \in G_2)\}$$

nótese que $G_2 \circ G_1 \subseteq X \times Z$.

EJEMPLO. (1) Sea $X = \{1, 2, 3\}$; $Y = \{a, b\}$; $Z = \{a, *\}$ consideremos

$$G_1 = \{(1, a), (2, a), (1, b), (3, b)\}$$

$$G_2 = \{(a, \diamond), (a, *)\}$$

$$G_3 = \{(b, *)\}$$

entonces

$$G_2 \circ G_1 = \{(1, \diamond), (1, *), (2, \diamond), (2, *)\} \text{ y } G_3 \circ G_1 = \{(1, *), (3, *)\}$$

(2) Sean $G_1 = \{(x, y)/x \in \mathbb{R} \wedge y = x^2\}$, $G_2 = \{x \in \mathbb{R} \wedge y = \sin x\}$

entonces

$$G_2 \circ G_1 = \{(x, y)/x \in \mathbb{R} \wedge y = \sin x^2\}.$$

Podemos ahora preguntarnos ¿si al componer dos gráficos funcionales se obtiene un gráfico funcional?, la respuesta es si. Más exactamente tenemos.

5.8 PROPOSICIÓN. Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ dos funciones entonces $g \circ f : X \longrightarrow Z$ es una función

DEMOSTRACIÓN. (i) Como f es función se tiene la veracidad de la siguiente proposición

$$(\forall x \in X)(\exists! y \in Y)((x, y) \in f)$$

y como g es también función para cada $y \in Y$ habrá un elemento $z \in Z$ tal que $(y, z) \in g$. Entonces ligando estas dos afirmaciones tenemos que

$$(\forall x \in X)(\exists z \in Z)((x, z) \in g \circ f) \Rightarrow X \subseteq D(g \circ f) \subseteq X$$

entonces se tiene que

$$D(g \circ f) = X$$

(ii) Tomemos $(x, z) \in g \circ f \wedge (x, z') \in g \circ f$ entonces

$$[(\exists y \in Y)((x, y) \in f \wedge (y, z) \in g)] \wedge [(\exists y' \in Y)((x, y') \in f \wedge (y', z') \in g)]$$

de la asociatividad de la conjunción se desprende que

$$[(x, y) \in f \wedge (x, y') \in f] \wedge [(y, z) \in g \wedge (y', z') \in g]$$

Como f es una función cumple el axioma (ii) por lo tanto

$$y = y' \wedge [(y, z) \in g \wedge (y', z') \in g]$$

ahora como g es funcional cumple también (ii) de donde

$$z = z'$$

Así como $g \circ f$ cumple (i) y (ii) de la definición de función se sigue que $g \circ f$ es una función de X en Z . En este caso es costumbre escribir $(x, z) \in g \circ f$ en la forma $z = (g \circ f)(x)$, ó, $z = g(f(x))$.

□

5.9 EJERCICIOS

(1) Halle las gráficas inversas de

$$F = \{(x, y)/x \in \mathbb{R} - \{0\} \wedge y = \frac{1}{x}\}; G = \{(x, y)/x \in \mathbb{R} \wedge y = \sin x\}$$

(2) Sean G_1 y G_2 gráficas de X en Y demuestre que

(a) Si $G_1 \subseteq G_2$ entonces $G_1^{-1} \subseteq G_2^{-1}$

(b) $(G_1^{-1})^{-1} = G_1$

(3) ¿ Que relación encuentra entre dominio G , recorrido de G , dominio de G^{-1} y recorrido de G^{-1} ?

(4) ¿La relación " x es profesor de y " es una función? ¿Lo sería la relación " x es alumno de y " ?.

(5) Halle dominio y recorrido de la relación " x es hijo de y " . ¿ es una función?. Reflexione antes de responder.

(6) Sean $A = \{0, 5, 7, 4\}$ y $B = \{1, 2, 3\}$ dos conjuntos. Defina cuatro funciones de A en B y cuatro de B en A .

(7) Dadas las funciones

(a) $f(x) = \frac{1}{x+2}$ (b) $g(x) = 1 - 2x^2$ (c) $F(x) = 2x + 3$

(d) $G(x) = -\sqrt{\frac{2}{3x} + 3}$ (e) $b(x) = \sqrt{\frac{x+1}{x+2}}$

(f) $u(z) = z^2 - 2$ (g) $v(x) = \frac{x^2}{x+2}$

i) Calcule su valor en el número real 1.

ii) Halle los números $f(8), g(1.5), b(\frac{1}{5}), F(0), G(-3), u(6), u(0), u(-5), v(3)$, y $v(0)$.

iii) Halle el dominio y el recorrido de cada una de ellas

(8) Consideremos las siguientes funciones:

(a) $\mathbb{R} \xrightarrow{F} \mathbb{R}$ (b) $\mathbb{R} \xrightarrow{c_3} \mathbb{R}$ (c) $\mathbb{R} \xrightarrow{g} \mathbb{R}$
 $x \mapsto x^2 - 5$ $x \mapsto 3$ $x \mapsto x^3$

(d) $\mathbb{R} \xrightarrow{id} \mathbb{R}$ (e) $\mathbb{R} \xrightarrow{s} \mathbb{R}$ (f) $\mathbb{R} \xrightarrow{L} \mathbb{R}$
 $x \mapsto id(x) = x$ $x \mapsto -x$ $x \mapsto 3x + 2$

$$\mathbb{R} \xrightarrow{\text{abs}} \mathbb{R}$$

$$(g) \quad x \mapsto x \text{ si } x \geq 0$$

$$x \mapsto -x \text{ si } x < 0$$

es decir, $\text{abs}(x) = x$ si $x \geq 0$ y si $x < 0$, $\text{abs}(x) = -x$ (Se llama valor absoluto de x , en lugar de $\text{abs}(x)$ se acostumbra escribir $|x|$)

(i) Halle $c_3(0)$, $c_3(-1)$, $c_3(10)$, $g(-1)$, $\text{id}(2)$, $\text{id}(-3)$, $L(2)$, $L(-5)$, $s(2)$, $s(0)$, $\text{abs}(-2)$, $\text{abs}(2)$, $\text{abs}(0)$, $|-1 - |0||$.

(ii) Halle el recorrido de cada una de las funciones inmediatamente anteriores.

§6. CLASES DE FUNCIONES

6.1 DEFINICIÓN. Sea $f : X \longrightarrow Y$ una función. Si el recorrido de f es todo Y , entonces f se llama *sobreyectiva* o una epiyección o simplemente f es una función de X sobre Y .

Puede también decirse en forma equivalente, que $f : X \longrightarrow Y$ es una función *sobre* cuando la siguiente proposición es verdadera

$$(\forall y \in Y)(\exists x \in X)(y = f(x))$$

6.2 DEFINICIÓN. Sea $f : X \longrightarrow Y$ una función. Se dice que f es una función uno a uno ó una *inyección* si la siguiente proposición es verdadera

$$(\forall x)(\forall y)(f(x) = f(y) \Rightarrow x = y)$$

Esta proposición es claramente equivalente a

$$(\forall x)(\forall y)(x \neq y \Rightarrow f(x) \neq f(y)).$$

EJEMPLO. (1) $\{(x, y)/x \in \mathbb{R} \wedge y = x^3\}$ es una función uno a uno de \mathbb{R} sobre \mathbb{R}
 (2) $f = \{(x, y)/x \in \mathbb{R} \wedge y = 2^x\}$ es una función uno a uno de \mathbb{R} en \mathbb{R} . No es sobre, pues el recorrido de f no contiene al cero ni a los números negativos. Se puede volver sobre tomando $X = \mathbb{R}$ e $Y = \mathbb{R}_+$ = números reales positivos. Así

$$f: X \longrightarrow Y$$

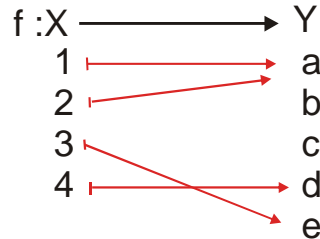
$$x \mapsto 2^x$$

es uno a uno y sobre.

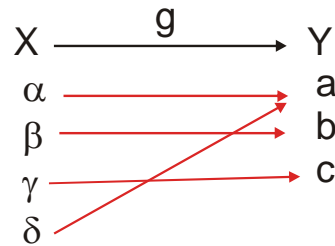
Una función que a la vez es una inyección y una epiyección se le llama una *biyección*.

6.3 FUNCIÓN INVERSA

Sea $f : X \rightarrow Y$ una función. Sabemos que $f^{-1} = \{(y, x) / (x, y) \in f\}$ es una gráfica inversa, nos preguntamos ¿en que caso f^{-1} es una función? Veamos antes algunos ejemplos.



o sea $f = \{(1, a), (2, b), (3, e), (4, d)\}$, la gráfica inversa es $f^{-1} = \{(a, 1), (b, 2), (e, 3), (d, 4)\}$. Analizando el dominio de f^{-1} , vemos que $D_{f^{-1}} \neq Y$. Luego f^{-1} no puede ser función ¿la causa? puesto que $\text{Recorrido de } f \neq \text{Dominio de } f^{-1}$; tenemos que f no es sobre. Consideremos otro caso dado por



o sea $g = \{(\alpha, a), (\beta, b), (\gamma, c), (\delta, a)\}$ entonces su gráfica inversa será

$$g^{-1} = \{(a, \alpha), (b, \beta), (c, \gamma), (a, \delta)\}$$

puesto que $\alpha \neq \delta$ y $(a, \alpha) \in g^{-1}, \wedge (a, \delta) \in g^{-1}$, se sigue que g^{-1} no es función ¿la causa? g no es uno a uno.

Estos ejemplos nos dicen que si f no es uno a uno ó f no es sobre entonces f^{-1} no es una función. Es decir, si f^{-1} es función, entonces f debe ser uno a uno y sobre. Como $f = (f^{-1})^{-1}$ es una función entonces f^{-1} es también uno a uno y sobre.

En este caso, para todo $x \in X$ existe $y \in Y$ tal que $(x, y) \in f \wedge (y, x) \in f^{-1}$ de donde $(x, x) \in f^{-1} \circ f$ por lo tanto $x = (f^{-1} \circ f)(x) = \Delta_X(x)$ luego $f^{-1} \circ f = \Delta_X = \text{diagonal de } X$.

Análogamente, para todo $y \in Y$ existe $x \in X$ tal que $(y, x) \in f^{-1} \wedge (x, y) \in f$ entonces $(y, y) \in f \circ f^{-1}$ entonces $y = (f \circ f^{-1})(y) = \Delta_Y(y)$ luego

$$f \circ f^{-1} = \Delta_Y = \text{diagonal de } Y.$$

En forma de diagonal

$$\begin{array}{ccc} X \longrightarrow Y \longrightarrow X & & Y \longrightarrow X \longrightarrow Y \\ x \mapsto f(x) \mapsto f^{-1}(f(x))=x & & y \mapsto f^{-1}(y) \mapsto f(f^{-1}(y))=y \\ \underbrace{\hspace{10em}}_{\Delta_X} & & \underbrace{\hspace{10em}}_{\Delta_Y} \end{array}$$

6.4 DEFINICIÓN. Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow X$ funciones, se dice que f y g son funciones inversas si

$$g \circ f = \Delta_X \quad \text{y} \quad f \circ g = \Delta_Y$$

Las ideas anteriores quedan resumidas en el siguiente teorema

6.5 TEOREMA. Sea $f : X \longrightarrow Y$ una función, f tiene función inversa si y sólo si f es uno a uno y sobre.

DEMOSTRACIÓN. (a) " \Rightarrow " Sea f una función y g su inversa

$$\text{Si } f(x) = f(x') \text{ entonces } g(f(x)) = g(f(x'))$$

$$\text{o sea } (g \circ f)(x) = (g \circ f)(x') \text{ entonces } \Delta_X(x) = x = x' = \Delta_X(x')$$

Luego f es uno a uno

Ahora como g es función se tiene $(\forall y \in Y)(\exists x \in X)(g(y) = x)$ entonces

$$f(g(y)) = f(x) = (f \circ g)(y) = \Delta_Y(y) = y$$

Luego $(\forall y \in Y)(\exists x \in X)(f(x) = y)$ así f es sobre.

(b) " \Leftarrow " Supongamos que f es uno a uno y sobre entonces

$$(\forall y \in Y)(\exists x \in X)(f(x) = y)$$

pero éste x es único ya que f es uno a uno. Si llamamos

$$g = \{(y, x) / y = f(x)\}$$

g es una función de Y en X y evidentemente $g = f^{-1}$ ya que:

$$(g \circ f)(x) = g(f(x)) = g(y) = x = \Delta_X(x)$$

$$(f \circ g)(y) = f(g(y)) = f(x) = y = \Delta_Y(y).$$

□

6.6 ALGUNAS PROPIEDADES DE LAS FUNCIONES

6.6.1 DEFINICIÓN. Sea $f : X \longrightarrow Y$ una función, y $A \subseteq X$, llamamos $f(A)$ al conjunto de las *imágenes* de los elementos de A

$$f(A) = \{f(x) / x \in A\}$$

Notacionalmente $p \in f(A) \Leftrightarrow (\exists x \in A)(f(x) = p)$.

6.6.2 PROPOSICIÓN. Sean $f : X \longrightarrow Y$ una función, $A \subseteq X \wedge B \subseteq X$. Las siguientes proposiciones son verdaderas

$$(a) f(A \cup B) = f(A) \cup f(B)$$

$$(b) f(A \cap B) \subseteq f(A) \cap f(B)$$

DEMOSTRACIÓN. Usando tipo de demostración directa tenemos:

$$\begin{aligned}
 (a) \quad & p \in f(A \cup B) \Leftrightarrow (\exists x \in A \cup B)(f(x) = p) \Leftrightarrow (\exists x)(x \in A \cup B \wedge f(x) = p) \Leftrightarrow \\
 & \Leftrightarrow (\exists x)((x \in A \vee x \in B) \wedge f(x) = p) \Leftrightarrow (\exists x)((x \in A \wedge f(x) = p) \vee (x \in B \wedge f(x) = p)) \\
 & \Leftrightarrow (p \in f(A) \vee p \in f(B)) \Leftrightarrow p \in f(A) \cup f(B) \\
 (b) \quad & p \in f(A \cap B) \Leftrightarrow (\exists x)(x \in A \cap B \wedge f(x) = p)
 \end{aligned}$$

entonces

$$(\exists x)(x \in A \wedge x \in B \wedge f(x) = p)$$

entonces

$$(\exists x)([x \in A \wedge f(x) = p] \wedge [x \in B \wedge f(x) = p])$$

entonces

$$p \in f(A) \wedge p \in f(B)$$

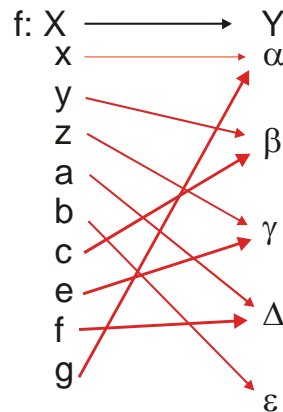
de donde

$$p \in f(A) \cap f(B)$$

□

La igualdad de (b) no se tiene en general como lo podemos apreciar en el siguiente ejemplo

EJEMPLO. Sea $X = \{x, y, z, a, b, c, e, f, g\}$, $Y = \{\alpha, \beta, \gamma, \Delta, \epsilon\}$, $A = \{x, y, g\}$, $B = \{a, b, c, g\}$ y consideremos la función dada por



tenemos $f(A) = \{\alpha, \beta\}$, $f(B) = \{\Delta, \epsilon, \alpha, \beta\}$, $f(A) \cap f(B) = \{\alpha, \beta\}$, $A \cap B = \{g\}$ y $f(A \cap B) = \{\alpha\}$, de aquí tenemos

$$f(A \cap B) = \{\alpha\} \subset \{\alpha, \beta\} = f(A) \cap f(B)$$

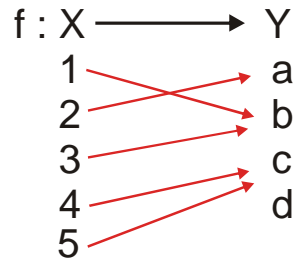
6.6.3 DEFINICIÓN: Sean $f : X \longrightarrow Y$ y $D \subseteq Y$; se llama *imagen recíproca* de D por f al conjunto

$$f^{-1}(D) = \{x \in X / f(x) \in D\}$$

En el lenguaje de la teoría de conjuntos tenemos

$$p \in f^{-1}(D) \Leftrightarrow f(p) \in D$$

EJEMPLO. Sea la función



entonces $f^{-1}(\{b, c, d\}) = \{1, 3, 4, 5\}$, $f^{-1}(\{d\}) = \Phi$, $f^{-1}(\{c\}) = \{4, 5\}$. Es evidente que $f^{-1}(Y) = X$.

6.6.4 PROPOSICIÓN. Sea $f : X \longrightarrow Y$ una función $C \subseteq Y$ y $D \subseteq Y$ entonces $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

DEMOSTRACIÓN. Sea $x \in f^{-1}(C \cup D) \Leftrightarrow f(x) \in C \cup D \Leftrightarrow f(x) \in C \vee f(x) \in D \Leftrightarrow x \in f^{-1}(C) \vee x \in f^{-1}(D) \Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D)$.

□

6.6.5 PROPOSICIÓN. Sea $f : X \longrightarrow Y$ una función y sea $A \subseteq X$. Entonces tenemos

- (a) $f^{-1}(f(A)) \supseteq A$
- (b) Si f es uno a uno, $f^{-1}(f(A)) \subseteq A$

DEMOSTRACIÓN. (a) Sea $x \in A$ entonces $f(x) \in f(A)$ usando la definición de imágenes recíprocas se tiene $x \in f^{-1}(f(A))$

(b) Sea $x \in f^{-1}(f(A))$ entonces $f(x) \in f(A)$ teniéndose que

$$(\alpha) x \notin A \quad \vee \quad (\beta) x \in A$$

Veamos que (α) es falsa, en esta forma (β) es verdadera y quedará la proposición demostrada.

Si $x \notin A$, como $y = f(x) \in f(A)$ deberá existir por definición de $f(A)$, un elemento $x' \in A$ tal que $f(x') = y \in f(A)$ entonces $f(x) = f(x')$ y $x \neq x'$ esto implica que f no es uno a uno lo cual está contra la hipótesis de que f es uno a uno

□

6.7 EJERCICIOS

(1) Hallar las funciones inversas de

$$\begin{array}{lll}
 (a) \mathbb{R} \longrightarrow \mathbb{R} & (b) \mathbb{R} \longrightarrow \mathbb{R}_+ & (c) \mathbb{R}_+ \longrightarrow \mathbb{R}_+ \\
 x \mapsto x^3 & x \mapsto 2^x & x \mapsto x^2
 \end{array}$$

(2) Demuestre que si f es uno a uno entonces $f(A) \cap f(B) \subseteq f(A \cap B)$ con lo cual la parte (b) de 6.6.2 se tendría $f(A) \cap f(B) = f(A \cap B)$

(3) Demuestre que $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

- (4) Sea $f : X \longrightarrow Y$ y sea $D \subseteq Y$. Demuestre que
- $f(f^{-1}(D)) \subseteq D$
 - Si f es sobre $f(f^{-1}(D)) = D$
- (5) Pruebe que una restricción de una función $f : A \longrightarrow B$ se puede definir simplemente como una función $g : C \longrightarrow D$ tal que $g \subseteq f$ y $D \subseteq B$
- Nota: $g \subseteq f$ significa que $(x, y) \in g \Rightarrow (x, y) \in f$ es decir, $\forall x \in \text{Dom}(g)(g(x) = f(x))$
- (6) (a) Si A es un conjunto con diez elementos y B un único elemento, halle todas las funciones de A en B .
- (b) Halle todas las funciones de un conjunto A con tres elementos, en otro con dos elementos.
- (c) Halle todas las funciones de un conjunto A con cuatro elementos en otro B con dos elementos.
- (d) Podría hallar una fórmula para calcular el número de funciones de un conjunto A con n elementos en otro B con m elementos. ¿Podría justificar dicha fórmula?
- (7) Dada la función $f(x) = x^2 + 2x - 8$ de \mathfrak{R} en \mathfrak{R} ,
- Halle su recorrido.
 - Restrinja el codominio de f para obtener una función sobreyectiva.
 - Sin variar el codominio de la función en (b), halle una restricción biyectiva que sea continua.
 - Halle gráfica y algebraicamente la función inversa de la restricción hallada en (c).
- (8) Si $f : A \longrightarrow B$ y $g : C \longrightarrow D$ son biyecciones, demuestre que la función inversa de $g \circ f$ es $f^{-1} \circ g^{-1}$.
- (9) Sean $f : A \longrightarrow B$ biyectiva, f^{-1} su inversa y N un subconjunto de B . Pruebe que la imagen recíproca f^{-1} es igual a la imagen directa de N por medio de la función inversa f^{-1} .

§ 7. LEYES DE COMPOSICIÓN INTERNA (OPERACIONES)

7.1 DEFINICIÓN: Sea E un conjunto. Una función T de $E \times E$ en E

$$T : E \times E \longrightarrow E$$

se llama una *ley de composición interna* definida en toda parte de E ó una operación binaria definida en todo E .

En adelante, siempre que digamos ley de composición definida en E , se entenderá definida en toda parte de E . Se acostumbra notar $T(x, y)$ en la forma xTy .

EJEMPLOS 1. Una ley de composición interna es la suma de números naturales

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$(m, n) \mapsto +(m, n) = m + n$$

es decir,

$$+ = \{((m, n), m + n) / m \in \mathbb{N} \wedge n \in \mathbb{N}\}$$

2. La suma común y corriente de números reales

$$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

$$(x, y) \mapsto (x, y) = x + y$$

es claramente una ley de composición interna en \mathbb{R} .

Nótese que los ejemplos (1) y (2) son diferentes, aún cuando se notan las funciones con el mismo signo.

3. Sea $E = \{a, b\}$ consideremos $T = \{((a, a), a), ((a, b), b), ((b, a), a), ((b, b), a)\}$ se obtiene que T es una ley de composición interna en E ; también se acostumbra escribir en la forma

$$aTa = a, aTb = b, bTa = a \quad \text{y} \quad bTb = a$$

ó en un cuadrado de la forma

T	a	b
a	a	b
b	a	a

Así si se quiere hallar xTy , deberá tomarse x sobre la primera columna de la izquierda y y sobre la primera fila y el resultado está en el cruce de la fila con la columna correspondiente.

4. Sea E el conjunto de todas las proposiciones. Decimos que dos proposiciones son iguales, si son equivalentes, es decir $p = q$ significa p es verdadera si y sólo si q es verdadera.

Entonces $\wedge : E \times E \longrightarrow E$ (la conjunción entre proposiciones)

$$(p, q) \mapsto p \wedge q$$

es una ley de composición interna en E .

5. Sea E como en el ejemplo 4. la implicación de dos proposiciones

$$\Rightarrow : E \times E \longrightarrow E$$

$$(p, q) \mapsto p \Rightarrow q$$

es una ley de composición interna.

6. Sea X un conjunto y denotemos con $\mathcal{P}(X)$ al conjunto formado con todos los subconjuntos de X , también llamado partes de X . La reunión es una ley de composición interna definida en $\mathcal{P}(X)$

$$\cup : \mathcal{P}(X) \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$$

$$(A, B) \mapsto A \cup B$$

7.
$$* : \mathbb{R}_+ \times \mathbb{R}_+ \longrightarrow \mathbb{R}_+$$

$$(x, y) \mapsto x * y = x^y$$
 la exponenciación definida en los números reales positivos es una ley de composición interna definida en toda parte de \mathbb{R}_+ . Si en lugar de \mathbb{R}_+ se toma \mathbb{R} , no se tendría definida una ley de composición definida en toda parte de \mathbb{R} ya que $x^{\frac{1}{2}}$ no es real cuando $x < 0$.

8. Sea X un conjunto no vacío. Sea \mathfrak{F} el conjunto de todas las funciones de X en X ($\mathfrak{F} = \{f/f : X \longrightarrow X\}$)

$$\circ : \mathfrak{F} \times \mathfrak{F} \longrightarrow \mathfrak{F}$$

$$(f, g) \mapsto f \circ g$$

la composición usual entre funciones, es una ley de composición interna en \mathfrak{F} .

7.1.2 EJERCICIOS

(1) Sea \mathbb{R} el conjunto de los números reales

$$- : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

$$(x, y) \mapsto x - y$$

la diferencia entre números reales, se pregunta ¿es $-$ una ley de composición interna definida en toda parte de \mathbb{R} ?

(2) Sea E un conjunto cualquiera y $\alpha \in E$. ¿ Son

$$\perp : E \times E \longrightarrow E$$

$$(x, y) \mapsto x \perp y = x$$

$$, T : E \times E \longrightarrow E$$

$$(x, y) \mapsto xTy = \alpha$$

leyes de composición definidas en toda parte de E ?

(3) Consideremos $\div : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ la división en \mathbb{R} entonces \div

$$(x, y) \mapsto x \div y$$

no es una ley de composición interna definida en toda parte de \mathbb{R} ¿por qué?

7.2 CLASES DE LEYES DE COMPOSICIÓN

(a) Una ley de composición $T : E \times E \longrightarrow E$ se llama **asociativa** si y sólo si

$$(\forall a \in E)(\forall b \in E)(\forall c \in E)((aTb)Tc = aT(bTc))$$

Se puede probar fácilmente que las leyes de composición dadas en los ejemplos (1), (2), (3), (4), (6) y (8) anteriores son leyes asociativas. Así para (8), tenemos

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))), \quad \forall x \in X$$

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) \quad \forall x \in X$$

Como coinciden en todos los puntos de X se tiene

$$(f \circ g) \circ h = f \circ (g \circ h)$$

Las leyes de los ejemplos (5) y (7) no son asociativas, puesto que

$$[(p \Rightarrow q) \Rightarrow r] \neq [p \Rightarrow (q \Rightarrow r)]$$

puesto que si se toman proposiciones p, q, r todas falsas entonces $(p \Rightarrow q) \Rightarrow r$ resulta falsa pero $p \Rightarrow (q \Rightarrow r)$ es verdadera.

Ahora en (7) se tiene

$$(2*3)*2 = (2^3)^2 \neq 2^{(3^2)} = 2*(3*2)$$

(b) Una ley de composición T se llama **conmutativa** si

$$(\forall x \in E)(\forall y \in E)(xTy = yTx)$$

Las operaciones binarias de los ejemplos (1), (2), (4) y (6) anteriores son conmutativas, mientras que (3), (5), (7), (8) no son conmutativas. Así en (3) $aTb = b \neq a = bTa$, en (5) $p \Rightarrow q \neq q \Rightarrow p$ en muchos casos, en (7) $2^3 \neq 3^2$ y en (8) $f \circ g \neq g \circ f$ en general

(c) Una ley de composición binaria T en E se llama **modulativa** si existe $e \in E$ tal que

$$(\forall x \in E)(eTx = xTe = x)$$

e es llamado el módulo de T .

EJEMPLOS. (1) $\cdot : \mathfrak{R} \times \mathfrak{R} \longrightarrow \mathfrak{R}$ el producto de números reales es modulativo pues, $(x, y) \mapsto x \cdot y$
 $(\forall x \in \mathfrak{R})(x \cdot 1 = 1 \cdot x = x)$

(2) Si suponemos que cero es un número natural entonces la suma de números naturales es modulativa pues; $(\forall n \in \mathbb{N})(0 + n = n + 0 = n)$

(3) Para la suma entre números reales el cero también es el módulo; en el conjunto $\mathcal{P}(X)$ partes de X el conjunto vacío es el módulo para la unión de conjuntos pues, $(\forall A \in \mathcal{P}(X))(A \cup \Phi = \Phi \cup A = A)$; en el conjunto \mathfrak{F} de todas las funciones definidas sobre un conjunto X la aplicación idéntica de X , ó la diagonal de X es el módulo para la composición de funciones pues, $(\forall f \in \mathfrak{F})(f \circ \Delta_X = \Delta_X \circ f = f)$

Claramente los ejemplos (3), (4) y (5) de la sección 7.1 no son modulativos lo mismo que (7) ya que $1^X \neq X^1 = X$.

(d) Una operación T en E modulativa, se llama **invertiva** si

$$(\forall x \in E)(\exists x' \in E)(xTx' = x'Tx = e)$$

donde e es el módulo de E para T .

EJEMPLOS. (1) El ejemplo (1) del numeral 7.1 no es invertiva ya que no existe un número natural x' tal que $5 + x' = x' + 5 = 0$

(2) De la misma sección el ejemplo (2) es una ley invertiva; el ejemplo (6) es de una ley modulativa pero no es invertiva puesto que

$(\forall A \in \mathcal{P}(X))(A \cup \Phi = \Phi \cup A = A)$, pero dado $A \neq \Phi$ no existe un conjunto A' tal que $A \cup A' = A' \cup A = \Phi$ ya que $A \cup A' \supset A \neq \Phi$.

(3) La ley de composición dada en el ejemplo 8 de la sección 7.1 no es invertiva, pues si $f : X \rightarrow X$ es una función que no es ni uno a uno ni sobre, no existe f' tal que $f \circ f' = f' \circ f = \Delta_X$. Sin embargo en este conjunto se habla con frecuencia de funciones invertibles a la derecha ó a la izquierda. Ahora si se toma \mathfrak{M} como el conjunto de las funciones de X en X que son uno a uno y sobre ó sea de las biyecciones entonces

$$\begin{aligned} \circ : \mathfrak{M} \times \mathfrak{M} &\longrightarrow \mathfrak{M} \\ (f, g) &\mapsto f \circ g \end{aligned}$$

es una ley de composición invertible.

7.3 EJERCICIOS.

(1) Sea $S = \{par, impar\}$ y definamos en S una adición así:

$$\begin{aligned} S \times S &\longrightarrow S \\ (par, par) &\mapsto par + par = par \\ (par, impar) &\mapsto par + impar = impar \\ (impar, par) &\mapsto impar + par = impar \\ (impar, impar) &\mapsto impar + impar = par \end{aligned}$$

¿Es una operación esta adición? ¿en caso de serlo es modulativa e invertiva?

(2) ¿Es la operación resta entre números reales modulativa e invertiva?

(3) Busque dos ejemplos más de operaciones no conmutativas y dos de operaciones modulativas no invertivas.

(4) (a) En un conjunto de dos elementos, defina una operación asociativa y no conmutativa.

(b) ¿Conoce una operación asociativa y no conmutativa definida en un conjunto infinito?

(5) Definamos $a \odot b = (a + b) + (a \cdot b)$ siendo a y b números reales cualesquiera; demostrar que

(a) \odot es una operación

(b) \odot es conmutativa

(c) \odot es asociativa

(d) ¿Bajo qué condiciones \odot es modulativa?

(e) ¿Es \odot invertiva?

Nota: \odot es llamada *adiplicación*.

(6) Pruebe que para una operación modulativa, el módulo es único

(7) Demuestre que si $*$ es invertiva en S , entonces para un elemento cualquiera, su inverso es único.

§8. CONCEPTO DE GRUPO

8.1 DEFINICIÓN. Sea G un conjunto en el cual se ha definido una ley de composición interna T . G se llama un **grupo** para T , ó la dupla $\langle G, T \rangle$ se llama un **grupo**, si T es una ley de composición que es asociativa, modulativa e invertiva. Si además T es conmutativa, G se llama un grupo abeliano o conmutativo.

EJEMPLOS (1) $\langle \mathbb{R}, + \rangle$, es decir, los números reales con la suma son un grupo abeliano.

(2) $\langle \mathbb{R} - \{0\}, \cdot \rangle$ es un grupo abeliano, pues los axiomas de \mathbb{R} afirman que

$$(\forall a \in \mathbb{R} - \{0\})(\forall b \in \mathbb{R} - \{0\})(\forall c \in \mathbb{R} - \{0\})((a \cdot b) \cdot c = a \cdot (b \cdot c))$$

$$(\forall a \in \mathbb{R} - \{0\})(1 \cdot a = a \cdot 1 = a)$$

$$(\forall a \in \mathbb{R} - \{0\})(\exists a' \in \mathbb{R} - \{0\})(a \cdot a' = a' \cdot a = 1)$$

$$(\forall a \in \mathbb{R} - \{0\})(\forall b \in \mathbb{R} - \{0\})(a \cdot b = b \cdot a)$$

(3) Sea $\mathfrak{M} = \{f : X \longrightarrow X/f \text{ es uno a uno y sobre}\}$ donde $X \neq \Phi$, consideremos

$$\circ : \mathfrak{M} \times \mathfrak{M} \longrightarrow \mathfrak{M}$$

$$(f, g) \mapsto f \circ g$$

como ley de composición en \mathfrak{M} . Entonces $\langle \mathfrak{M}, \circ \rangle$ es un grupo no abeliano. Ya demostramos que la composición de funciones cualesquiera es asociativa, luego en particular en este caso se tiene la asociatividad. Como Δ_X es uno a uno y sobre, $\Delta_X \in \mathfrak{M}$, entonces se tiene que la composición es modulativa y también es invertiva.

(4) Sea $G = \mathbb{Z}/(2) = \mathbb{Z}/_{Pares} = \{\dot{0}, \dot{1}\}$ y considere la tabla

+	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{1}$
$\dot{1}$	$\dot{1}$	$\dot{0}$

la cual define en $\mathbb{Z}/(2)$ una operación, asociativa, modulativa ($\dot{0}$ es el módulo), invertiva ($\dot{0} + \dot{0} = \dot{0} \wedge \dot{1} + \dot{1} = \dot{0}$) y conmutativa, Luego $\langle \mathbb{Z}/(2), + \rangle$ es un grupo abeliano.

(5) Consideremos el plano euclidiano y en él un punto fijo P ; podemos rotar alrededor de P el plano un ángulo φ

$$-360^0 < \varphi < 360^0$$

ó mejor

$$-2\pi < \varphi < 2\pi$$

se mide en radianes. φ es considerado positivo cuando se rota en el sentido contrario al movimiento de las agujas del reloj, y negativo en el otro sentido. Una rotación del plano en un ángulo φ lo denotaremos R_φ y

es en realidad una aplicación del plano en si mismo, más aún es una función uno a uno del plano sobre si mismo. Sea

$$G = \{R_\varphi / R_\varphi \text{ es una rotación del plano}\}$$

Definimos en G la operación

$$\circ : G \times G \longrightarrow G \\ (R_\varphi, R_\psi) \mapsto R_\varphi \circ R_\psi = R_{\varphi+\psi}$$

Sabemos ya que \circ es asociativa, además tomando R_0 como módulo la ley es modulativa y como

$$R_\varphi \circ R_{-\varphi} = R_0 = R_{-\varphi} \circ R_\varphi \quad \forall R_\varphi$$

se sigue que la ley es invertiva. Claramente es conmutativa, luego $\langle G, \circ \rangle$ es un grupo abeliano.

(6) Sea Π un plano euclidiano con un sistema de coordenadas cartesianas. Sabemos que un punto P se determina dando sus coordenadas (x, y) . Identifiquemos entonces P con sus coordenadas (x, y) . Definimos una función

$$H_t : \Pi \longrightarrow \Pi$$

así

$$H_t((x, y)) = (tx, ty) \quad t \neq 0$$

Teniéndose que H_t es uno a uno, ya que

$$H_t((x, y)) = H_t((x_1, y_1)) \Leftrightarrow (tx, ty) = (tx_1, ty_1) \Leftrightarrow tx = tx_1 \wedge ty = ty_1$$

como $t \neq 0$ podemos simplificar para obtener

$$x = x_1 \wedge y = y_1 \Leftrightarrow (x, y) = (x_1, y_1)$$

H_t es sobre; puesto que dado $(x, y) \in \Pi$ entonces $(\frac{x}{t}, \frac{y}{t}) \in \Pi$ y se tiene que

$$H_t\left(\frac{x}{t}, \frac{y}{t}\right) = (x, y)$$

Sea ahora $H = \{H_t : \Pi \longrightarrow \Pi / t \in \mathfrak{R} - \{0\}\}$ y definimos en H la siguiente ley de composición

$$\circ : H \times H \longrightarrow H \\ (H_t, H_s) \mapsto H_t \circ H_s = H_{ts}$$

entonces resulta que \circ es asociativa y conmutativa en H , como se prueba fácilmente. Además H_1 es el módulo y

$$H_t \circ H_{\frac{1}{t}} = H_1 \quad \forall H_t$$

luego la ley es invertiva. Así $\langle H, \circ \rangle$ es un grupo abeliano llamado de las *homotecias* del plano.

(7) Sea Π un plano euclidiano, si $(x, y) \in \Pi$ y $a, b \in \mathfrak{R}$ definimos la aplicación $T_{a,b} : \Pi \longrightarrow \Pi$ como sigue:

$$T_{a,b}((x, y)) = (a + x, b + y)$$

Es fácil ver que $T_{a,b}$ es uno a uno y sobre. Considérese

$$\mathfrak{A} = \{T_{a,b} : \Pi \longrightarrow \Pi / a, b \in \mathfrak{R}\}$$

al conjunto de todas las posibles $T_{a,b}$, y definamos en \mathfrak{A} la siguiente ley de composición

$$\begin{aligned} \circ : \mathfrak{P} \times \mathfrak{P} &\longrightarrow \mathfrak{P} \\ (T_{a,b}, T_{c,d}) &\mapsto T_{a,b} \circ T_{c,d} = T_{a+c,b+d} \end{aligned}$$

la cual resulta asociativa y conmutativa en \mathfrak{P} como fácilmente se puede verificar, $T_{0,0}$ es el módulo, además como

$$T_{a,b} \circ T_{-a,-b} = T_{0,0} \quad \forall T_{a,b}$$

entonces la ley es también inversible, así $\langle \mathfrak{P}, \circ \rangle$ es un grupo abeliano llamado el grupo de las **translaciones**.

8.2 EJERCICIOS

(1). Demuestre que $H_s \circ H_t = H_{st}$, donde H_t se define como en el ejemplo (6) de la anterior sección.

(2) Dé una interpretación geométrica a los efectos producidos en el plano por las homotecias y las translaciones.

(3) En el conjunto cociente $\mathbb{Z}/(k) = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{k-1}\}$ definimos una relación muy especial dada por

$$\begin{aligned} \mathbb{Z}/(k) \times \mathbb{Z}/(k) &\longrightarrow \mathbb{Z}/(k) \\ (\bar{a}, \bar{b}) &\mapsto \overline{a+b} \end{aligned}$$

Demuestre que esta relación es una ley de composición en $\mathbb{Z}/(k)$ y que esta operación hace de $\mathbb{Z}/(k)$ un grupo conmutativo.

NOTA. Este ejercicio es una generalización del ejemplo (4) de la sección anterior, donde se ha definido una operación análoga en el conjunto cociente $\mathbb{Z}/(2)$.

(4) Pruebe que el conjunto E es el módulo de la operación " \cap " definida en $P(E) = \{N/N \subseteq E\}$ pero que ningún subconjunto propio de E tiene inverso para ella. ¿Es " \cap " cancelativa?

(5) Demuestre que $\langle P(E), \cup \rangle$ no es grupo. ¿Es la unión cancelativa?

(6) Defina una nueva operación entre subconjuntos de E llamada la **diferencia simétrica**:

$$A \Delta B = \{x \in E / x \in A \vee x \in B\}.$$

Teniéndose en cuenta la tabla de verdad del "o" exclusivo (§1) y la tautología $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ (verifíquelo primero), pruebe que:

(a) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$

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

(c) La diferencia simétrica es modulativa, dando el módulo explícitamente.

(d) " Δ " es invertiva en $P(E)$.

(e) $\langle P(E), \Delta \rangle$ es un grupo conmutativo.

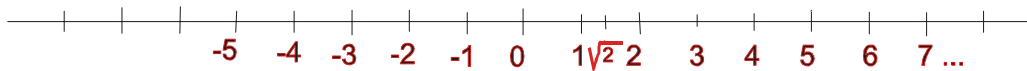
(f) La intersección es distributiva con respecto a la diferencia simétrica.

(9) ¿La operación $a \triangleright b = a \cdot b + a$ entre números reales es asociativa?

§9. LOS NÚMEROS REALES

9.1 En épocas pasadas bastaban al hombre, para sus necesidades referentes a conteos y mediciones, los llamados números naturales $1, 2, \dots$. En cambio hoy en día no es demasiado exigir que un estudiante de secundaria esté acostumbrado a manejar números como, $0, 1, -2, 13, -\frac{3}{4}, -31, 42, -\frac{17}{431802}, 2, \pi, (\sqrt{3})^{-\sqrt{5}}, e, \dots etc,$

los cuales manejan en calculadoras y computadores, y que son llamados "números reales", aunque, por otra parte, no se sepa qué son en última instancia; es decir, que nunca se haya o lo hayan enfrentado con la pregunta ¿qué es un número real? . En lo que sigue se usarán sin comentario previo, algunos de los hechos más elementales relativos a estos números; entre ellos su representación geométrica por medio de los puntos de una recta



a cada punto de dicha recta ("recta real", ó, "recta numérica") le corresponde un número, y sólo uno, y a cada número un punto, y sólo uno, de la recta. En todo caso, y con el objeto de representar los conceptos, se enunciarán a continuación las propiedades características de los números reales, los cuales se llamarán en adelante, salvo que se advierta lo contrario, simplemente números.

El filósofo griego Pitágoras (hacia el 600 a.C.) sabía ya que la razón $r = \frac{d}{l}$ entre la longitud de la diagonal de un cuadrado (d) y la longitud l de su lado, satisface la igualdad

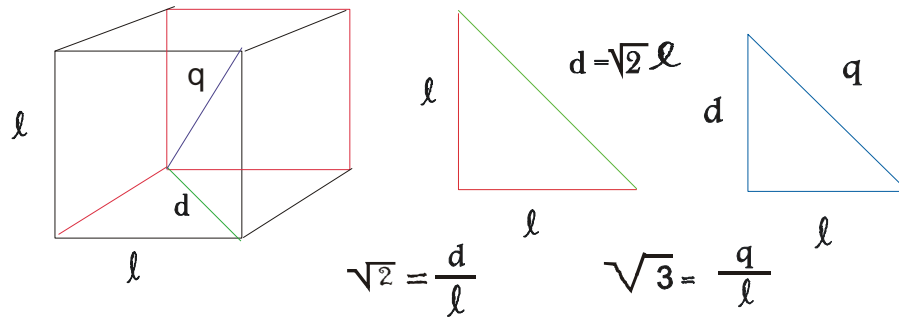
$$d^2 = (rl)^2 = l^2 + l^2 \quad (1)$$

Así pues, razonaba él: existe un "número" r tal que $r^2 = 1 + 1 = 2$. Pero por otra parte, Pitágoras reconoció que r no podía representarse como un cociente $r = \frac{a}{b}$ de enteros. En efecto, tomando a y b primos entre sí

$$\left(\frac{a}{b}\right)^2 = 2 \Rightarrow a^2 = 2b^2$$

Más aún, descomponiendo a en factores primos, resulta que a^2 es divisible por 2 un número par de veces (es decir, $a = 2k$) y por lo análogo 2 dividirá a $2b^2$ un número impar de veces (es decir, $2b^2 = (2k)^2$ o sea $4k^2 = 2b^2 \Leftrightarrow 2k^2 = b^2$ de donde $b = 2m$) y a no sería primo relativo con b . Luego $a^2 = 2b^2$ es imposible para a y b enteros. Únicamente podemos solucionar este "dilema de Pitágoras" introduciendo los **números irracionales**: números que no son cociente de enteros.

Razonamientos análogos demuestran que la razón $\sqrt{3}$ entre la longitud de la diagonal de un cubo C y la longitud de su arista.



Estos resultados son casos particulares del siguiente teorema mucho más general:

9.2 TEOREMA. Sea $p(x) = x^n + a_1x^{n-1} + \dots + a_n$ un polinomio con su primer coeficiente igual a 1 y los demás a_1, a_2, \dots, a_n enteros. Si la ecuación $p(x) = 0$ tiene raíces racionales, éstas son números enteros.

DEMOSTRACIÓN. Supongamos que $p(x) = 0$ para alguna fracción $x = \frac{a}{b}$. Dividiendo a y b por su *m.c.d* (máximo común divisor) puede expresarse x como cociente $x = \frac{r}{l}$ de dos enteros r, l primos entre sí. Sustituyendo este valor en $p(x)$ y quitando denominadores

$$0 = l^n p\left(\frac{r}{l}\right) = r^n + a_1 r^{n-1} l + a_2 r^{n-2} l^2 + \dots + a_n l^n$$

luego

$$r^n = -a_1 r^{n-1} l - \dots - a_n l^n$$

de donde l divide a r^n . Esto exige que cualquier factor primo de l divide a r^n y por lo tanto a r . Pero r y l no tienen divisores comunes, y por lo tanto $l = \pm 1$, y la fracción dada $x = \frac{r}{\pm 1} = \pm r$ es un número entero, lo cual queríamos demostrar.

□

Para probar la irracionalidad de $\sqrt{28}$, por ejemplo fundándonos en el teorema 9.2, procedemos como sigue: Si $|x| \geq 6$, entonces $x^2 - 28 > 0$, y, si $|x| \leq 5$, entonces $x^2 - 28 < 0$; luego ningún entero puede ser solución de $x^2 - 28 = 0$, y por el teorema 9.2 la solución de $x^2 = 28$, que es $\sqrt{28}$ no puede ser racional.

Otros números irracionales son π , e y muchos otros.

Es de notar que la mayoría de los números reales son irracionales e incluso, a diferencia de $\sqrt{2}$, no pueden satisfacer ninguna ecuación algebraica. Este resultado que hemos ampliado, nos indica ya que para contestar a la pregunta ¿qué es un número real? necesitamos utilizar ideas enteramente nuevas.

La naturaleza de estas ideas y la relación entre los números reales y los racionales serán examinadas parcialmente en los párrafos que siguen.

9.3 MÉTODO GEOMÉTRICO Y EXPANSIÓN DECIMAL

Los griegos de la época clásica usaron un método geométrico de aproximación para el cálculo de los números reales. Para ellos, un número era simplemente una razón $(a : b)$ entre dos segmentos rectilíneos a y b . En consecuencia, dieron construcciones geométricas para establecer la igualdad entre razones, así como para la adición, sustracción, multiplicación y división de razones. De este modo las leyes del álgebra aparecen como teoremas geométricos.

La versión griega de la noción de igualdad entre números racionales y reales se basaba en una condición debida a Eudoxio, que especificaba cuándo eran iguales dos razones. Esta condición se hacía depender de las posibilidades de formar geoméricamente los múltiplos enteros $m \cdot a$ de un segmento dado a y comparar geoméricamente las longitudes de los dos segmentos. Se estipulaba que $(a : b) = (c : d)$ cuando, para todo par de enteros positivos m y n

$$\text{si } ma > nb, \text{ también } mc > nd, \text{ si } ma < nb, \text{ también } mc < nd \quad (2)$$

Algebraicamente, $ma > nb$ significa que $\frac{a}{b} > \frac{n}{m}$ suponiendo siempre que b y m sean positivos. Entonces (2) puede leerse así:

$\frac{a}{b} = \frac{c}{d}$, cuando cualquier número racional $\frac{n}{m}$ que sea mayor que $\frac{a}{b}$ es también mayor que $\frac{c}{d}$.

La validez de la condición (2) de Eudoxio expresa, evidentemente, la circunstancia de que dos números reales positivos $(a : b)$ y $(c : d)$ son diferentes si y sólo si existe algún número racional mayor que uno de ellos y menor que el otro. También su condición para $(a : b) < (c : d)$ tiene el mismo fundamento y es el siguiente:

$$ra < lb \text{ y } rc < ld, \text{ para enteros convenientes } r \text{ y } l \quad (3)$$

El estudio geométrico de los números reales es ya desacostumbrado. En la actualidad se les estudia aritméticamente, mediante aproximaciones racionales, en expansión decimal (un decimal es, como se sabe, un número racional cuyo denominador es potencia de diez (10)). Por ejemplo, el irracional $\sqrt{2}$ se reemplaza en la práctica por las aproximaciones sucesivas

$$1, 1.4, 1.41, 1.414, 1.4142, \dots \quad (4)$$

El número π es aproximado análogamente, por los decimales

$$d_1 = 3.1, d_2 = 3.14, d_3 = 3.141, d_4 = 3.1415, d_5 = 3.14159, \dots \quad (5)$$

y así sucesivamente.

9.4 PROPIEDADES ALGEBRAICAS

Para cada par (x, y) de números está definido un número (y uno sólo) designado $x + y$, que es la suma de x con y , y un número (y uno sólo)

designado por xy que es su producto. La operación que al par (x, y) le hace corresponder en número $x + y$ (respectivamente xy) se llama **adición** (respectivamente **multiplicación**) y se tienen los siguientes axiomas

A.1 La adición y la multiplicación son asociativas, es decir para cualesquiera números x, y, z , se cumple

$$x + (y + z) = (x + y) + z$$

$$x(yz) = (xy)z$$

A.2 Los números 0 y 1 ($0 \neq 1$) son módulos para la adición y la multiplicación respectivamente, en el sentido siguiente

$$x + 0 = 0 + x = x, \quad \forall x \in \mathfrak{R}$$

$$x \cdot 1 = 1 \cdot x = x, \quad \forall x \in \mathfrak{R}$$

A.3 Dado un número x , existe un número x' , y uno sólo, tal que $x + x' = x' + x = 0$. Éste x' se llama el opuesto de x y se designa por $-x$. Análogamente dado x un número tal que $x \neq 0$, existe un número x'' , y uno sólo, tal que $xx'' = x''x = 1$. Este x'' es el inverso de x y se le denota por x^{-1} .

A.4 La adición y la multiplicación son conmutativas, es decir

$$x + y = y + x, \quad xy = yx$$

para todo número x y todo número y .

A.5 La adición es distributiva con respecto a la multiplicación, esto es,

$$x(y + z) = xy + xz$$

cualquiera que sean los números x, y, z

A.6 El número 1 es diferente al número 0.

A.7 Si $a = b$ y $c = d$ entonces $a + c = b + d$, $ac = bd$.

9.4.1 **TEOREMA.** $a \cdot 0 = 0$ para todo número a

PRUEBA. $1 = 1 + 0$, entonces $a \cdot 1 = a(1 + 0)$ de A.2 y A.5

$$a = a \cdot 1 + a \cdot 0 \Leftrightarrow a = a + a \cdot 0 \text{ aplicando A.7}$$

$$(-a) + a = (-a) + (a + a \cdot 0) \text{ de A.3 y A.1 tenemos}$$

$$0 = [(-a) + a] + a \cdot 0 \text{ de A.3}$$

$$0 = 0 + a \cdot 0 \quad \text{de A.2 se tiene finalmente}$$

$$0 = a \cdot 0$$

□

9.4.2 **TEOREMA.** Si $ab = 0$, entonces $a = 0$, ó, $b = 0$.

PRUEBA. Supongamos que $a \neq 0$, entonces existe a^{-1} por lo tanto

$$a^{-1}(ab) = a^{-1} \cdot 0 = 0$$

pero

$$a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$$

por lo tanto

$$b = 0$$

□

9.4.3 TEOREMA. El 0 no tiene inverso. Esto es, no hay un número real x tal que $0 \cdot x = 1$.

PRUEBA. Conocemos por 9.4.1 que $0 \cdot x = 0$. Si tenemos $0 \cdot x = 1$ para algún x , tendríamos que $0 = 1$, y , $0 \neq 1$ por el axioma A.6, esto es una contradicción.

□

9.4.4 TEOREMA. (*Ley cancelativa de la adición*) Si $a + b = a + c$ entonces $b = c$.

PRUEBA. Si $a + b = a + c$, entonces $(-a) + (a + b) = (-a) + (a + c)$, usando el axioma A.1 tenemos $[(-a) + a] + b = [(-a) + a] + c$ pero de A.3 se recibe $0 + b = 0 + c$ finalmente de A.2 se tiene $b = c$.

□

9.4.5 TEOREMA. (*Ley cancelativa de la multiplicación*) Si $ab = ac$ y $a \neq 0$ entonces $b = c$

PRUEBA. Si $ab = ac$ y $a \neq 0$, entonces a tiene inverso a^{-1} . Por lo tanto de A.7 se tiene

$$a^{-1}(ab) = a^{-1}(ac)$$

por A.1 tenemos

$$(a^{-1}a)b = (a^{-1}a)c$$

usando A.3

$$1 \cdot b = 1 \cdot c$$

por A.2 se llega a

$$b = c.$$

□

9.4.6 TEOREMA. Para cualquier número a se tiene $-(-a) = a$.

PRUEBA. Por definición del opuesto, el número $-(-a)$ es un número x tal que

$$(-a) + x = x + (-a) = 0$$

Para a por el axioma A.3 se tiene que

$$(-a) + a = a + (-a) = 0$$

luego el número $-a$ tiene dos opuestos aditivos a saber x y a , pero el axioma A.3 garantiza que

$$a = x = -(-a).$$

Para mayor seguridad se puede demostrar la unicidad del opuesto

LEMA. El opuesto aditivo es único.

En efecto, sea a un número por el axioma A.3 existe a' tal que $a + a' = a' + a = 0$. Supongamos que hay otro a'' tal que $a + a'' = a'' + a = 0$, resulta entonces que

$$a' = 0 + a' = (a'' + a) + a' = a'' + (a + a') = a'' + 0 = a''.$$

□

9.4.7 TEOREMA. Para cualesquiera números a y b se tiene que $(-a)b = -(ab)$.

PRUEBA. Basta probar que

$$(-a)b + ab = ab + (-a)b = 0$$

puesto que en esta forma se tiene que $(-a)b$ es el opuesto aditivo de ab y según el lema anterior $(-a)b = -(ab)$.

Ahora por el axioma A.5 tenemos

$$(-a)b + ab = [(-a) + a]b$$

por el axioma A.3 se tiene

$$(-a)b + ab = 0 \cdot b = 0.$$

□

9.4.8 TEOREMA. $(-a)(-b) = ab$ cualesquiera sean los números a y b .

PRUEBA.

$$\begin{aligned} (-a)(-b) &= -[a(-b)] \quad \text{¿porqué?} \quad \text{-----} \\ &= -[(-b)a] \quad \text{¿porqué?} \quad \text{-----} \\ &= -[-(ab)] \quad \text{¿porqué?} \quad \text{-----} \\ &= ba = ab \quad \text{¿porqué?} \quad \text{-----} \end{aligned}$$

□

9.4.9 TEOREMA. Si a y b son números diferentes de cero cualesquiera, entonces $(ab)^{-1} = a^{-1}b^{-1}$.

PRUEBA. Debemos mostrar que

$$(ab)(a^{-1}b^{-1}) = 1$$

ahora

$$\begin{aligned} (ab)(a^{-1}b^{-1}) &= a[b(a^{-1}b^{-1})] = a[b(b^{-1}a^{-1})] \\ &= a[(bb^{-1})a^{-1}] = a[1 \cdot a^{-1}] = aa^{-1} = 1 \end{aligned}$$

como el inverso multiplicativo de (ab) es $(ab)^{-1}$ y por la unicidad del inverso se tiene la igualdad.

Para mayor claridad mostemos que el inverso multiplicativo también es único; sabemos que para $a \neq 0$ existe a' tal que $aa' = a'a = 1$, supongamos ahora que existe otro número a'' tal que $aa'' = a''a = 1$ tenemos entonces

$$a'' = 1 \cdot a'' = (a'a)a'' = a'(aa'') = a' \cdot 1 = a'.$$

□

9.4.10 **TEOREMA.** Para cualesquiera números a y b se tiene

$$-(a + b) = (-a) + (-b)$$

PRUEBA. Nos basta con probar que

$$(a + b) + [(-a) + (-b)] = 0$$

En efecto; $(a + b) + [(-a) + (-b)] = a + (b + [(-a) + (-b)])$
 $= a + (b + [(-b) + (-a)]) = a + ([b + (-b)] + (-a))$
 $= a + (0 + (-a)) = a + (-a) = 0.$

□

9.4.11 **EJERCICIOS.**

Pruebe cada una de las siguientes igualdades aclarando los axiomas y resultado usados

(1) $b(-a) = -(ab)$

(2) $(-a)(-b) = ba$

(3) $a(b - c) = ab - ac$

(4) $-0 = 0$

(5) $a - 0 = a$

(6) $b - a = b + (-a)$

(7) $\left(\frac{a}{b}\right) = \left(\frac{c}{d}\right) \Leftrightarrow ad = bc$

(8) $\left(\frac{a}{b}\right) \pm \left(\frac{c}{d}\right) = \frac{(ad \pm bc)}{bd}$

(9) $\left(\frac{a}{b}\right) + \left(\frac{-a}{b}\right) = 0$

(10) $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$

(11) $\left(\frac{a}{b}\right) \neq 0 \Rightarrow \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1$

(12) $(-b)^{-1} = -(b^{-1})$

(13) Analice todas las demostraciones de los teoremas 9.4.1 a 9.4.10 y concluya que tipo de demostración fue utilizada.

9.5 PROPIEDADES DE ORDEN

Existe en los números una relación $>$ (es mayor que) que establece un orden entre los números y que está regida por los siguientes axiomas llamados de orden

O.1 Dados dos números reales x, y cualesquiera, se cumple una y una sola de las tres alternativas siguientes:

$$x > y, \quad x = y, \quad y > x$$

O.2 Si $x > y$, y a su vez $y > z$, entonces $x > z$.

OA.1 Si $x > y$ entonces $x + z > y + z$, para todo número z .

OA.2 Si $x > 0$, y $y > 0$, entonces $xy > 0$.

Estos últimos axiomas relacionan las propiedades algebraicas con el orden.

En lugar de " $x > y$, ó, $x = y$ " se escribe $x \geq y$. Se acostumbra también escribir $y < x$, y , $y \leq x$ en lugar de $x > y$, \wedge , $x \geq y$.

9.5.1 TEOREMA. Cualesquiera dos desigualdades pueden ser adicionadas. Esto es, si $b > a$ y $d > c$ entonces $b + d > a + c$

PRUEBA. Por OA.1 se tiene

$b + c > a + c \wedge b + d > b + c \Leftrightarrow b + d > b + c, \wedge, b + c > a + c$
entonces por O.2 se tendrá

$$b + d > a + c.$$

□

9.5.2 TEOREMA. $b > a$ si y sólo si $b - a > 0$

PRUEBA. Si $b > a$, entonces por OA.1 se tiene $b - a > a - a$. Por lo tanto $b - a > 0$.

Inversamente si $b - a > 0$, entonces $(b - a) + a > 0 + a$ de donde $b > a$.

□

9.5.3 TEOREMA. Una desigualdad es preservada si multiplicamos ambos miembros, por el mismo número positivo. Esto es

$$a > b \wedge c > 0, \Rightarrow ac > bc$$

PRUEBA. Puesto que $a > b$, tenemos $a - b > 0$. Por lo tanto usando OA.2 tenemos $c(a - b) > 0$ y por A.5 tenemos $ca - cb > 0$, usando el teorema 9.5.2 tenemos $ac > bc$.

□

9.5.4 TEOREMA. Si $a > 0$ entonces $-a < 0$.

PRUEBA. Si $a > 0$ entonces $a - a > 0 - a$ (por OA.1). Así $0 > -a \Leftrightarrow -a < 0$

□

9.5.5 TEOREMA. Si $0 > a$, entonces $-a > 0$.

PRUEBA. Si $0 > a$, entonces $0 - a > 0$ (por 9.5.2) $\Leftrightarrow -a > 0$.

□

9.5.6 TEOREMA. Si $b > a$ y $0 > c$ entonces $ac > bc$.

PRUEBA. Si $b > a$ entonces $b - a > 0$, y por otro lado si $0 > c$, entonces $-c > 0$. Por lo tanto $(-c)(b - a) > 0 \Leftrightarrow ac - bc > 0$ por el teorema 9.5.2 $ac > bc$.

□

9.5.7 EJERCICIOS.

(1) Ordene de menor a mayor los racionales siguientes

$$\frac{1}{2}, \frac{2}{3}, \frac{2}{5}, \frac{3}{7}, \frac{3}{4}, \frac{6}{7}, \frac{4}{5}.$$

(2) Determine sobre una recta numérica los puntos de coordenadas

$$-3, \sqrt{3}, \sqrt{5}, \frac{1}{2}, -\sqrt{6}, 0.3, 2\sqrt{2}.$$

(3) Pruebe que no es posible tener $x < y \wedge y < x$ para dos reales cualesquiera.

(4) Haga ver que $x \leq y \Leftrightarrow (x < y \vee x = y)$.

(5) Pruebe que $(x \leq y \wedge y \leq x) \Rightarrow x = y$.

(6) Establezca las propiedades análogas a OA.1 y al teorema 9.5.1 anteriores dadas para la relación " \leq ".

(7) Demuestre que si $x > 0$ y z es tal que $xz = 1$, entonces $z > 0$.

(8) Pruebe que si $a < b \wedge c > 0$, entonces $\frac{a}{c} < \frac{b}{c}$

¿Qué ocurrirá si $c < 0$?

(9) Demuestre que si $0 < a < b$, entonces $0 < \frac{1}{b} < \frac{1}{a}$.

(10) Defina y represente gráficamente los intervalos semiabiertos $(a, b]$ y $[a, b)$.

Aquí ; $(a, b] = \{x \in \mathbb{R} / a < x \leq b\}$ y $[a, b) = \{x \in \mathbb{R} / a \leq x < b\}$

(11) ¿Qué significan los intervalos (a, a) , $(a, b]$, $[a, b)$ y $[a, a]$?

(12) Halle y represente gráficamente los conjuntos siguientes:

$$(a) [0, 2] \cup [2, 6] \qquad (c) [-\frac{1}{2}, +\infty) \cup (-\infty, 2)$$

$$(b) [0, 2] \cup [2, 6] \qquad (d) (-\infty, 3) \cap (-1, +\infty)$$

$$(e) (0, 3) \cap [2, +\infty) \qquad (f) [0, 2] \cap [2, 3]$$

$$(g) [0, 3] \cap (3, 4] \qquad (h) [-1, +\infty) \cap [2, 4].$$

(13) Represente los números reales sobre una recta vertical, de tal manera que el punto correspondiente al 1 esté por encima del correspondiente al cero. Si $a < b$, ¿cómo estarán ubicados sus puntos correspondientes A y B?

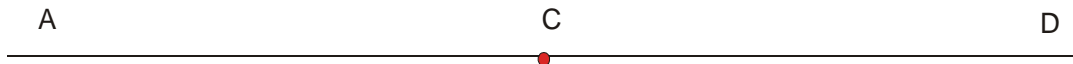
(14) ¿Cómo es el producto de los dos números reales negativos?. ¿Cómo es la suma de dos números negativos?. Demuestre que sus afirmaciones son verdaderas.

(15) Demuestre que el cuadrado de un número distinto de cero, es estrictamente mayor que cero.

9.6 PROPIEDAD DE COMPLECIDAD.

Como era de esperarse, esta propiedad afirma, en total acuerdo con la intuición, que la recta numérica no tiene huecos, que carece de discontinuidades: que es *completa*. Sin embargo, como puede apreciarse por el lenguaje usado, la propiedad en cuestión no está descrita con precisión suficiente para ser inequívoca y aceptable. Para lograr la anhelada precisión puede procederse de la manera siguiente:

En primer lugar una pregunta; si la recta numérica tuviera huecos ¿cómo podrían detectarse estos?. La existencia de uno de tales huecos o cortes



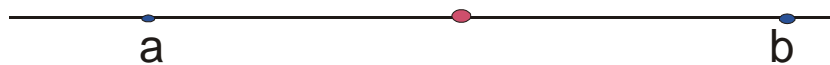
automáticamente daría al conjunto de los puntos de la recta, en virtud del orden que los afecta, una clasificación natural: los puntos que están antes del corte (puntos AC) y los puntos que están después del corte (puntos CD). Todo punto es un AC ó un CD (pero no las dos cosas al tiempo), además, todo punto anterior a un AC es un AC y todo punto posterior a un CD es un CD. Por último, no existiría un punto tal que todo punto anterior a él fuera un AC y todo punto posterior a él fuera un CD, (este elemento "sería" precisamente el que falta).

Más formalmente se procede así: una *cortadura* $(A|B)$ es una clasificación de todos los números en dos conjuntos ó clases A y B de tal manera que:

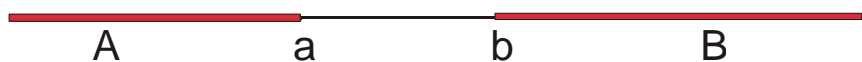
(i) Hay números en ambas clases (es decir, que ninguna de las dos clases es vacía)

(ii) Si $a \in A$ y $b \in B$, entonces $a < b$

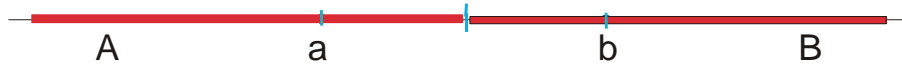
Dada la cortadura $(A|B)$, como las clases A y B no son vacías existe por lo menos un número $a \in A$ y un número $b \in B$, y por la condición (ii) se debe tener que $a < b$



Si un número $x < a$, entonces como debe estar clasificado, se encontrará en A ó en B , pero como por (ii) no puede estar en B , entonces necesariamente estará en A . Análogamente, todo número mayor que b debe pertenecer a B .



Por otra parte, los elementos entre a y b también deben estar clasificados, luego las clases A , B deben tener una disposición como la siguiente



Si existe un número c mayor o igual que todos los de A y menor o igual que todos los de B , este número c se llama número ó punto frontera de la cortadura $(A|B)$.

Intuitivamente puede verse que si existiera una cortadura $(A|B)$ sin frontera, la recta tendría un hueco, ó corte, es decir, no sería continua la recta numérica.

En este caso dado un elemento a de A , siempre existiría otro elemento $a' \in A$ tal que $a' > a$; análogamente para B $((\forall b \in B)(\exists b' \in B)/b' < b)$. Luego ningún elemento de A ó de B podría ser frontera, y como cada número real debe estar en A ó en B , entonces no existiría punto frontera alguno.

La última propiedad de los números reales asegura la inexistencia de estos "huecos" ó "discontinuidades" en el conjunto de los reales:

C. Toda cortadura $(A|B)$ en el conjunto de los números reales determina un número c que es su frontera.

Si el número c pertenece a la clase A , entonces A es el conjunto de todos los números *menores* o iguales que c y entonces c es el mayor de los elementos de A ó el "máximo" de A .

Si $c \in B$, entonces A es el conjunto de los números menores que c y B es el conjunto de los números *mayores* o iguales que c , siendo c el menor de los elementos de B , ó el "mínimo" de B .

Las propiedades que se acaban de enunciar caracterizan al conjunto de los números reales, en el sentido siguiente: si un sistema tiene esencialmente estas propiedades, entonces salvo notaciones usadas, este sistema es idéntico al de los números reales.

Es claro que los números reales tienen muchas propiedades pero, cada una de ellas es consecuencia estrictamente lógica de los axiomas antes enunciados. Como ejemplo consideremos el siguiente teorema conocido como la propiedad Arquimediana de los números.

9.6.2 TEOREMA. Si x e y son números reales positivos y si se localizan sucesivamente $x, 2x, 3x, 4x, \dots$ entonces llega un momento en que estos puntos sobrepasan a y , es decir, existe un número entero n tal que $nx > y$.

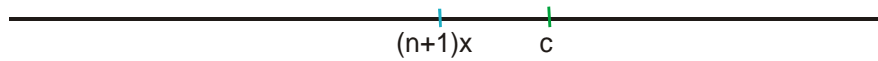
Este hecho, de tan grande evidencia intuitiva, puede sin embargo demostrarse usando sólo propiedades características de los números reales.

En efecto; si todos los múltiplos $x, 2x, 3x, 4x, \dots$ de x fueran $\leq y$, llamando B la clase de los números b que son mayores ó iguales que cada uno de los nx entonces, si $A = \mathbf{C}B$ se tiene

(i) $A \neq \Phi$ pues todos los múltiplos nx están en ella (cada uno de ellos es menor que el siguiente). B tampoco es vacío pues por ejemplo y es un número que está en esta clase.

(ii) Si $a \in A$ y $b \in B$, entonces a es menor que algún nx y b será mayor o igual que este nx , luego $a < b$.

Como además es claro que todos los números están clasificados, resultando que $(A|B)$ es una cortadura. Si c es la frontera de $(A|B)$ entonces todos los múltiplos de x serían menores o iguales que c , en particular, para todo natural n se cumpliría $(n + 1)x \leq c$ o lo que es lo mismo, $nx \leq c - x$ es decir, que todos los múltiplos de x serían también menores o iguales que $c - x$



Luego, si k es un número entre $c - x$ y c (por ejemplo $k = c - \frac{x}{2}$) siendo mayor que todos los nx debería estar en B y siendo menor que c debería estar en A , pero esto no es posible porque A y B no pueden tener elementos comunes. En consecuencia debe existir un múltiplo de x mayor que y .

□

Como se vio hace un instante, dados dos números diferentes x e y , es fácil hallar números que estén entre ellos, por ejemplo $z = \frac{x+y}{2}$ tiene esta propiedad.

Sin embargo usando la propiedad Arquimediana (9.6.2) puede demostrarse que entre dos números reales distintos x e y (tales que $x < y$ por ejemplo) siempre se halla una fracción $\frac{m}{n}$ (m, n enteros con $n \neq 0$).

La idea de la demostración es ésta: las fracciones

$$\dots, -\frac{2}{n}, -\frac{1}{n}, \frac{0}{n}, \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots$$

están repartidas a igual distancia unas de otras sobre la recta, para asegurar que una de ellas está entre x e y basta tomar $\frac{1}{n} < y - x$, en efecto, como $y > x$ entonces $y - x > 0$ luego existe $n \in \mathbb{N}$ tal que $n(y - x) > 1$ es decir $\frac{1}{n} < y - x$.

Si además m es el menor de los enteros que son mayores que nx , es decir $m > nx$ pero $m - 1 \leq nx$ o también $\frac{m-1}{n} \leq x$ entonces

$$\frac{m}{n} = \frac{m-1}{n} + \frac{1}{n} < x + (y - x) = y$$

y como $m > nx$ entonces $\frac{m}{n} > x$, luego

$$x < \frac{m}{n} < y.$$

Nos resta preguntar ¿dónde se usó la propiedad Arquimediana?

□

9.7. EJERCICIOS

1. Demostrar que si $(L|U)$ y $(L'|U')$ son cortaduras en el cuerpo de los racionales, cualquier número racional con una excepción a lo más, puede escribirse como $x + y$ ($x \in L, y \in L'$) o como $u + v$ ($u \in U, v \in U'$)
2. Demostrar que para todo $\epsilon > 0$ existe un n bastante grande para que $10^{-n} < \epsilon$.
3. A veces se define una cortadura de Dedekind en un campo ordenado F como un par de subconjuntos L' y U' de F tales, que cualquier elemento de F esté siempre en L' o en U' , y tal que $x < y$ siempre que $x \in L'$ e $y \in U'$. Por adición y supresión de convenientes números particulares, demostrar que cualquier cortadura $(L'|U')$ de este tipo da una cortadura $(L|U)$ en sentido del texto, y viceversa.
4. Si t es un elemento de un dominio ordenado D con $0 < t < 1$, demostrar que $s = 2 - t$ tienen las propiedades $s > 1, st \leq 1$.
5. Sea D un dominio ordenado "completo". (a) Si D no es isomorfo con \mathbb{Z} , demostrar que D contiene un elemento t con $0 < t < 1$. (b) Si b y c son elementos positivos cualesquiera de D , demostrar que $t^n b < c$ para algún n .
6. Demuestre que \mathfrak{R} satisface la propiedad arquimediana: dados $y \in \mathfrak{R} \wedge x > 0$, existe un natural n tal que $nx > y$.
7. Demuestre que dado cualquier real, siempre existe un real estrictamente mayor y otro estrictamente menor.
8. Pruebe que todo subconjunto de \mathfrak{R} no vacío y acotado inferiormente posee \inf en \mathfrak{R} .
9. Pruebe que \mathbb{N} no es un subconjunto superiormente acotado de \mathfrak{R} .

§ 10. LOS NÚMEROS NATURALES.

Se trata con seguridad del conjunto pionero en el estudio de la matemática, pues acogiéndonos al concepto del matemático alemán Leopoldo Kronecker nos atrevemos a decir que: "el buen Dios nos dió los números naturales; el resto ha sido obra del hombre". Hacemos a continuación una presentación, de estos números, desde un punto de vista axiomático como sigue:

10.1 DEFINICIÓN. Los números naturales, denotados por el símbolo \mathbb{N} , son un conjunto, dos de cuyos elementos son denotados con los símbolos 0 y 1 ($0 \neq 1$), junto con dos operaciones llamadas adición y multiplicación, denotadas por $+$ y \cdot respectivamente. Las siguientes propiedades algebraicas debe satisfacer la adición

1A $m + n = n + m$ para todo $m \in \mathbb{N}$ y para todo $n \in \mathbb{N}$

Esta propiedad es la ley conmutativa de la adición

2A $(n + m) + p = n + (m + p)$ para todo $n, m, p \in \mathbb{N}$

3A $\forall n \in \mathbb{N} \Rightarrow n + 0 = n$

4A $n = m \Leftrightarrow n + 1 = m + 1$ para todo $n, m \in \mathbb{N}$

5A $n \in \mathbb{N} \Rightarrow 0 \neq n + 1 \in \mathbb{N}$

Las siguientes propiedades algebraicas deben satisfacer la multiplicación

1M $n \cdot m = m \cdot n$ para todo $n, m \in \mathbb{N}$

2M $n \cdot (m \cdot p) = (n \cdot m) \cdot p$ para todo $n, m, p \in \mathbb{N}$

3M $n \in \mathbb{N} \Rightarrow 1 \cdot n = n$

La siguiente propiedad algebraica adicional debe cumplirse

D $n \cdot (m + p) = n \cdot m + n \cdot p$ para todo $n, m, p \in \mathbb{N}$.

Finalmente en adición a las anteriores propiedades algebraicas, la siguiente propiedad, que es llamada *el principio de inducción matemática*, debe tenerse

MI Si $S \subseteq \mathbb{N}$, es tal que $0 \in \mathbb{N}$ y

" $n \in S \Rightarrow n + 1 \in S$ " en verdadera

entonces $S = \mathbb{N}$.

Veamos algunos resultados que se deducen de la definición anterior y que se hacen como una ilustración

10.2 **TEOREMA.** Si $n \in \mathbb{N}$ y $n \cdot 0 = 0$ entonces $(n + 1) \cdot 0 = 0$

PRUEBA. $(n + 1) \cdot 0 = 0 \cdot (n + 1) = 0 \cdot n + 0 \cdot 1 = 0 + 0 = 0$

□

10.3 **TEOREMA.** Si $n \in \mathbb{N}$ y $n \neq 0$ entonces $n = k + 1$ para algún $k \in \mathbb{N}$

PRUEBA. Sea $S = \{0\} \cup \{k + 1/k \in \mathbb{N}\}$. S tiene las siguientes propiedades

(i) $0 \in \{0\} \Rightarrow 0 \in S$

(ii) Supóngase que $n \in S$. Pero, puesto que $S \subseteq \mathbb{N}$, tenemos que $n \in \mathbb{N}$ y además $n + 1 \in \{k + 1/k \in \mathbb{N}\}$, por lo tanto $n + 1 \in S$.

Luego S cumple las hipótesis de MI, siguiéndose que $S = \mathbb{N}$. Concluimos así que si $n \in \mathbb{N}$ y $n \neq 0$ entonces $n \in \{k + 1/k \in \mathbb{N}\}$ esto indica que $n = k + 1$ para algún $k \in \mathbb{N}$.

□

En la construcción de los números naturales el resultado dado por (10.3) es utilizado como la propiedad del "sucesor", el axioma MI es conocido como el *principio de inducción*. Dada nuestra pobreza en el campo de la lógica matemática y el espíritu de este trabajo no nos entramos en lo profundo del conjunto de los números naturales pero invitamos a

nuestros cibernautas a que estudien el libro introducción a la teoría de conjuntos capítulo IV pg 153 del profesor José M. Muñoz Quevedo y publicado por la Universidad Nacional en 1994 donde se hallan los números naturales con lujo de detalles.

10.4 EJERCICIOS

Utilice el principio de inducción para dar solución a los problemas 1 a 3 siguientes:

1. Si $S \subseteq \mathbb{Z}$ tal que el cero es su primer elemento, y se $n \in S$ entonces $n + 1 \in S$, ¿Cuál es el conjunto S ?
2. Si $S \subseteq \mathbb{Z}$ es tal que el primer elemento es -10 y el sucesor de cualquier elemento de S es también elemento de S . Halle el conjunto S .
3. Encuentre el subconjunto S de \mathbb{Z} constituido precisamente por aquellos n tales que $3^n - 1$ es divisible (exactamente!) por 2.
4. ¿Cuál sería el subconjunto A de \mathbb{Z} tal que
 - (i') 2 es el último elemento
 - (ii') el antecesor de cualquier elemento de A está también en A ?

Nota: Si $n \in A$, entonces a $n - 1$ se le llama el antecesor y a $n + 1$ el sucesor.

§11. LOS NUMEROS ENTEROS

En el conjunto de los números naturales y desde un punto de vista algebraico, se tiene la tendencia a estudiar ecuaciones de la forma más elemental posible como $5 + x = 2$, ó problema como, dados $m, n \in \mathbb{N}$ hallar x tal que $m + x = n$. Este problema no tiene en general solución en \mathbb{N} y para tratar de hallarle una solución se procede a extender \mathbb{N} y esta extensión es conocida como el conjunto de los números enteros y es el conjunto donde la resta ó diferencia es una operación y donde tenga sentido de hablar de perdidas y ganancias o de temperaturas bajo cero o negativas y que presentamos en una forma axiomática en la siguiente definición:

11.1 DEFINICIÓN. Sea M un conjunto que es dado por $\{-n/n \in \mathbb{N}\}$. Entonces los números enteros, denotados por el símbolo \mathbb{Z} , es el conjunto formado por $M \cup \mathbb{N}$, junto con dos operaciones, la adición y la multiplicación denotadas $+$ y \cdot respectivamente, y donde las siguientes propiedades se deben cumplir:

1. El subconjunto $\mathbb{N} \subseteq \mathbb{Z}$ junto con las operaciones $+$ y \cdot forman el sistema de los números naturales.

2. Las operaciones $+$ y \cdot satisfacen las propiedades algebraicas 1A, 2A, 3A, 4A, 1M, 2M, 3M y D para los elementos tomados en \mathbb{Z}
3. Para todo $z \in \mathbb{Z}$ existe $-z \in \mathbb{Z}$ tal que $z + (-z) = (-z) + z = 0$
 Nótese que así $\langle \mathbb{Z}, + \rangle$ es un grupo abeliano.

11.1.2 DEFINICIÓN. Un conjunto \mathcal{D} es llamado un *dominio de integridad* cuando entre sus elementos están definidas dos operaciones, notadas aditiva y multiplicativamente, con las propiedades:

DI.1. $(\forall a \in \mathcal{D})(\forall b \in \mathcal{D}) \left(\begin{smallmatrix} a+b \in \mathcal{D} \\ a \cdot b \in \mathcal{D} \end{smallmatrix} \text{ unívocamente} \right)$, de modo que sean validas la ley distributiva, las dos leyes asociativas y las dos conmutativas

DI.2 $(\exists 0 \in \mathcal{D})(\exists 1 \in \mathcal{D})$ tales que $0 \neq 1$ y $\left(\begin{smallmatrix} (\forall x \in \mathcal{D})(x+0=x) \\ (\forall x \in \mathcal{D})(x \cdot 1=x) \end{smallmatrix} \right)$

DI.3 $(\forall a \in \mathcal{D})$, la ecuación $a + x = 0$ tiene solución en \mathcal{D} dada por $x = -a$

DI.4 Se cumple la ley de simplificación para el producto, es decir

$$(\forall x \in \mathcal{D} - [0]) (a \cdot x = b \cdot x \Rightarrow a = b).$$

Según esta definición \mathbb{Z} , el conjunto de los números enteros, es un dominio de integridad.

Veamos algunos resultados destacados en \mathbb{Z}

11.2 TEOREMA. Si $a, b \in \mathbb{Z}$ entonces existe un único elemento $x \in \mathbb{Z}$ tal que $a + x = b$.

DEMOSTRACIÓN. La dividimos en dos partes a saber

(α) Si $a, b \in \mathbb{Z}$, entonces $a + x = b$ para algún $x \in \mathbb{Z}$

(β) Si $a, b \in \mathbb{Z}$, $a + x = b$, y $a + y = b$, entonces $x = y$

(α) Supóngase $a, b \in \mathbb{Z}$, hay dos posibilidades

(i) Si $a \in \mathbb{N}$ entonces $x = (-a) + b$, puesto que tenemos

$$a + x = a + [(-a) + b] = [a + (-a)] + b = 0 + b = b$$

(ii) Si $a \in M$, entonces $a = -n$ para algún $n \in \mathbb{N}$. En este caso tomamos $x = n + b$ teniéndose

$$a + x = (-n) + (n + b) = [(-n) + n] + b = 0 + b = b$$

así en este caso $x \in \mathbb{Z}$ y $a + x = b$.

(β) Supongamos $a + x = b$ y $a + y = b$, donde $a, b, x, y \in \mathbb{Z}$ entonces $a + x = a + y$. Presentándose dos casos nuevamente

(i) Si $a \in \mathbb{N}$, entonces obtenemos

$$\begin{aligned} x &= 0 + x = [(-a) + a] + x = (-a) + (a + x) = \\ &= (-a) + (a + y) = [(-a) + a] + y = 0 + y = y \end{aligned}$$

(ii) Si $a = -n$ para algún $n \in \mathbb{N}$, entonces

$$\begin{aligned} x &= x + 0 = x + (a + n) = (x + a) + n = (a + x) + n \\ &= (a + y) + n = (y + a) + n = y + (a + n) = y + 0 = y \end{aligned}$$

En cada caso $x = y$.

□

11.3 DEFINICIÓN. Para cada $a, b \in \mathbb{Z}$, se define $b - a$ al único número $x \in \mathbb{Z}$ tal que $a + x = b$. La operación en \mathbb{Z} así definida por el símbolo $-$ es llamada sustracción.

Como los números enteros \mathbb{Z} son la base de la aritmética en los párrafos 14, 15 y 16 destacaremos algunas otras de sus múltiples propiedades y aplicaciones.

11.3.1 EJERCICIO.

(1) Demuestre que $\langle \mathbb{Z}, - \rangle$ no es un grupo.

Mostrar utilizando el principio de inducción matemática

(2) $\forall n \geq 1, 1 + 3 + 5 + \dots + (2n - 1) = n^2$

(3) $\forall n \geq 1, 1 + 4 + 7 + \dots + (3n - 2) = \frac{n(3n-1)}{2}$

(4) $\forall n \geq 1, 5^n \geq 1 + 4n$

(5) $\forall n \geq N, 4^n - 1$ es divisible (exactamente) por 3.

(6) $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}, \forall n \geq 1.$

(7) $(\forall n \geq 1) \left(a + ar + ar^2 + \dots + ar^n = \frac{a(r^{n+1}-1)}{r-1} \right)$ cuando $r \neq 1.$

(8) Probar que las siguientes reglas valen en todo dominio de integridad:

(i) $(a - b) + (c - d) = (a + c) - (b + d)$

(ii) $(a - b) - (c - d) = (a + d) - (b + c)$

(iii) $(a - b)(c - d) = (ac + bd) - (ad + bc)$

(iv) $(a - b) = (c - d)$ si, y sólo si, $a + d = b + c$

(9) ¿Cuáles de los siguientes conjuntos de números son dominios de integridad?

(a) Todos los enteros pares

(b) Todos los enteros impares

(c) Todos los números de la forma $a + a\sqrt{2}$ con a y b números enteros

(d) Todos los números reales de la forma $a + b \cdot 5^{\frac{1}{4}}$, donde a y b son números enteros

(e) Todos los números reales de la forma $a + b \cdot \sqrt[4]{9}$, donde a y b

son

números enteros

(f) Todos los números enteros positivos.

(g) Todos los números racionales enteros cuyo denominador sea 1 o una potencia de 2

§12. NUMEROS RACIONALES

Nuevamente una propiedad algebraica nos permite la extensión de los números enteros al tratar de solucionar el problema:

"dados $a, b \in \mathbb{Z}$ hallar un número x tal que $ax = b$ ".

Este problema por lo general no tiene solución de \mathbb{Z} y con esta idea se extiende el conjunto \mathbb{Z} a uno que lo contenga y donde este problema tenga solución. En seguida damos una presentación de la extensión de \mathbb{Z} en la forma siguiente.

12.1 DEFINICIÓN. Un cuerpo F es un conjunto en el cual se tienen definidas dos leyes de composición distintas, las cuales se notan con $+$ y \cdot (adición y multiplicación) para las cuales $\langle F, + \rangle$ y $\langle F, \cdot \rangle$ son grupos abelianos y además

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{para todo } x, y, z \in F$$

Nótese que si F es un cuerpo para cada $a \neq 0$ existe a^{-1} "inverso" multiplicativo que satisface la ecuación $aa^{-1} = a^{-1}a = 1$

12.2 TEOREMA. Sea F un cuerpo, la división (excepto por cero) es una operación en $F - \{0\}$.

PRUEBA. Basta demostrar que para todo $a \neq 0$ y todo $b \in F$ la ecuación $ax = b$ tiene una única solución $x \in F$

Si $a \neq 0$, entonces existe $a^{-1} \in F$, podemos así construir un elemento

$$x = a^{-1}b$$

el cual por sustitución directa se prueba que $ax = b$.

Supongamos por otra parte que $ax = b$ y $ay = b$, entonces $ax = ay$, de aquí $a^{-1}(ax) = a^{-1}(ay) \Leftrightarrow (a^{-1}a)x = (a^{-1}a)y$ de donde se tiene $x = y$.

La solución de $ax = b$ es denotada $\frac{b}{a}$ ó $b \div a$, teniéndose así definida la división en F . En particular $a^{-1} = \frac{1}{a}$.

□

12.3 TEOREMA. En todo cuerpo F , los cocientes obedecen a las siguientes leyes (en donde $b \neq 0$ y $d \neq 0$)

- (1) $\left(\frac{a}{b}\right) = \left(\frac{c}{d}\right) \Leftrightarrow ad = bc$
- (2) $\left(\frac{a}{b}\right) \pm \left(\frac{c}{d}\right) = \frac{ad \pm bc}{bd}$
- (3) $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$
- (4) $\left(\frac{a}{b}\right) + \left(-\frac{a}{b}\right) = 0$
- (5) Si $\left(\frac{a}{b}\right) \neq 0$, entonces $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1$.

PRUEBA. (1) $\left(\frac{a}{b}\right) = \left(\frac{c}{d}\right) \Leftrightarrow ab^{-1} = cd^{-1}$, así

$$ad = a(bb^{-1})d = a(b^{-1}b)d = (ab^{-1})bd = (cd^{-1})db = c(d^{-1}d)b = cb$$

Recíprocamente

$$\begin{aligned} \frac{a}{b} &= ab^{-1} = b^{-1}a = b^{-1}a(dd^{-1}) = b^{-1}(ad)d^{-1} = b^{-1}(cb)d^{-1} = \\ &= b^{-1}(bc)d^{-1} = (b^{-1}b)cd^{-1} = cd^{-1} = \frac{c}{d} \end{aligned}$$

(2) Sabemos que $x = \frac{a}{b}$ e $y = \frac{c}{d}$ son las soluciones de las ecuaciones $bx = a$ y $dy = c$. Estas ecuaciones pueden combinarse para dar

$$dbx = ad, \quad bdy = bc, \quad bd(x \pm y) = ad \pm bc$$

Así pues, $x \pm y$ es la única solución $(\frac{ad \pm bc}{bd})$ de la ecuación $(bd)z = ad \pm bc$

(3) Como antes, las ecuaciones $bx = a \wedge dy = c$ pueden combinarse para dar

$$(bd)(xy) = (bx)(dy) = ac$$

de la cual sale $xy = \frac{ac}{bd}$

(4) Sustituyendo en (2) tenemos

$$\left(\frac{a}{b}\right) + \left(-\frac{a}{b}\right) = \frac{ab-ba}{b^2} = 0(b^2)^{-1} = 0$$

(5) Sustituyendo en (3) tenemos $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \frac{ab}{ab}$. Pero $\frac{ab}{ba}$ es la única solución de la ecuación

$$(ba)x = ab$$

Como $x = 1$ satisface a esta ecuación se tendrá $\frac{ab}{ba} = 1$.

□

EJEMPLO. Se sigue de los axiomas de \mathfrak{R} que \mathfrak{R} es un cuerpo.

12.4 DEFINICIÓN. Un subcuerpo K de un cuerpo dado F es un subconjunto de F que es así mismo un cuerpo respecto a las operaciones de adición y multiplicación en F restringidas a K .

12.5 TEOREMA. Un subcuerpo S de un cuerpo F es un subconjunto que contiene al cero y la unidad de F , además es cerrado para la adición, cerrado para la multiplicación, para cada $a \in S$ se tiene que $-a \in S$ y si $a \neq 0$ entonces $a^{-1} \in S$, y recíprocamente.

EJEMPLO. $\mathfrak{R}(\sqrt{2}) = \left\{ a + b\sqrt{2} / a \in \mathfrak{R}, b \in \mathfrak{R} \right\}$ es un subcuerpo de los números reales.

12.6 CONSTRUCCIÓN DE LOS ELEMENTOS RACIONALES

Los enteros solos no forman un cuerpo, la construcción de los números racionales a partir de los enteros como una extensión, es esencialmente la construcción de un cuerpo que contenga a los enteros como subconjunto. Naturalmente este cuerpo deberá además, contener las soluciones de todas las ecuaciones del tipo $bx = a$ con coeficientes enteros a y $b \neq 0$. La construcción abstracta de los "números racionales" que resuelvan estas ecuaciones se sigue, simplemente, introduciendo

ciertos símbolos nuevos $r = (a, b)$, a los que llamaremos pares, cada uno de los cuales es solución de una ecuación

$$bx = a$$

Debemos hacer ver que estos nuevos entes puedan igualarse, sumarse y multiplicarse, exáctamente como los cocientes en un cuerpo.

12.6.1 DEFINICIÓN. El conjunto \mathbb{Q} de números racionales está constituido por todos los pares (a, b) de enteros a y $b \neq 0$. La igualdad entre pares se rige por el convenio siguiente

$$(a, b) = (a', b') \Leftrightarrow ab' = a'b$$

Mientras que la suma y el producto se definen así

$$(a, b) + (a', b') = (ab' + a'b, bb')$$

$$(a, b) \cdot (a', b') = (aa', bb')$$

Los resultados son siempre pares teniendo por segundo componente a $bb' \neq 0$.

12.6.2 PROPIEDAD. Si $(a, b) = (a', b')$ entonces se tiene

$$(a, b) + (a'', b'') = (a', b') + (a'', b'')$$

En efecto, como $(a, b) = (a', b')$ entonces $ab' = a'b$ así,

$$(a, b) + (a'', b'') = (ab'' + a''b, bb'')$$

y

$$(a', b') + (a'', b'') = (a'b'' + a''b', b'b'')$$

ahora

$$\begin{aligned} (ab'' + a''b)b'b'' &= (ab'')(b'b'') + (a''b)b'b'' = b''(ab')b'' + a''(bb')b'' = \\ &= b''(a'b)b'' + a''(b'b)b'' = (a'b'')(bb'') + (a''b')(bb'') = (a'b'' + a''b')(bb'') \end{aligned}$$

Luego

$$(ab'' + a''b)(b'b'') = (a'b'' + a''b')(bb'')$$

de donde

$$(ab'' + a''b, bb'') = (a'b'' + a''b', b'b'')$$

y se tiene

$$(a, b) + (a'', b'') = (a', b') + (a'', b'').$$

□

Pueden probarse ahora varias leyes algebraicas para los números racionales que hemos definido. Así, en la ley distributiva se puede reducir simultáneamente ambos miembros de la igualdad de acuerdo con la definición, del siguiente modo (supongamos que r, r' y r'' están en \mathbb{Q})

$$\begin{array}{ll} r(r' + r'') & rr' + rr'' \\ (a, b)[(a', b') + (a'', b'')] & (a, b)(a', b') + (a, b)(a'', b'') \\ (a, b)(a'b'' + a''b', b'b'') & (aa', bb') + (aa'', bb'') \\ (aa'b'' + aa''b', bb'b'') & (aa'bb'' + aa''bb', bb'bb'') \end{array}$$

Estos dos resultados dan parejas iguales, ya que el segundo resultado difiere del primero sólo en la presencia de un factor b en todos los términos. Pero un factor extra en un par, da siempre otro par igual, pues

$$(bx, by) = (x, y) \Leftrightarrow bxy = bxy \Leftrightarrow xy = xy, \text{ ya que } b \neq 0$$

Esta demostración explícita de la ley distributiva para números racionales (ó pares) es sólo un ejemplo del método. Por el mismo empleo directo de las definiciones y de las leyes de los enteros, se prueban la conmutatividad y la asociatividad, en efecto

CONMUTATIVIDAD

$$\begin{array}{ccc} r + r' & r' + r & rr' & r'r \\ (a, b) + (a', b') & (a', b') + (a, b) & (a, b)(a', b') & (a', b')(a, b) \\ (ab' + a'b, bb') = & (a'b + ab', b'b) & (aa', bb') = & (a'a, b'b) \end{array}$$

ASOCIATIVIDAD

$$\begin{array}{ccc} (r + r') + r & r + (r' + r'') & \\ [(a, b) + (a', b')](a'', b'') & (a, b) + [(a', b') + (a'', b'')] & \\ (ab' + a'b, bb') + (a'', b'') & (a, b) + (a'b'' + a''b', b'b'') & \\ (ab'b'' + a'bb'' + a''bb', bb'b'') = & (ab'b'' + a'bb'' + a''bb', bb'b'') & \\ (r \cdot r')r'' & r(a'r'') & \\ [(a, b)(a', b')](a'', b''), & (a, b)[(a', b')(a'', b'')] & \\ (aa', bb')(a'', b'') & (a, b)(a'a'', b'b'') & \\ (aa'a'', bb'b'') = & (aa'a'', bb'b'') & \end{array}$$

Un elemento idéntico para la adición es el par $(0, 1)$ ya que

$$(0, 1) + (a, b) = (0 \cdot b + 1 \cdot a, 1 \cdot b) = (a, b)$$

La ley de simplificación se conserva y el par $(1, 1)$ es el elemento idéntico para la multiplicación. El opuesto de (a, b) es

$$-(a, b) = (-a, b)$$

Se cumplen pues todos los postulados que definen a un cuerpo. En resumen tenemos

12.7 TEOREMA. El conjunto \mathbb{Q} de los números racionales, constituido por todos los pares de números enteros es un cuerpo y definiendo

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

se tiene que

$$\mathbb{Q} = \{(a, b) / (a, b) = \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\}\}.$$

12.8 EJERCICIO.

1. Admitiendo que el conjunto de los números reales es un cuerpo ¿Cuáles de los siguientes conjuntos son subcuerpos de \mathbb{R} ?

(a) Todos los enteros positivos

(b) Todos los números de la forma $a + b\sqrt{3}$ con $a \in \mathbb{Q}, b \in \mathbb{Q}$

- (c) Todos los números de la forma $a + b\sqrt[3]{5}$ con a y b números racionales.
- (d) Todos los números racionales no enteros.
- (e) Todos los números de la forma $a + b\sqrt{5}$ con a y b números racionales.
2. Hallar el número racional cuyo desarrollo decimal es 0.334444...
3. Demostrar que el desarrollo decimal de x termina en cero (ó en nueve) si x es racional y su denominador es de forma $2^n 5^m$, donde m y n son enteros positivos o nulos y recíprocamente.
4. Demostrar que $\sqrt{2} + \sqrt{3}$ es irracional
5. Si a, b, c, d son racionales y x es irracional, demostrar que $(ax + b)/(cx + d)$ es, en general irracional. ¿Cuándo se presentan excepciones?
6. Dado cualquier real $x > 0$, encontrar un número irracional comprendido entre 0 y x .
7. Si $\frac{a}{b} < \frac{c}{d}$ siendo $b > 0, d > 0$, demostrar que $\frac{a+c}{b+d}$ está comprendida entre $\frac{a}{b}$ y $\frac{c}{d}$.
8. Sean a y b enteros positivos. Demostrar que $\sqrt{2}$ siempre está comprendido entre dos fracciones $\frac{a}{b}$ y $\frac{a+2b}{a+b}$. ¿Cuál de las fracciones está más próximo a $\sqrt{2}$?
9. Designemos por a y b las raíces de la ecuación cuadrática $x^2 - x - 1 = 0$ y sea $x_n = \frac{a^n - b^n}{a - b}$. Demostrar que $x_1 = 1, x_2 = 1, x_3 = 2, \dots, x_{n+1} = x_n + x_{n-1}$.
10. Determinar para qué valores del entero $n \geq 1$ número $\sqrt{n-1} + \sqrt{n+1}$ es racional, y para cuáles es irracional.

§ 13. ACOTACIÓN. TERMINACIÓN. EXTREMACIÓN.

13.1 DEFINICIÓN. Sea L un conjunto ordenado, es decir un conjunto en donde se cumplen los axiomas O1, O2, AO1, y AO2 de la sección 9.5. Se dice que un subconjunto A de L ($A \subseteq L$) es **acotado superiormente** por un elemento $x \in L$ si

$$(\forall a \in A)(a \leq x)$$

Se dice que A es **acotado inferiormente** por un elemento $y \in L$ si

$$(\forall a \in A)(y \leq a)$$

En estos casos decimos que x es una cota superior de A y que y es una cota inferior de A .

A se dice **acotado** si lo es superior e inferiormente.

EJEMPLOS (1) El conjunto $\{x/x = \frac{1}{n}, n \in \mathbb{N} - \{0\}\} = \{1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots\}$ es un conjunto acotado, pues, 1 es la cota superior y 0 es la cota inferior.

(2) El conjunto $A = \{x \in \mathbb{R}/x^2 > 2\}$ no es un conjunto acotado ¿porqué?

13.2 **DEFINICIÓN.** Sea A un conjunto de números reales acotado superiormente. Supongamos que exista un número real x que satisfice las dos condiciones siguientes

(a) x es una cota superior de A

(b) Si y es otra cota superior de A , entonces $x \leq y$

Entonces el número x es llamado **extremo superior** del conjunto A .

Análogamente se define el **extremo inferior** (a') y es una cota inferior de A y (b') si y_1 es otra cota inferior de A , entonces $y_1 \leq y$).

Cuando un conjunto es tal que admite extremo superior y extremo inferior entonces se dice que es un conjunto **terminado**.

NOTACIÓN. Al extremo superior se le suele llamar el **supremun** y se nota \sup . Al extremo inferior se llama con frecuencia **infimun** y se le nota \inf .

Sea $\sup A$ el supremun de un conjunto A si $\sup A \in A$ entonces el $\sup A$ es llamado **máximo** de A . Por analogía si $\inf A \in A$, entonces el infimun de A es llamado **mínimo** de A .

NOTA. Sea A un conjunto acotado y sea $x = \sup A$ entonces se suele escribir

$$(\text{Dado } \epsilon > 0)(\exists a \in A)(x - \epsilon < a)$$

Análogamente si $t = \inf A$ entonces se suele caracterizar con la siguiente proposición

$$(\text{Dado } \epsilon > 0)(\exists a' \in A)(t + \epsilon > a').$$

13.3 **TEOREMA.** Sean A y B dos conjuntos acotados de números reales con $a = \sup A$, $b = \sup B$. Designemos por C al conjunto

$$C = \{x + y/x \in A, y \in B\}$$

entonces $a + b = \sup C$.

PRUEBA. Si $z \in C$ entonces $z = x + y \leq a + b$, de modo que $a + b$ es una cota superior de C . Sea c otra cota superior de C . Tenemos que $a + b \leq c$, para ello sea $\epsilon > 0$ un número positivo dado, existe un número $x \in A$ y existe un número $y \in B$ tales que

$$a - \epsilon < x, \quad b - \epsilon < y$$

Por la adición de estas desigualdades, encontramos

$$a + b - 2\epsilon < x + y \leq c$$

Esto es $a + b \leq c + 2\epsilon$. Pero ϵ es arbitrario, resulta así

$$a + b \leq c$$

□

13.3.1 **DEFINICIÓN.** Un subconjunto de números reales se dice **mayorado** cuando admite cotas superiores y **minorado** cuando admite cotas inferiores. Un conjunto se dice extremado ó limitado cuando admite cota inferior y cota superior.

A continuación enunciamos el axioma de completitud para los números reales, el cual, en este momento, estamos preparados para probarlo.

13.4 (C') Si un conjunto X de números reales es mayorado, entonces X tiene supremum.

Dualmente se tiene si X es un conjunto de números reales que está minorado entonces X tiene ínfimum.

DEMOSTRACIÓN. Sea B el conjunto de las cotas superiores de X , entonces, por hipótesis $B \neq \emptyset$, pues X es mayorado. Sea ahora $A = \mathbb{C}B$ el conjunto de los números que no son cotas superiores de X , es decir, A es el conjunto de todos los números a tales que existe un elemento $x \in X$ tal que $x > a$. Entonces A tampoco es vacío pues cualquier número menor que un elemento de X (que no es vacío) pertenece a A .

Además

(i) Es claro que cada número real está en A o en B pero no en ambos

(ii) Si $a \in A$ y $b \in B$, entonces $a < b$, en efecto, si $a \in A$ entonces existe $x \in X$ tal que $a < x$ y como $b \in B$, b es una cota superior de X entonces $x \leq b$ así

$$a < x \wedge x \leq b$$

luego por la transitividad se tiene $a < b$.

Concluimos así que $(A|B)$ es una cortadura, entonces por el axioma C de los números reales $(A|B)$ tiene un punto frontera. Sea c la frontera de esta cortadura teniéndose que c no está en A puesto que si esto ocurriera existiría un elemento x de X tal que $c < x$ pero entonces los elementos entre c y x estarían en A (por ser menores que x) y serían mayores que c (que es la frontera). Luego c es el mínimo de B es decir, es la mínima cota superior de X o sea el supremum de X .

Análogamente se demuestra que todo conjunto no vacío y minorado tiene ínfimum.

Nota. Cuando este resultado se generaliza a conjuntos ordenados y cadenas de orden, es conocido como el lema de Zorn.

13.4.1 EJERCICIOS

1. Demostrar que el sup y el inf de un conjunto son únicos cuando existe.
2. Hallar el sup y el inf de cada uno de los siguientes conjuntos de números reales
 - (a) Todos los números de la forma $2^{-p} + 3^{-q} + 5^{-r}$, donde p, q y r toman todo los valores enteros positivos.
 - (b) $S = \{x/3x^2 - 10x + 3 < 0\}$.
 - (c) $S = \{x/(x-a)(x-b)(x-c)(x-d) < 0\}$, siendo $a < b < c < d$.

3. Sean S un conjunto de números reales acotados superiormente, $a = \sup S$ y ϵ un número positivo. Demostrar que existe por lo menos un número $x \in S$ tal que $a - \epsilon < x \leq a$.

4. Sean A y B dos conjuntos de números reales acotados superiormente, $a = \sup(A)$ y $b = \sup(B)$. Si C es el conjunto de los números reales formados, considerando todos los productos de la forma xy , donde $x \in A$ e $y \in B$, demostrar que, en general, $ab \neq \sup(C)$.

5. Sean x un número real > 0 , y k un entero positivo > 1 . Representemos por a_0 el mayor entero $\leq x$ y suponiendo que a_0, a_1, \dots, a_{n-1} hayan sido definidos, representemos por a_n el mayor entero tal que

$$a_0 + \frac{a_1}{k} + \frac{a_2}{k^2} + \dots + \frac{a_n}{k^n} \leq x.$$

(a) Demostrar que $0 \leq a_i \leq k - 1$ para $i = 1, 2, \dots$

(b) Explicar cómo pueden obtenerse geoméricamente los números a_0, a_1, a_2, \dots

(c) Demostrar que la serie $a_0 + \frac{a_1}{k} + \frac{a_2}{k^2} + \dots$ converge y tiene por suma x

(d) Demostrar que x es el sup del conjunto de las sumas parciales de serie dada en (c)

Nota. La serie dada en (c) origina un desarrollo decimal de x en el sistema de base k .

13.5 PRINCIPIO DE BUENA ORDENACIÓN

Los números enteros poseen otra propiedad importante no caracterizada algebraicamente y no compartida por otros sistemas de números. Tal propiedad es la siguiente:

Cualquier subconjunto de números enteros positivos que contenga al menos un elemento, contiene elemento mínimo.

En otras palabras, cualquier selección dada de números enteros positivos contiene un entero positivo m tal que cualquiera que sea el entero a en la selección dada se tiene $m \leq a$.

Por ejemplo el más pequeño entero positivo par es 2.

Más generalmente, un conjunto de números se llama *bien ordenado* si cualquiera de sus subconjuntos no vacíos contiene un elemento mínimo.

Así pues, el principio anterior indica que los enteros positivos están bien ordenados.

13.5.1 TEOREMA. No hay ningún número entero entre 0 y 1.

PRUEBA. Esto se ve inmediatamente sin más que echar una ojeada al orden natural de los enteros pero lo que pretendemos es probarlo utilizando las hipótesis fundamentales (postulados), sin necesidad de utilizar la referida serie de enteros (en el caso 0, 1). Daremos una prueba indirecta (vea 3.3). Si hay un entero c tal que $0 < c < 1$, sea C el conjunto de todos

los enteros c tales que $0 < c < 1$, entonces $C \neq \Phi$. Por el principio de la buena ordenación, existe un entero m que es el mínimo para C y tal que $0 < m < 1$. Multiplicando esta desigualdad por m obtenemos

$$0 < m^2 < m$$

Entonces m^2 es otro número entero de C , menor que el supuesto mínimo de C . Esta contradicción demuestra el teorema.

13.5.2 TEOREMA. Un conjunto S de números enteros positivos que incluya al 1 y que incluya al $n + 1$ siempre que incluya a n , incluye también a cualquier entero positivo.

PRUEBA. Bastará probar que el conjunto S' de todos los números enteros positivos no contenidos en S es vacío. Supongamos que S' no sea vacío, por el principio de buena ordenación S' contendrá un elemento mínimo m . Pero $m \neq 1$ por hipótesis, luego por el teorema anterior, $m > 1$ y $m - 1$ deberá ser positivo. Como además $m - 1 < m$ resulta que, por la definición de m , $m - 1$ debe estar en S . Se deduce de la hipótesis que $(m - 1) + 1 = m$, así $m \in S \wedge m \in S'$ o sea $m \in S \wedge m \notin S$ esta contradicción demuestra el teorema.

13.5.3 EJERCICIOS

1. Demostrar que para cualquier entero a , $a - 1$ es el mayor entero menor que a .
2. ¿Cuáles de los siguientes conjuntos son bien ordenados?
 - (a) Todos los enteros positivos impares
 - (b) Todos los negativos pares
 - (c) Todos los enteros mayores que -7
 - (d) Todos los enteros impares mayores que 249.
3. Probar que todo subconjunto de un conjunto ordenado está bien ordenado.
4. Demostrar que el conjunto de enteros que contiene a -1000 y que contiene a $x + 1$, si contiene a x , contiene a todos los enteros positivos.
5. (a) Un conjunto S de enteros tiene al entero b como "cota inferior" si $b \leq x$ para todo x en S ; el mismo b puede pertenecer o no pertenecer a S . Demostrar que cualquier S no vacío que tiene una cota inferior, tiene un elemento mínimo.
 - (b) Demostrar que cualquier conjunto de enteros no vacío que tiene una "cota superior" contiene un elemento máximo.

13.6 DIVISIBILIDAD

Una ecuación $ax = b$ con coeficientes enteros, no siempre tiene solución entera. Cuando existe tal solución, se dice que b es divisible por a

13.6.1 DEFINICIÓN. Un entero b es divisible por un entero a cuando hay algún entero d tal que $b = ad$. Entonces escribimos $a|b$, diremos también que b es un múltiplo de a y que a es un factor o divisor de b .

$$a|b \Leftrightarrow \exists d \in \mathbb{N} / b = ad$$

He aquí una nueva relación " $a|b$ ". Son propiedades de esta relación la reflexividad y la transitividad

$$a|a, \quad a|b \wedge b|c \Rightarrow a|c$$

La primera propiedad es trivial pues $a = a \cdot 1 \Leftrightarrow a|a$

La segunda tiene por hipótesis directa que $b = ad_1$, y $c = bd_2$, siendo d_1 y d_2 dos enteros adecuados; de lo cual resulta

$$c = a(d_1d_2) \text{ como } d_1 \cdot d_2 \in \mathbb{Z} \Leftrightarrow a|c$$

□

13.6.2 TEOREMA. Los únicos divisores enteros de 1 son ± 1 .

PRUEBA. El teorema afirma que si dos enteros a y b son tales que $ab = 1$ se debe tener $a = \pm 1$ y $b = \pm 1$, en efecto, $ab = 1$ así $|ab| = |a||b| = 1$. Como $a \neq 0, b \neq 0$, $|a|$ y $|b|$ son enteros positivos y no hay enteros entre 0 y 1, por la ley de tricotomía

$$|a| \geq 1 \text{ y } |b| \geq 1$$

Si los dos signos ó en el peor de los casos uno, son desiguales el producto $|a||b|$ no puede ser igual a 1. Entonces $|a| = 1 \wedge |b| = 1$ y por lo tanto $a = \pm 1$ y $b = \pm 1$.

Como $a = a \cdot 1 = (-a)(-1)$ todo entero a es divisible por $a, -a, 1$ y -1 . Los números a y $-a$ por dividirse mutuamente, se llaman "asociados".

13.6.3 DEFINICIÓN. Dos enteros a y b se llaman asociados si se verifican las relaciones $a|b$ y $b|a$. Los asociados de 1 se llaman unidades.

Esta definición significa que un entero es una unidad si y sólo si es un divisor de 1, con esto, el teorema 13.6.2 establece, simplemente que las únicas unidades son ± 1 . Si a y b son asociados, $a = bd_1$ y $b = ad_2$. Luego $a = a(d_1d_2)$ y por la ley de simplificación queda

$$1 = d_1d_2$$

O sea que d_1 es un divisor de 1 y por lo tanto, $d_1 = \pm 1$. Por lo tanto es $b = ad_1 = \pm a$, así que los únicos asociados de a son $\pm a$.

Dos enteros a y b son asociados si y sólo si $|a| = |b|$.

13.6.4 DEFINICIÓN. Un entero p es primo si, siendo distinto de 0 y de ± 1 , es divisible únicamente por ± 1 y $\pm p$.

Los primeros números primos son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots$$

Todo número que no es primo puede descomponerse en un producto de factores primos:

EJEMPLO. $128 = 2^7$; $90 = 10 \times 9 = 2 \cdot 5 \cdot 3^2$; $672 = 96 \cdot 7 = 7 \cdot 12 \cdot 8 = 7 \cdot 3 \cdot 2^5$

Se observa por experiencia, que obtenemos los mismos factores primos cualesquiera que sea el método de descomposición. Esta unicidad la demostraremos al estudiar el *m.c.d.*

13.6.5 DEFINICIÓN. Para todo $x \in \mathfrak{R}$, $|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$

13.6.6 TEOREMA. Para todo $x \in \mathfrak{R}$, $|x| \geq 0$.

PRUEBA. (1) Si $x \geq 0$, entonces $|x| \geq 0$ porque en este caso $|x| = x$.

(2) Si $x < 0$, entonces $-x > 0$. Por lo tanto $|x| > 0$ porque aquí $|x| = -x$.

□

13.6.7 TEOREMA. Para cualquier $x \in \mathfrak{R}$, $|-x| = |x|$

PRUEBA. (1) Si $x \geq 0$, entonces $-x \leq 0$, así $|x| = x$ y por lo tanto $|x| = -(-x) = x$, siguiéndose que $|x| = |-x|$

(2) Si $x < 0$, entonces $-x > 0$, así $|x| = -x$ ahora $|-x| = -x$ por lo tanto $|x| = |-x|$

□

13.6.8 TEOREMA. Para cualesquier $x \in \mathfrak{R}$ se tiene $|x| \geq x$.

PRUEBA. Si $x \geq 0$, esto es verdad porque $x \geq x$.

Si $x < 0$ entonces $x < |x|$ puesto que $|x| \geq 0$.

□

13.6.9 TEOREMA. $|xy| = |x||y|$ para todo $x, y \in \mathfrak{R}$

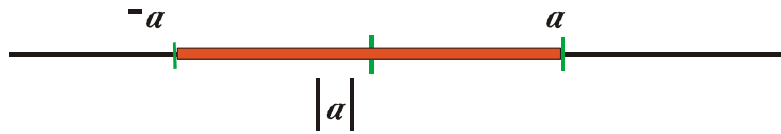
PRUEBA. Cuando x es reemplazado por $-x$ esto es $x < 0 \wedge y > 0$, $|xy| = -xy = |x||y|$. Análogamente si $x > 0 \wedge y < 0$. Ahora si $x \geq 0 \wedge y \geq 0$ entonces $|xy| = xy = |x||y|$.

Finalmente si $x < 0 \wedge y < 0$, entonces $xy > 0 \wedge (-x)(-y) > 0$ luego

$$|xy| = xy = (-x)(-y) = |x||y|.$$

□

13.6.10 **TEOREMA.** Sea $a > 0$, entonces $|x| < a \Leftrightarrow -a < x < a$



PRUEBA. (1) Si $x \geq 0$ entonces $|x| < a$ indica que $x < a$, además $0 \leq x < a$
 (2) Si $x < 0$, entonces $|x| < a$ indica que $-x < a$, ó, $-a < x$ aquí $|x| < a$ es verdad cuando $-a < x < 0$.

Por lo tanto $|x| < a$ implica $-a < x < a$

□

13.6.11 **TEOREMA.** Para cualesquiera $a, b \in \mathbb{R}$ se tiene $|a + b| \leq |a| + |b|$. Esta desigualdad es llamada **desigualdad triangular**.

PRUEBA. Caso 1. Supongamos que $a + b \geq 0$. En este caso $|a + b| = a + b$ pero $a \leq |a|$ y $b \leq |b|$ así $a + b \leq |a| + |b|$ luego $|a + b| \leq |a| + |b|$

Caso 2. Supóngase que $a + b < 0$ entonces $(-a) + (-b) > 0$ aplicando el caso 1 tenemos $|(-a) + (-b)| \leq |-a| + |-b|$ pero

$$|(-a) + (-b)| = |-(a + b)| = |a + b| \text{ y } |-a| = |a|, |-b| = |b|$$

Luego

$$|a + b| \leq |a| + |b|$$

□

1.3.6.12 EJERCICIOS.

(1) Demuestre que si $b \neq 0$ entonces $|\frac{1}{b}| = \frac{1}{|b|}$

(2) Demostrar que para todo $a \in \mathbb{R}$ y todo $b \in \mathbb{R} - \{0\}$ se tiene

$$|\frac{a}{b}| = \frac{|a|}{|b|}$$

(3) Demuestre que para tado $a, b \in \mathbb{R}$ se tiene $|a - b| \geq |a| - |b|$

(4) Demostrar que para todo $a, b \in \mathbb{R}$ se tiene $|a + b| \geq |a| - |b|$.

(5) Demostrar que para todo $a, b \in \mathbb{R}$ se tiene $||a| - |b|| \leq |a - b|$

(6) Demuestre el recíproco del teorema 13.6.10.

(7) Demostrar que si $a|b$ y $a|c$, entonces $a|(b + c)$

(8) Demostrar que si b es positivo y no primo, entonces tiene un divisor positivo $d \leq \sqrt{b}$.

(9) Presentar la lista de todos los primos positivos menores de 100. (Sugerencia: Suprimir los múltiplos 2, 3, 5, 7 y usar el ejercicio(8))

(10) Si $a|b$, demostrar que $|a| \leq |b|$, cuando es $b \neq 0$.

13.7 EL ALGORITMO DE EUCLIDES

El proceso ordinario de dividir un entero a por otro b nos da un cociente q y un resto r . El resultado

$$\frac{a}{b} = q + \frac{r}{b}$$

puede expresarse sin usar explícitamente las fracciones, así

ALGORITMO DE LA DIVISIÓN: Para dos enteros a y b con $b > 0$ existen dos enteros q y r , tales que

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

13.7.1 IMAGEN GEOMÉTRICA. Si imaginamos los números enteros representados sobre el eje real, los posibles múltiplos bq de b forman un conjunto de puntos equidistantes sobre el eje



El punto respectivo de a debe caer en uno de los intervalos determinados por esos puntos, por ejemplo, en el intervalo bq y $b(q+1)$, excluyendo el punto $b(q+1)$. Esto significa que $a = bq + r$ siendo r menor que la amplitud b del intervalo. Esta imagen sugiere la siguiente demostración, basada solo en los postulados.

Existen ciertamente algunos múltiplos enteros de b que no exceden a a , por ejemplo, como $b > 0$, $b \geq 1$ así

$$(-|a|)b \leq -|a| \leq a$$

Por lo tanto, el conjunto de las diferencias $a - bx$ contiene por lo menos un entero no negativo, a saber $a - (-|a|)b$. De aquí, por el postulado de buena ordenación existe un mínimo no negativo para $a - bx$, al que llamaremos $a - bq = r$. Por construcción, $r \geq 0$; mientras que si $r \geq b$, entonces $a - b(q+1) = r - b \geq 0$ sería menor que $a - bq$, contra lo afirmado al elegir q . Concluimos pues que $0 \leq r < b$ y que $a = bq + (a - bq) = bq + r$.

□

13.7.2 COROLARIO. Dados los dos enteros a y b , quedan determinados unívocamente el cociente q y el resto r , que satisfacen a

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

DEMOSTRACIÓN. Suponiendo que sea $a = bq + r = bq' + r'$, verificándose $0 \leq r < b$ y $0 \leq r' < b$. Entonces $r - r' = b(q' - q)$ es en valor absoluto menor que b , y es múltiplo de b , luego debe ser cero. De aquí que $r = r'$, $bq = br'$, $q = q'$.

□

Frecuentemente debemos considerar conjuntos de enteros, semejantes a $\{\dots, -6, -3, 0, 3, 6, 9, \dots\}$ formados por todos los múltiplos de 3. Estos conjuntos tienen la propiedad de que la suma o diferencia de dos cualesquiera de ellos pertenece al conjunto. En general, un conjunto S de números enteros, se llama *cerrado* para la adición y *cerrado* para la sustracción, cuando S contiene la suma $a + b$ y la diferencia $a - b$ de dos enteros cualesquiera a y b de S . Todos los enteros pares (positivos, negativos y cero) forman un conjunto cerrado para suma y sustracción.

Más generalmente, el conjunto de todos los múltiplos xm de un entero m , es cerrado para la adición y sustracción, pues $xm \pm ym = (x \pm y)m$ es múltiplo de m . Ahora vamos a probar que estos conjuntos constituidos por los múltiplos de un entero son los únicos conjuntos de enteros que tienen dicha propiedad.

13.7.3 TEOREMA. Todo conjunto no vacío de números enteros, cerrado para la adición y sustracción consiste del cero o contiene un número positivo mínimo del cual son múltiplos todos los demás.

PRUEBA. Sea S el conjunto y supongamos ($S \neq \Phi$) que contiene un elemento $a \neq 0$, por definición S contendrá a la diferencia $a - a = 0$ y por lo tanto la diferencia $0 - a = -a$. Luego S contiene al menos un número positivo a ó $-a$. El principio de buena ordenación nos dice que en S hay un mínimo positivo b .

El conjunto S debe contener todos los múltiplos de b en efecto, procediendo por inducción se ve en primer lugar que contiene a $b \cdot 1$ y seguidamente si está bk tiene que estar $bk + b = b(k + 1)$. Los múltiplos negativos tal como $-bn = 0 - bn$ también están en S por ser diferencia entre 0 y nb . Pero S no puede contener enteros no múltiplos de b , pues si hubiera uno digamos a no múltiplo de b , estaría también en S el resto de la división de ambos, $r = a - bq$. Pero r no es negativo y es menor que b , que es el mínimo entero positivo en S , luego debe ser $r = 0$ y $a = bq$.

□

13.7.4 DEFINICIÓN. Un entero d se llama máximo común divisor (*m.c.d.*) de dos enteros a y b , si es simultáneamente divisor de a y b , y además es múltiplo de cualquier otro divisor común.

En el lenguaje objeto de la teoría de números, el *m.c.d.* debe cumplir las tres propiedades siguientes

$$\text{si } d = \text{m.c.d.}\{a, b\}, \quad d|a \wedge d|b, \text{ y } c|a \wedge c|b \Rightarrow c|d$$

Por ejemplo, 3 y -3 son máximos comunes divisores de 6 y 9 . De acuerdo con la definición, si hay varios *m.c.d.* de dos números, cada uno

de ellos debe dividir al otro, luego serán asociados y difieren sólo en el signo. Del par $\pm d$ de máximos comunes divisores de a y b el número positivo se indicará con el símbolo

$$m.c.d\{a, b\} = (a, b).$$

Nótese que el calificativo "máximo" en la definición de $m.c.d$ no significa en principio que $(m.c.d)$ tenga mayor magnitud que cualquier otro divisor común c , sino que $(m.c.d)$ es el múltiplo de cualquier tal c .

13.7.5 TEOREMA. Si dos enteros cualesquiera $a \neq 0$, $b \neq 0$, tienen un $m.c.d$ positivo (a, b) , entonces éste puede expresarse como

$$(a, b) = sa + tb \quad s, t \in \mathbb{Z}$$

Una expresión como $sa + tb$ es llamada una "combinación lineal" con coeficientes enteros.

PRUEBA. Consideremos los números de la forma $sa + tb$, para todos los casos

$$(s_1a + t_1b) \pm (s_2a + t_2b) = (s_1 \pm s_2)a + (t_1 \pm t_2)b$$

Por lo tanto, el conjunto S de todos los enteros de la forma $sa + tb$ es cerrado para la adición y sustracción, y por el teorema 13.7.3 estará constituido por los múltiplos de un número entero positivo $d = sa + tb$. Por esta fórmula, es claro que todo c factor común de a y b debe ser un factor común de d . Además los enteros dados $a = 1 \cdot a + 0 \cdot b$, $b = 0 \cdot a + 1 \cdot b$ pertenecen ambos a S , luego serán múltiplos del mínimo número d del conjunto S . En otras palabras, d es un divisor común al cual dividen todos los demás divisores comunes, luego $d = (a, b)$.

□

Análogamente, el conjunto M de todos los múltiplos comunes de a y b es cerrado para la adición y sustracción, su mínimo elemento positivo m es un múltiplo común que divide a todos los demás múltiplos comunes y se llama el mínimo común múltiplo ($m.c.m$) de a y b .

13.7.6 TEOREMA. Dos enteros cualesquiera a y b tienen un mínimo común múltiplo $m.c.m\{a, b\} = [a, b]$, el cual es divisor de todos los múltiplos comunes, siendo él a su vez un múltiplo común.

Para hallar explícitamente el $m.c.d$ de dos enteros a y b , se puede utilizar el llamado algoritmo de Euclides.

Sean a y b enteros positivos, ya que un entero negativo puede reemplazarse por su asociado positivo sin alterar el $m.c.d$ (o sea $m.cd(a, b) = m.c.d(-a, b)$). El algoritmo de la división da

$$a = bq_1 + r_1, \quad a \leq r_1 < b \quad (1)$$

Cualquier entero que divida a los enteros a y b , divide al resto r_1 , recíprocamente, todo divisor común de b y r_1 es divisor de a , como resulta por (1). Los divisores comunes del par a, b son pues, los mismos que los del par b, r_1 así que $(a, b) = (b, r_1)$. Esta reducción puede repetirse con b y r_1 , e iterar el proceso

$$\begin{aligned}
 b &= r_1q_2 + r_2 & 0 < r_2 < r_1 \\
 r_1 &= r_2q_3 + r_3 & 0 < r_3 < r_2 \\
 &\vdots & \vdots \\
 r_{n-2} &= r_{n-1}q_n + r_n & 0 < r_n < r_{n-1} \\
 r_{n-1} &= r_nq_{n+1}
 \end{aligned} \tag{2}$$

Como el resto disminuye constantemente, habrá finalmente un resto 0 como hemos indicado en la última igualdad. Este razonamiento nos dice que el *m.c.d* buscado es

$$(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n)$$

Pero la última igualdad de (2) muestra que r_n es divisor de r_{n-1} así que el *m.c.d* de ambos es el propio r_n . El *m.c.d* de dos enteros dados a, b , es el último resto distinto de cero que se obtiene aplicándole el algoritmo de Euclides.

El mismo algoritmo puede utilizarse para representar explícitamente al *m.c.d* como combinación lineal $sa + tb$. Esto se consigue expresando los restos sucesivos r_i mediante a y b en esta forma:

$$\begin{aligned}
 r_1 &= a - bq_1 = a + (-q_1)b \\
 r_2 &= b - q_2r_1 = (-q_2)a + (1 + q_1q_2)b \\
 &\vdots
 \end{aligned}$$

La forma de estas igualdades, indica que puede obtenerse r_n como combinación lineal de a y b con coeficientes enteros s y t en cuya expresión intervienen los cocientes q_i .

La forma $(a, b) = sa + tb$ del *m.c.d* es de gran utilidad. Una consecuencia importante es que si un número primo divide a un producto de dos factores, debe dividir por lo menos a uno de ellos.

13.7.7 TEOREMA. Si p es un numero primo, $p|ab \Rightarrow p|a \vee p|b$.

PRUEBA. Por definición de número primo, los únicos factores de p son ± 1 y $\pm p$. Si la conclusión $p|a$ es falsa, los únicos divisores comunes de p y a son ± 1 , así que 1 es un *m.c.d* de a y p , y por lo tanto, $1 = sa + tp$. Multiplicando por b resultará:

$$b = sab + tpb$$

Los dos términos de la derecha son divisibles por p luego b será divisible por p , que es la segunda alternativa del enunciado.

□

Si $(a, b) = 1$ diremos que a y b son primos entre sí. En otras palabras, dos enteros a y b son primos entre sí, si no tienen divisores comunes salvo ± 1 . La demostración del teorema 13.7.7 prueba también la siguiente generalización

13.7.8 TEOREMA. Si $(a, c) = 1$ y $c|ab$, entonces se debe tener $c|b$

De aquí resulta una consecuencia, relativa a un entero m que sea múltiplo de dos números primos entre sí a y c . Pues el número m que es de la forma $m = ad$, es divisible por c , así que por el teorema 13.7.8, será $c|d$ y $m = ad = a(cd')$ luego el producto ac divide a m . Esto demuestra

13.7.9 TEOREMA. Supuesto que $(a, c) = 1$, $a|m \wedge c|m \Rightarrow ac|m$.

13.8 EJERCICIOS

- (1) Mediante el algoritmo de Euclides, calcular el *m.c.d* de

(a) (14, 35)	(b) (11, 15)	(c) (180, 252)
(d) (2873, 6643)	(e) (4148, 7684)	(f) (1001, 7655)
- (2) Escribir (x, y) en la forma $sx + ty$ (s, t son enteros), en los tres primeros casos del ejercicio (1)
- (3) Demostrar que $(0, a) = |a|$ para cualquier entero a .
- (4) Si $a > 0$, demostrar que $(ac, ac) = a(b, c)$
- (5) Demostrar que $b|c$ y $|c| < b$, implica $c = 0$
- (6) (a) Demostrar que tres enteros cualesquiera, a, b, c , tienen un *m.c.d* que puede expresarse en la forma $sa + tb + uc$
- (b) Demostrar que $((a, b), c) = (a, (b, c)) = ((a, c), b)$

§14 TEOREMA FUNDAMENTAL DE LA ARITMÉTICA.

ENUNCIADO: Todo entero distinto de cero puede expresarse como el producto de ± 1 por factores primos positivos. Esta expresión es única, salvo el orden en que los factores se consideren.

Que todo entero a pueda escribirse como un tal producto, puede demostrarse descomponiéndolo sucesivamente en factores menores. Este proceso supone el segundo principio de inducción completa el cual enunciamos a continuación

Principio de inducción- segunda forma: Sea $p(n)$ una proposición condicional en la variable libre $n \in \mathbb{N}$ si

- (i) $p(0)$ es verdadera y
- (ii) $p(n+1)$ es verdadera cada vez que $p(n)$ es verdadera (es decir $(\forall n \in \mathbb{N})(p(n) \Rightarrow p(n+1))$).

Entonces $p(n)$ es verdadera para todo número natural, es decir, $(\forall n \in \mathbb{N})(p(n))$.

Sea $p(a)$ la proposición que dice: " a puede descomponerse en factores como expresa el enunciado del teorema". Si $a = 1$ ó si a es primo, $p(a)$ es evidentemente cierta. Si a no es un número primo tendrá un divisor positivo b , distinto de 1 y de a , así que $a = bc$ con $b < a$, $c < a$. Pero, de acuerdo con el segundo principio de inducción, podemos suponer que $p(b)$ y $p(c)$ son verdaderas, así que b y c puede expresarse como producto de factores primos

$$b = p_1 p_2 \cdots p_r, \quad c = q_1 q_2 \cdots q_s$$

obteniéndose para a la expresión completa.

$$a = bc = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

que es la forma requerida.

Para demostrar la unicidad, consideremos dos posibles descomposiciones en factores primos del entero a :

$$a = (\pm 1) p_1 p_2 \cdots p_m = (\pm 1) q_1 q_2 \cdots q_n$$

Como todos los números primos p_j y q_j son positivos, las unidades ± 1 de ambas descomposiciones han de ser iguales. El factor p_1 es un divisor de $a = \pm q_1 q_2 \cdots q_n$, así que la aplicación del teorema 13.7.7 asegura que p_1 divide por lo menos a su factor q_j de este producto. Como p_1 divide a q_j y los dos son primos, se deberá tener $p_1 = q_j$ ordenando el producto para que q_j aparezca de primero y simplificando p_1 con q_j queda

$$p_2 p_3 \cdots p_m = q'_2 q'_3 \cdots q'_n$$

donde los acentos indican los q_i en el nuevo orden. Podemos continuar este proceso hasta que en uno de los dos miembros de la igualdad no quede ningún factor. Tampoco podrán quedar en el otro, así $m = n$. Hemos pues identificado las dos descomposiciones, sin más que reordenar los factores del segundo miembro, como asegurábamos en el teorema de unicidad. En una descomposición puede aparecer un número primo p varias veces. Agrupando los factores, podemos escribir

$$a = \pm p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}, \text{ siendo } (0 < p_1 < p_2 < \cdots < p_n)$$

El teorema de unicidad demuestra, que el exponente e_i , corresponde al factor primo p_i , queda determinado de modo único para cada entero a .

□

14.1 EJERCICIOS

1. Describir un proceso sistemático para hallar el *m.c.d* y el *m.c.m* de dos enteros, de los que se conoce la descomposición en factores primos, ilustrándolo con $a = 216$, $b = 360$ y $a = 144$, $b = 625$ (Sugerencia: Es conveniente usar los exponentes 0 para los factores primos que dividen a uno de los números a o b , pero no al otro)

2. Si $V_p(a)$ indica el exponente de la más alta potencia del primo p divisor de a , demostrar las fórmulas

$$(1) V_p(a + b) \geq \min\{V_p(a), V_p(b)\}$$

$$(2) V_p((a, b)) = \min\{V_p(a), V_p(b)\} \quad ((,) = m.c.d)$$

$$(3) V_p(a \cdot b) = V_p(a) + V_p(b)$$

$$(4) V_p([a, b]) = \max\{V_p(a), V_p(b)\}. \quad ([,] = m.c.m)$$

3. Si $\|a\| = 2^{-V_2(a)}$, para V_p como en el ejercicio 2, demostrar que

$$\|ab\| = \|a\| \cdot \|b\| \quad \text{y} \quad \|a + b\| \leq \max(\|a\|, \|b\|)$$

4. Mediante las fórmulas del ejercicio 2, demostrar que para números enteros positivos a y b , $ab = (a, b)[a, b]$.

5. Demostrar que el número de primos es infinito (Euclídes)(Sugerencia: Si p_1, p_2, \dots, p_n son n primos, el producto $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ no es divisible por ninguno de estos primos)

6. Si un producto mn positivo es un cuadrado y si $(m, n) = 1$, demostrar que m y n son ambos cuadrados.

§15 CONGRUENCIAS

Al numerar las horas del día, se acostumbra a contar sólo hasta 12 y volver a empezar. Esta sencilla idea de prescindir de los múltiplos de un número fijo, 12 en este caso, es la base de la noción aritmética de congruencias. Diremos que dos enteros son congruentes "módulo 12" si difieren en un entero múltiplo de 12. Por ejemplo 7 y 19 son congruentes y se escribe

$$7 \equiv 19 \pmod{12}$$

15.1 DEFINICIÓN. $a \equiv b \pmod{m}$ significa que $m|(a - b)$.

Se puede decir igualmente que $a \equiv b \pmod{m}$, cuando la diferencia $a - b$ pertenece al conjunto de los números múltiplos de m . Todavía cabe otra definición, basada en que el resto de la división de a por m es único. Podemos, pues establecer lo que sigue:

15.2 TEOREMA. La condición necesaria y suficiente para que dos enteros a y b sean congruentes módulo m , es que den el mismo resto al dividirlos por m .

PRUEBA. Como $a \equiv b \pmod{m}$, si y sólo si $a \equiv b \pmod{-m}$ bastará demostrar este teorema en el caso $m > 0$. Supongamos primero que

$a \equiv b(\text{mod}.m)$, entonces $a - b = cm$ para algún entero c . Dividiendo b por m , se obtendrá un resto r , dado por $b - mq = r$, $0 \leq r < m$. entonces

$$a = b + cm = (qm + r) + cm = (q + c)m + r$$

Esta ecuación indica que r es el resto de a al dividirlo por m ; sea, que a y b dan el mismo resto al dividirlos por m .

Recíprocamente, supongamos que el resto es igual y que por ende

$$a = mq + r, \quad b = mq' + r$$

En este caso $a - b = (q + q')m \Leftrightarrow (a - b)|m$, así que $a \equiv b(\text{mod}.m)$

□

La relación de congruencia para un módulo fijo m tiene para enteros cualesquiera a, b, c las siguientes propiedades que recuerdan propiedades análogas de la igualdad

Reflexiva: $a \equiv a(\text{mod}.m)$

Simétrica: $a \equiv b(\text{mod}.m) \Rightarrow b \equiv a(\text{mod}.m)$

Transitiva: $a \equiv b(\text{mod}.m) \wedge b \equiv c(\text{mod}.m) \Rightarrow a \equiv c(\text{mod}.m)$

Cada una de estas leyes se demuestra con la definición de congruencia.

La ley de simetría así dada, requiere simplemente que

$$m|(a - b) \Rightarrow m|(b - a)$$

La hipótesis es $a - b = dm$ y la conclusión $m|(b - a)$, puesto que $b - a = (-d)m$.

La relación de congruencia para un módulo fijo tiene otra propiedad que también recuerda a las de la igualdad; las sumas y productos de enteros congruentes son también congruentes.

15.3 TEOREMA. Si $a \equiv b(\text{mod}.m)$ para todo entero x resulta: $a + x \equiv b + x(\text{mod}.m)$, $ax \equiv bx(\text{mod}.m)$, $(-a) \equiv (-b)(\text{mod}.m)$.

También aquí la prueba se reduce a recordar la definición. Así la hipótesis es que $a - b = km$ para algún k ; de aquí podemos obtener las conclusiones en la forma

$$m|(a + x - b - x), \quad m|(ax - bx), \quad m|(-a + b)$$

La ley de simplificación, válida en las igualdades, no lo es en las congruencias. Así $2 \cdot 7 \equiv 2 \cdot 1(\text{mod}.12)$, pero no es $7 \equiv 1(\text{mod}.12)$.

Esto sucede por ser 2 divisor del módulo, así que la diferencia $2 \cdot 7 - 2$ será divisible por 12 en tanto se conserve el factor 2. Puede enunciarse la ley de simplificación algo modificada.

15.4 TEOREMA. Si c es un número primo con m

$$ca \equiv cb(\text{mod}.m) \Rightarrow a \equiv b(\text{mod}.m).$$

PRUEBA. De acuerdo con la definición, la hipótesis nos dice que $m|(ac - ab)$, o sea, $m|c(a - b)$ y por ser m primo con c usando el teorema 13.7.8 resulta que $m|(a - b)$, esto es $a \equiv b(\text{mod}.m)$.

□

El estudio de las ecuaciones lineales puede extenderse a las congruencias

15.5 TEOREMA. Si c es primo con m , la congruencia $cx \equiv b \pmod{m}$ tiene una solución entera x . Dos soluciones cualesquiera x_1 y x_2 son congruentes módulo m .

PRUEBA. Por hipótesis, $(c, m) = 1$, luego $1 = sc + tm$ para dos enteros convenientes s y t . Multiplicando por b tenemos

$$b = bsc + btm$$

Esto último se puede escribir así

$$b - bsc = (bt)m \Leftrightarrow b \equiv (bs)c \pmod{m}.$$

Esto expresa que $x = bs$ es la solución de $b \equiv cx \pmod{m}$.

Por otra parte, dos soluciones x_1 y x_2 de esta congruencia se tiene

$$b \equiv cx_1 \pmod{m} \wedge b \equiv cx_2 \pmod{m}$$

por ser la relación de congruencia simétrica y transitiva se tiene que

$$cx_1 \equiv cx_2 \pmod{m}$$

Como c es primo con m , se puede simplificar (15.4) y resulta $x_1 \equiv x_2 \pmod{m}$.

□

Un caso particular importante se presenta cuando el módulo m es primo, entonces todo entero no divisible por m es primo con él. Esto nos demuestra el siguiente resultado.

15.6 COROLARIO. Si p es primo y $c \not\equiv 0 \pmod{p}$ entonces $cx \equiv b \pmod{p}$ tiene solución única módulo p .

Consideremos ahora congruencias simultáneas.

15.7 TEOREMA. Si los módulos m_1 y m_2 son primos entre si, las congruencias

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}$$

tienen una solución común, x . Dos soluciones cualesquiera son congruentes módulo $m_1 m_2$.

PRUEBA. La primera congruencia tiene como solución b_1 ; la solución más general es $x = b_1 + ym_1$ para algún entero y . Esta debe verificar la segunda congruencia

$$b_1 + ym_1 \equiv b_2 \pmod{m_2}$$

o

$$ym_1 \equiv (b_2 - b_1) \pmod{m_2}$$

como m_1 y m_2 son primos entre si, podemos resolver esta congruencia por el método de (15.5).

Supongamos ahora que x y x' son dos soluciones del sistema, se tendrá

$$x' - x \equiv 0 \pmod{m_1} \quad \text{y} \quad x' - x \equiv 0 \pmod{m_2}$$

Como m_1 y m_2 son primos entre si, la diferencia $x' - x$ es divisible por $m_1 m_2$. Así que $x \equiv x' \pmod{m_1 m_2}$.

El mismo método de resolución se aplica a dos o más congruencias de la forma $a_i x \equiv b_i \pmod{m_i}$ con $m.c.d\{a_i, m_i\} = 1$ y con los módulos primos entre si dos a dos.

15.8 EJERCICIOS.

1. Demuestre las siguientes propiedades de la divisibilidad

- (a) $n|n \quad \forall n \in \mathbb{Z}$
- (b) $d|n \wedge n|m$ implica $d|m$; $d, n, m \in \mathbb{Z}$
- (c) $d|n \wedge d|m \Rightarrow d|(an + bm)$; $d, n, m, a, b \in \mathbb{Z}$
- (d) $d|n \Rightarrow ad|an$; $a, d, n \in \mathbb{Z}$
- (e) $ad|an \wedge a \neq 0, \Rightarrow d|n$
- (f) $1|n \quad \forall n \in \mathbb{Z}$
- (g) $n|0 \quad \forall n \in \mathbb{Z}$
- (h) $0|n \Rightarrow n = 0$
- (i) $d|n \wedge n \neq 0 \Rightarrow |d| \leq |n|$
- (j) $d|n \wedge n|d \Rightarrow |d| = |n|$
- (k) $d|n \wedge d \neq 0 \Rightarrow \left(\frac{n}{d}\right)|n$

En lo que sigue las letras a, b, c, \dots, x, y, z representan números enteros. Probar que las siguientes afirmaciones son verdaderas

- (2) Si $(a, b) = 1 \wedge c|a \wedge d|b$, entonces $(c, d) = 1$ ($(,) = m.c.d$)
- (3) Si $(a, b) = (a, c) = 1$. entonces $(a, bc) = 1$
- (4) Si $(a, b) = 1$ entonces $(a + b, a - b)$ es ó 1, ó 2
- (5) Si $(a, b) = 1$ y si $d|(a + b)$, entonces $(a, d) = (b, d) = 1$
- (6) Si $(a, b) = 1$ entonces $(a + b, a^2 - ab + b^2)$ es ó 1, ó 3.
- (7) Si $(a, b) = 1$ entonces $(a^n, b^k) = 1 \quad \forall n \geq 1, \forall k \geq 1$.
- (8) Un número racional $\frac{a}{b}$ con $(a, b) = 1$ es llamada una fracción reducible. Si la suma de dos fracciones reducibles es un número entero, digamos $\frac{a}{b} + \frac{c}{d} = n$, probar que $|a| = |d|$.
- (9) Para cada una de las afirmaciones siguientes dar una demostración ó hallar un contra-ejemplo
 - (a) Si $b^2|n$ y $a^2|n \wedge a^2 \leq b^2$, entonces $a|b$.
 - (b) Si b^2 es el cuadrado más grande que es divisor de n , entonces $a^2|n \Rightarrow a|b$

§16 CLASES RESIDUALES

Desde la más remota antigüedad, el hombre ha distinguido los enteros "pares" $2, 4, 6, 8, \dots$, de los "impares" $1, 3, 5, 7, \dots$. Las siguientes leyes de cálculo entre pares e impares son también conocidas:

$$\begin{aligned} \text{par} + \text{par} &= \text{impar} + \text{impar} = \text{par}, & \text{par} + \text{impar} &= \text{impar} \\ \text{par} \cdot \text{par} &= \text{par} \cdot \text{impar} = \text{par}, & \text{impar} \cdot \text{impar} &= \text{impar} \end{aligned}$$

Estas igualdades pueden considerarse, no como teorema relativo a los enteros ordinarios, sino como definición de dos operaciones "adición" y "multiplicación", en una nueva álgebra de los dos elementos "par" e "impar"

Esta álgebra puede también considerarse como un álgebra de restos módulo 2. Los enteros pares son aquellos que divididos por 2 dan resto 0, mientras que los impares dan resto 1. Estos dos restos, pueden sumarse y multiplicarse del modo ordinario, cuidando luego de reemplazar el resultado por su resto módulo 2. Esto nos da una tabla

$$\begin{array}{ll} 0 + 0 = 1 + 1 = 0 & 0 + 1 = 1 \\ 0 \cdot 0 = 0 \cdot 1 = 0 & 1 \cdot 1 = 1 \end{array}$$

que en esencia es la misma tabla para pares e impares. Inversamente, puede decirse que la igualdad $1 + 1 = 0$ es un nuevo modo de escribir la congruencia $1 + 1 \equiv 0 \pmod{2}$.

Un álgebra análoga J_n , de n elementos, resultará partiendo de las congruencias módulo n . En la última sección (§15) hemos visto que la congruencia tiene las propiedades características de la igualdad, reflexiva, simétrica y transitiva, y las congruencias pueden ser multiplicadas y sumadas, como las igualdades. En efecto, el teorema 15.4 muestra que si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$ resulta

$$a + c \equiv b + d \pmod{n} \quad \text{y} \quad ac \equiv bd \pmod{n} \quad (1)$$

El álgebra J_n de los elementos módulo n se obtiene reemplazando la congruencia módulo n por la igualdad. Según (1) la suma y el producto de dos enteros están unívocamente determinados con este nuevo significado de igualdad. Cualquier entero es igual a uno de los n restantes posibles

$$0, 1, 2, \dots, n - 1$$

Dos de estos restos pueden sumarse (o multiplicarse) en la forma habitual reduciendo luego el resultado a su resto módulo n , del que viene a ser "igual"

Las tablas para el caso $n = 5$ son las siguientes

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

16.1 TEOREMA. En el sistema J_n de enteros módulo n , son válidas para la adición y multiplicación todas las propiedades enumeradas a continuación:

- (i) $\langle J_n, \text{adición} \rangle$ grupo abeliano
- (ii) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ para todo $x, y, z \in J_n$
- (iii) $x \cdot y = y \cdot x$ para todo $x, y \in J_n$
- (iv) Existe $1 \in J_n$ tal que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in J_n$
- (v) $x \cdot (y + z) = x \cdot y + x \cdot z$ para todo $x, y, z \in J_n$

y no cumple la ley de simplificación (*), es de notar que se entenderá $x = y$ si y sólo si $x \equiv y(mod.n)$.

(*) para la multiplicación módulo n

PRUEBA. Acabamos de ver que dos elementos cualesquiera definen unívocamente su suma y su producto. Consideremos la ley distributiva. Cómo

$$a(b + c) = ab + ac$$

para enteros cualesquiera se debe tener

$$a(b + c) \equiv (ab + ac)(mod.n)$$

que es la ley distributiva para nuestro nuevo concepto de igualdad en J_n . El mismo tipo de razonamiento se aplica a las otras leyes, que se expresan mediante identidades entre sumas y elementos negativos. Los primeros miembros de cada identidad son congruentes módulo n con los segundos miembros. Por lo cual las correspondientes expresiones en J_n son iguales.

El único postulado que no se conserva inalterado es la ley de simplificación del producto. Esta ley equivale a asegurar la no existencia de divisores de 0 en J_n , así que $ab = 0$ deberá implicar $a = 0$, ó, $b = 0$. Pero estas igualdades se traducen en J_n por congruencias entre enteros, de modo que tal ley equivaldría a decir:

$$\text{Si } ab \equiv 0(mod.n) \text{ entonces } a \equiv 0(mod.n) \text{ ó } b \equiv 0(mod.n)$$

Esto, a su vez equivale a decir que

$$n|ab \Rightarrow n|a, \text{ ó, } n|b$$

Pero esta propiedad es cierta si n es primo. Si n no es primo, admite una descomposición $n = ab$ sin que $n|a$ ni $n|b$ (como $6 = 3 \cdot 2$, $6|3 \cdot 2$ sin, $6|3$ ni $6|2$). Luego, en este caso J_n no satisface la ley de simplificación.

16.2 Para que la ley de simplificación de la multiplicación sea válida en J_n , es necesario y suficiente que n sea un número primo.

Hay otro modo más sistemático para construir el álgebra de los enteros módulo n . El artificio de reemplazar congruencia por igualdad significa, esencialmente, que todos los enteros que dan el mismo resto en su división por n pueden agruparse y cada grupo viene a ser un "número" nuevo. Cada uno de tales grupos se llama una "clase residual". Para el módulo 5 hay cinco clases residuales, correspondientes a los posibles restos

$$0, \quad 1, \quad 2, \quad 3, \quad 4$$

algunas de estas clases son:

$$\begin{aligned} \dot{1} &= \{ \dots, -14, -9, -4, 1, 6, 11, 16, \dots \} \\ \dot{2} &= \{ \dots, -13, -8, -3, 2, 7, 12, 17, \dots \} \\ \dot{3} &= \{ \dots, -12, -7, -2, 3, 8, 13, 18, \dots \} \end{aligned}$$

Para cada módulo n la clase residual r_n determinada por un resto r con $0 \leq r < n$, está formada por todos los enteros a , que dan el mismo resto r en su división por n . Todos los enteros perteneciente a la misma clase, son congruentes módulo n . Hay n clases residuales módulo n , a saber

$$0_n, 1_n, 2_n, \dots, (n-1)_n$$

Las operaciones algebraicas en J_n pueden efectuarse directamente sobre estas clases. Supongamos que la suma de dos restos r y s dan en J_n un resto t , o sea

$$r + s \equiv t \pmod{n}$$

El mismo resultado se obtendria si en vez de tomar los restos r y s , tomásemos otros elementos en las clases correspondientes. Si a está en r_n y b en s_n , entonces $a + b$ está en la clase t_n , que contiene a su suma t , pues

$$a \equiv r \pmod{n} \wedge b \equiv s \pmod{n} \Rightarrow a + b \equiv r + s \equiv t \pmod{n}$$

En general el álgebra J_n puede definirse como el álgebra de las clases residuales; para sumar (ó multiplicar) dos clases se eligen dos elementos a y b representativos de estas clases y se busca la clase residual que contiene la suma (ó al producto) de estos elementos representativos. Si a_n indica la clase residual que contiene a a , ésta puede formularse así:

$$(a + b)_n = a_n + b_n, \quad (ab)_n = a_n b_n$$

Por ejemplo, la suma $1_5 + 2_5 = 3_5$ de las clases residuales escritas antes puede hallarse sumando dos elementos elegidos como representantes de

la mismas, $6 + (-13)$ por ejemplo, obteniéndose así (-7) , que está en la clase 3_5 . Otras elecciones como

$$-9 + (-3) = -12, \quad 11 + 7 = 18, \quad -14 + 17 = 3$$

darán siempre la misma suma 3_5 .

Las clases residuales que hemos definido mediante los restos, pueden definirse también directamente mediante las congruencias según el método que será tratado por los lectores interesados.

16.2 EJERCICIOS

(1) Resolver las siguientes congruencias

$$(a) 3x \equiv 2 \pmod{5} \quad (b) 2x \equiv 4 \pmod{10}$$

$$(c) 243x + 17 \equiv 101 \pmod{725} \quad (d) 4x + 3 \equiv 4 \pmod{5}$$

$$(e) 6x + 3 \equiv 4 \pmod{10} \quad (f) 6x + 3 \equiv 1 \pmod{10}$$

(2) Demostrar que la relación $a \equiv b \pmod{m}$ es reflexiva y transitiva.

(3) Demostrar directamente que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ implica $a + c \equiv b + d \pmod{m}$ y $ac \equiv bd \pmod{m}$

(4) a) Demostrar que la congruencia $ax \equiv b \pmod{m}$ tiene solución si y sólo si, $(a, m) | b$. [$(,) = m.c.d$]

b) Demostrar que si $(a, m) | b$, la congruencia tiene exactamente (a, m) soluciones incongruentes módulo m . [Sugerencia: Dividir a, b y m por (a, m) .]

(5) Si m es entero, mostrar que $m^2 \equiv 0$ ó $1 \pmod{m}$

(6) Demostrar que $x^2 \equiv 35 \pmod{100}$ no tiene solución.

(7) Demostrar que si $x^2 \equiv n \pmod{65}$ tiene una solución, también tiene solución $x^2 \equiv 65 - n \pmod{65}$. Generalizar este resultado.

(8) Si x es un número impar no divisible por 3, mostrar que $x^2 \equiv 1 \pmod{24}$

(9) Resolver las congruencias simultáneas:

$$a) x \equiv 2 \pmod{5} \quad 3x \equiv 1 \pmod{8}$$

$$b) 3x \equiv 2 \pmod{5} \quad 2x \equiv 1 \pmod{3}$$

(10) En una isla desierta, cinco hombres y un mono recogen cocos durante el día, y después duermen. El primer hombre se despierta y decide tomar su parte. Divide los cocos en cinco grupos iguales, y le sobra un coco, que lo da al mono. Después toma su parte y vuelve a dormirse. Entonces despierta el segundo hombre, y haciendo un montón con los cocos que quedaron, lo divide en cinco partes iguales, y le sobra un coco, que da al mono. Sucesivamente ocurre lo mismo con cada uno de los tres hombres restantes. Encontrar el número mínimo de cocos que formaban el montón original. (Sugerencia: Añadir 4 cocos).

(11) Construir las tablas de adición y multiplicación para J_3 y J_4 .

(12) Calcular en J_7 : $(3 \cdot 4) \cdot 5$, $3 \cdot (4 \cdot 5)$, $3 \cdot (4 + 5)$, $3 \cdot 4 + 3 \cdot 5$

(13) Hallar todos los divisores de cero en J_{26} y J_{24} .

(14) Determinar exactamente el conjunto de sumas $x + y$ y productos xy , para x en 4_8 , y en 4_8 ¿Cómo están relacionados los conjuntos $4_8 + 4_8$ y $4_8 \cdot 4_8$?

(15) Demostrar la ley asociativa para la adición de clases residuales, como en el caso de las congruencias módulo n .

§17. NÚMEROS COMPLEJOS.

Hemos llegado a nuestro último párrafo, dedicado al estudio del sistema de los números complejos, el cual presentaremos, siguiendo el formato ideado por el matemático irlandés Sir William R. Hamilton, en la forma más completa posible.

$$\mathbb{C} = \{(x_1, x_2) \in \mathbb{R} \times \mathbb{R} / x_1, x_2 \text{ son reales}\}$$

Se define en \mathbb{C} la adición y la multiplicación en la forma

$$\begin{aligned} + : \mathbb{C} \times \mathbb{C} &\longrightarrow \mathbb{C} \\ (x, y) &\mapsto x + y = (x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \\ \cdot : \mathbb{C} \times \mathbb{C} &\longrightarrow \mathbb{C} \\ (x, y) &\mapsto x \cdot y = (x_1, x_2) \cdot (y_1, y_2) = (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1) \end{aligned}$$

Además en \mathbb{C} se define la igualdad así

$$x \in \mathbb{C}, y \in \mathbb{C}, x = y \Leftrightarrow (x_1, x_2) = (y_1, y_2) \Leftrightarrow x_1 = y_1 \wedge x_2 = y_2$$

Tomando $x \in \mathbb{C}$, entonces $x = (x_1, x_2)$ en esta representación

$$\begin{aligned} x_1 &\text{ es llamado la parte real de } x \\ x_2 &\text{ es llamado la parte imaginaria de } x \end{aligned}$$

17.1 TEOREMA. Con la suma y multiplicación así definida en \mathbb{C} , entonces se tiene que \mathbb{C} es un cuerpo. Llamado el cuerpo de los números complejos.

DEMOSTRACIÓN. (i) $\langle \mathbb{C}, + \rangle$ es un grupo abeliano, en efecto

$$\begin{aligned} \text{G1. } (x + y) + z &= (x_1 + y_1, x_2 + y_2) + (z_1, z_2) = ((x_1 + y_1) + z_1, (x_2 + y_2) + z_2) \\ &= (x_1 + (y_1 + z_1), x_2 + (y_2 + z_2)) = (x_1, x_2) + (y_1 + z_1, y_2 + z_2) \\ &= x + [(y_1, y_2) + (z_1, z_2)] = x + (y + z) \end{aligned}$$

$$\begin{aligned} \text{G2. } x + y &= (x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) = (y_1 + x_1, y_2 + x_2) \\ &= (y_1, y_2) + (x_2 + x_1) = y + x \end{aligned}$$

$$\text{G3. } a + x = a \Leftrightarrow (a_1, a_2) + (x_1, x_2) = (a_1 + x_1, a_2 + x_2) = (a_1, a_2)$$

por la igualdad entre parejas se tiene

$$a_1 + x_1 = a_1 \wedge a_2 + x_2 = a_2$$

Pero en \mathfrak{R} estas ecuaciones tienen por solución única

$$x_1 = x_2 = 0$$

Luego $x = (0, 0)$ es el módulo aditivo

$$G4. \quad a + x = 0 \Leftrightarrow (a_1, a_2) + (x_1, x_2) = (0, 0) \Leftrightarrow (a_1 + x_1, a_2 + x_2) = (0, 0)$$

por la igualdad entre parejas se recibe

$$a_1 + x_1 = 0 \wedge a_2 + x_2 = 0$$

Cuyas soluciones en \mathfrak{R} son

$$x_1 = -a_1 \wedge x_2 = -a_2$$

Luego $x = (-a_1, -a_2) = -a$ teniéndose la invertiva de la adición

(ii) $\langle \mathbb{C}, \cdot \rangle$ es también un grupo abeliano, efectivamente se tiene que:

$$\begin{aligned} G1. \quad (x \cdot y) \cdot z &= [(x_1, x_2) \cdot (y_1, y_2)] \cdot (z_1, z_2) = (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1)(z_1, z_2) \\ &= ((x_1y_1 - x_2y_2)z_1 - (x_1y_2 + x_2y_1)z_2, (x_1y_1 - x_2y_2)z_2 + (x_1y_2 + x_2y_1)z_1) \\ &= (x_1y_1z_1 - x_2y_2z_1 - x_1y_2z_2 - x_2y_1z_2, x_1y_1z_2 - x_2y_2z_2 + x_1y_2z_1 + x_2y_1z_1) \quad (1) \end{aligned}$$

Por otra parte tenemos

$$\begin{aligned} x(yz) &= (x_1, x_2)[(y_1, y_2) \cdot (z_1, z_2)] = (x_1, x_2)(y_1z_1 - y_2z_2, y_1z_2 + y_2z_1) \\ &= (x_1(y_1z_1 - y_2z_2) - x_2(y_1z_2 + y_2z_1), x_1(y_1z_2 + y_2z_1) + x_2(y_1z_1 - y_2z_2)) \\ &= (x_1y_1z_1 - x_1y_2z_2 - x_2y_1z_2 - x_2y_2z_1, x_1y_1z_2 + x_1y_2z_1 + x_2y_1z_1 - x_2y_2z_2) \quad (2) \end{aligned}$$

comparando (1) y (2), y usando la definición de igualdad se concluye que

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$\begin{aligned} G2. \quad x \cdot y &= (x_1, x_2) \cdot (y_1, y_2) = (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1) = \\ &= (y_1x_1 - y_2x_2, y_2x_1 + y_1x_2) \\ &= (y_1, y_2) \cdot (x_1, x_2) = y \cdot x \end{aligned}$$

teniéndose la abelianidad del producto.

G3. Cálculo del módulo multiplicativo. Suponiendo $a \neq 0$;

$$a \cdot x = a \Leftrightarrow (a_1, a_2)(x_1, x_2) = (a_1, a_2)$$

lo cual es completamente equivalente a

$$(a_1x_1 - a_2x_2, a_1x_2 + a_2x_1) = (a_1, a_2)$$

de donde se desprende el siguiente sistema simultáneo de ecuaciones lineales

$$a_1x_1 - a_2x_2 = a_1$$

$$a_1x_2 + a_2x_1 = a_2$$

el cual resolvemos por el método de eliminación

$$a_1a_2x_1 - a_2^2x_2 = a_1a_2$$

$$-a_1a_2x_1 - a_1^2x_2 = -a_1a_2$$

entonces

$$-(a_1^2 + a_2^2)x_2 = 0$$

como $a_1^2 + a_2^2 \neq 0$, pues $a \neq 0$, en general se tiene que $x_2 = 0$.

Ahora

$$a_1^2x_1 - a_1a_2x_2 = a_1^2$$

$$a_2^2x_1 + a_1a_2x_2 = a_2^2$$

entonces recibimos

$$(a_1^2 + a_2^2)x_1 = a_1^2 + a_2^2 \Rightarrow x_1 = 1$$

así $x = (1, 0)$ es el módulo multiplicativo.

G4. Dado $a \neq 0$ calculemos su inverso multiplicativo;

$$a \cdot x = (1, 0) \Leftrightarrow (a_1, a_2)(x_1, x_2) = (1, 0)$$

lo cual podemos también escribir así

$$(a_1x_1 - a_2x_2, a_1x_2 + a_2x_1) = (1, 0)$$

de la definición de igualdad, recibimos el siguiente sistema simultáneo de ecuaciones

$$a_1x_1 - a_2x_2 = 1$$

$$a_1x_2 + a_2x_1 = 0$$

usando el método de eliminación tenemos

$$a_1^2x_1 - a_1a_2x_2 = a_1$$

$$a_2^2x_1 + a_1a_2x_2 = 0$$

de donde se tiene

$$(a_1^2 + a_2^2)x_1 = a_1 \Leftrightarrow x_1 = \frac{a_1}{a_1^2 + a_2^2}$$

y por otra parte

$$x_2 = -\frac{a_2}{a_1}x_1 = -\frac{a_2}{a_1^2 + a_2^2}$$

así

$$x_1 = \left(\frac{a_1}{a_1^2 + a_2^2}, -\frac{a_2}{a_1^2 + a_2^2} \right) = (a_1, a_2)^{-1} = a^{-1}$$

(iii) Se tiene la ley distributiva, en efecto

$$\begin{aligned} x(y + z) &= (x_1, x_2)[(y_1, y_2) + (z_1, z_2)] = (x_1, x_2)(y_1 + z_1, y_2 + z_2) \\ &= (x_1(y_1 + z_1) - x_2(y_2 + z_2), x_1(y_2 + z_2) + x_2(y_1 + z_1)) \\ &= (x_1y_1 + x_1z_1 - x_2y_2 - x_2z_2, x_1y_2 + x_1z_2 + x_2y_1 + x_2z_1) \end{aligned}$$

Ahora, por otro lado

$$\begin{aligned} xy + xz &= (x_1, x_2)(y_1, y_2) + (x_1, x_2)(z_1, z_2) = \\ &= (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1) + (x_1z_1 - x_2z_2, x_1z_2 + x_2z_1) \\ &= (x_1y_1 - x_2y_2 + x_1z_1 - x_2z_2, x_1y_2 + x_2y_1 + x_1z_2 + x_2z_1) \end{aligned}$$

De la definición de igualdad se sigue que

$$x(y + z) = xy + xz.$$

□

17.2 VALOR ABSOLUTO DE UN NÚMERO COMPLEJO

Vamos a generalizar el concepto de valor absoluto dado para los números reales

17.2.1 DEFINICIÓN. Si $x = (x_1, x_2)$, entonces definimos el módulo o valor absoluto de x , como el número real no negativo $|x|$ dado por

$$|x| = \sqrt{x_1^2 + x_2^2}$$

17.2.2 TEOREMA. El valor absoluto así definido cumple las siguientes propiedades

- (a) $|(0, 0)| = 0$, y $|x| > 0$ si $x \neq 0$
 (b) $|xy| = |x||y|$ para todo $x, y \in \mathbb{C}$
 (c) $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$ si $y \neq 0$
 (d) $|(x_1, 0)| = |x_1|$

DEMOSTRACIÓN. Las igualdades (a) y (d) son inmediatas

Para demostrar (b) escribimos $x = (x_1, x_2)$, $y = (y_1, y_2)$ así que

$$xy = (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1)$$

obteniendo

$$\begin{aligned} |xy|^2 &= (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2 \\ &= x_1^2y_1^2 + x_2^2y_2^2 + x_1^2y_2^2 + x_2^2y_1^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2) \\ &= |x|^2|y|^2 \end{aligned}$$

La ecuación (c) puede deducirse de (b) escribiéndola de la forma

$$|x| = |y| \left| \frac{x}{y} \right|$$

Geométricamente, $|x|$ representa la longitud del segmento que une el origen con el punto x . Más generalmente, $|x - y|$ es la distancia entre los puntos x y y colocados en un plano cartesiano.

□

17.2.3 DEFINICIÓN. Si $a \in \mathfrak{R}$ entonces a puede considerarse como un número complejo imponiendo la identificación

$$a = (a, 0)$$

en esta forma $\mathfrak{R} \subseteq \mathbb{C}$, diciéndose que los reales quedan encajados dentro de los complejos.

17.2.4 TEOREMA. La ecuación $x^2 = (-1, 0) = -1$ tiene por solución a $(0, 1)$ y $(0, -1)$

PRUEBA. Efectivamente, supongamos que $x = (x_1, x_2)$ y que

$$x^2 = (x_1, x_2)(x_1, x_2) = -1 = (-1, 0)$$

Por la definición de multiplicación se recibe

$$(x_1^2 - x_2^2, 2x_1x_2) = (-1, 0)$$

de donde se desprende el siguiente sistema cuadrático

$$\begin{aligned} x_1^2 - x_2^2 &= -1 \\ 2x_1x_2 &= 0 \end{aligned}$$

la segunda de estas dos ecuaciones afirma que

$$x_1 = 0 \quad \text{ó} \quad x_2 = 0$$

Si $x_1 = 0$ en la primera ecuación se tiene

$$x_2^2 = 1 \Leftrightarrow x_2 = \pm 1$$

en este caso se tendría que

$$x = (0, 1) \quad \text{ó} \quad x = (0, -1)$$

que son las dos soluciones deseadas.

Si $x_2 = 0$, entonces de la primera ecuación tendríamos

$$x_1^2 = -1$$

como $x_1 \in \mathfrak{R}$, esta ecuación no tiene solución.

□

17.2.6 DEFINICIÓN. Es universalmente denotado el número complejo $(0, 1)$, solución de $x^2 = -1$, con la letra i , así

$$i = (0, 1).$$

En esta forma si $x \in \mathbb{C}$ se sigue de 17.2.4 que

$$\begin{aligned} x &= (x_1, x_2) = (x_1, 0) + (0, x_2) = x_1 + (x_2, 0)(0, 1) \\ &= x_1 + x_2i \end{aligned}$$

que es la forma clásica para un número complejo.

En esta forma si $x \in \mathbb{C}$ (se dice si x es un número complejo) entonces

$$x = (a, b) = a + ib$$

a es llamado la parte real y se nota

$$a = \operatorname{Re} x$$

b se le llama la parte imaginaria y se le nota

$$b = \operatorname{Im} x$$

Una primera operación que se define en \mathbb{C} , es llamada **conjugación** la cual consiste en cambiarle el signo a la parte imaginaria , es decir,

$$\begin{aligned} \operatorname{conj} : \mathbb{C} &\longrightarrow \mathbb{C} \\ z = a + ib &\mapsto \bar{z} = a - ib \end{aligned}$$

Son propiedades de la conjugación las siguientes:

1. $\overline{z \pm w} = \bar{z} \pm \bar{w}$
2. $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
3. $\overline{\bar{z}} = z$
4. $\overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}$
5. $\operatorname{Re} z = \frac{z + \bar{z}}{2}$
6. $\operatorname{Im} z = \frac{z - \bar{z}}{2i}$

17.2.7 Si x y y son números complejos, tenemos

$$|x + y| \leq |x| + |y|$$

PRUEBA. Como no contamos con la desigualdad de Cauchy-Schwarz, procedemos en la siguiente forma:

Sean $x, y \in \mathbb{C}$ entonces $x = (x_1, x_2) \wedge y = (y_1, y_2)$ con $x_1, x_2, y_1, y_2 \in \mathfrak{R}$ entonces $x_1y_2 - x_2y_1 \in \mathfrak{R}$ por los postulados de \mathfrak{R} se sigue que

$$(x_1y_2 - x_2y_1)^2 \geq 0$$

de donde

$$\begin{aligned} x_1^2y_2^2 - 2x_1y_1x_2y_2 + x_2^2y_1^2 &\geq 0 \\ \Leftrightarrow 2x_1x_2y_1y_2 &\leq x_1^2y_2^2 + x_2^2y_1^2 \end{aligned}$$

$$\Leftrightarrow x_1^2 y_1^2 + 2x_1 x_2 y_1 y_2 + x_2^2 y_2^2 \leq x_1^2 y_1^2 + x_1^2 y_2^2 + x_2^2 y_1^2 + x_2^2 y_2^2$$

$$\Leftrightarrow (x_1 y_1 + x_2 y_2)^2 \leq (x_1^2 + x_2^2)(y_1^2 + y_2^2)$$

Tomando raíz cuadrada a los dos lados tenemos

$$x_1 y_1 + x_2 y_2 \leq \sqrt{(x_1^2 + x_2^2)(y_1^2 + y_2^2)}$$

$$\Leftrightarrow 2(x_1 y_1 + x_2 y_2) \leq 2(\sqrt{(x_1^2 + x_2^2)(y_1^2 + y_2^2)})$$

sumando cantidades iguales la desigualdad se mantiene

$$x_1^2 + x_2^2 + 2(x_1 y_1 + x_2 y_2) + y_1^2 + y_2^2 \leq x_1^2 + x_2^2 + 2(\sqrt{(x_1^2 + x_2^2)(y_1^2 + y_2^2)}) + y_1^2 + y_2^2$$

Esta desigualdad la podemos transformar en la forma equivalente siguiente

$$(x_1^2 + 2x_1 y_1 + y_1^2) + (x_2^2 + 2x_2 y_2 + y_2^2) \leq$$

$$\leq (\sqrt{x_1^2 + x_2^2})^2 + 2(\sqrt{(x_1^2 + x_2^2)(y_1^2 + y_2^2)}) + (\sqrt{y_1^2 + y_2^2})^2$$

$$\Leftrightarrow (x_1 + y_1)^2 + (x_2 + y_2)^2 \leq (\sqrt{x_1^2 + x_2^2} + \sqrt{y_1^2 + y_2^2})^2$$

$$\Leftrightarrow |(x_1 + y_1, x_2 + y_2)|^2 \leq (|(x_1, x_2)| + |(y_1, y_2)|)^2$$

Tomando raíz cuadrada llegamos a la desigualdad deseada

$$|x + y| \leq |x| + |y|$$

Esta desigualdad es conocida como la desigualdad triangular

□

17.3 IMPOSIBILIDAD DE ORDENAR LOS NÚMEROS COMPLEJOS

Todavía no hemos definido una relación de la forma $x < y$ si x y y son números complejos arbitrarios, por la razón de que es imposible dar una definición de $<$ para números complejos que posea todas las propiedades expresadas por los axiomas O1, O2, AO1, y AO2 dadas en 9.5.

Para justificarlo, supongamos que fuera posible definir una relación de orden $<$ que cumpliera los axiomas O1, O2, AO1, y AO2. Entonces, puesto que $i \neq 0$, tendríamos, o bien

$$i > 0 \quad \text{ó} \quad i < 0$$

según el axioma de tricotomía. Supongamos $i > 0$.

Tomando $x = y = i$ y según AO2 tendríamos

$$i^2 > 0$$

pero $i^2 = -1$, así $-1 > 0$, sumando 1 a los dos miembros llegaríamos a que $0 > 1$, lo cual es contradictorio. Por lo tanto el supuesto $i > 0$ nos lleva a una contradicción. Un razonamiento parecido demuestra que no podemos tomar $i < 0$. Por lo tanto, los números complejos no pueden ser ordenados de manera que los axiomas O1, O2, AO1 y AO2 se satisfagan.

17.4 EXPONENCIALES COMPLEJOS

La exponencial e^x ($x \in \mathfrak{R}$) es dada por la serie

$$e^x = 1 + x + \frac{1}{2}x^2 + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots + \frac{x^n}{n!} + \cdots$$

Queremos ahora definir e^z , cuando z es un número complejo. Vamos a hacerlo de manera que las propiedades principales de la función exponencial real se conserven. Las citadas propiedades para $x \in \mathbb{R}$ vienen dadas por la ley de exponentes

$$e^{x_1} e^{x_2} = e^{x_1+x_2}$$

y por el hecho de que

$$e^0 = 1$$

Daremos una definición de e^z para z complejo que conserve tales propiedades y que se reduzca a la exponencial ordinaria cuando z es real.

Si escribimos $z = x + iy$ ($x, y \in \mathbb{R}$), con objeto de que se mantenga la ley de exponentes, es necesario que sea

$$e^{x+iy} = e^x e^{iy}$$

Queda por definir lo que significa e^{iy} .

17.4.1 DEFINICIÓN. Si $z = x + iy$, definimos $e^z = e^{x+iy}$ como el número complejo

$$e^z = e^x (\cos y + i \sin y).$$

Tal definición coincide claramente con la función exponencial ordinaria cuando z es real (esto es, $y = 0$). Tenemos ahora que la ley de exponentes se cumple.

17.4.2 TEOREMA. Si $z_1 = x_1 + iy_1 \wedge z_2 = x_2 + iy_2$ son números complejos, se verifica

$$e^{z_1+z_2} = e^{z_1} e^{z_2}$$

PRUEBA. $e^{z_1} = e^{x_1} (\cos y_1 + i \sin y_1)$

$$e^{z_2} = e^{x_2} (\cos y_2 + i \sin y_2)$$

$$e^{z_1} e^{z_2} = e^{x_1} e^{x_2} [\cos y_1 \cos y_2 - \sin y_1 \sin y_2 + i(\cos y_1 \sin y_2 + \sin y_1 \cos y_2)]$$

Ahora bien: $e^{x_1} e^{x_2} = e^{x_1+x_2}$, puesto que x_1 y x_2 son reales. Así mismo,

$$\cos y_1 \cos y_2 - \sin y_1 \sin y_2 = \cos(y_1 + y_2)$$

y

$$\cos y_1 \sin y_2 + \sin y_1 \cos y_2 = \sin(y_1 + y_2)$$

y por consiguiente

$$e^{z_1} e^{z_2} = e^{x_1+x_2} [\cos(y_1 + y_2) + i \sin(y_1 + y_2)] = e^{z_1+z_2}$$

□

Ahora vamos a obtener algunas propiedades importantes de la exponencial compleja.

17.4.3 TEOREMA. e^z nunca es cero

PRUEBA. $e^z e^{-z} = e^0 = 1$. Luego e^z no puede ser cero.

□

17.4.4 TEOREMA. Si x es real, entonces $|e^{ix}| = 1$.

PRUEBA. $|e^{ix}|^2 = \cos^2 x + \sin^2 x = 1$ y $|e^{ix}| > 0$.

□

17.4.5 TEOREMA. $e^z = 1$, si z es múltiplo entero de $2\pi i$, y recíprocamente.

PRUEBA. Si $z = 2\pi in$, siendo n entero, entonces

$$e^z = \cos(2\pi n) + i\sin(2\pi n) = 1$$

Inversamente, supongamos que $e^z = 1 \wedge z = x + iy$. Esto significa que $e^x \cos y = 1$ y $e^x \sin y = 0$. Ya que $e^x \neq 0$, es necesario que $\sin y = 0 \Leftrightarrow y = k\pi$ siendo k un número entero. Pero $\cos(k\pi) = (-1)^k$. Por lo tanto $e^x \cos(k\pi) = 1$. Siendo por otra parte $e^x > 0$, k debe ser par, es decir, $y = 2\pi n$. Por eso $e^x = 1$ luego $x = 0$. El teorema está probado.

□

17.4.6 TEOREMA $e^{z_1} = e^{z_2}$, si $z_1 - z_2 = 2\pi in$ ($n \in \mathbb{Z}$) y recíprocamente.

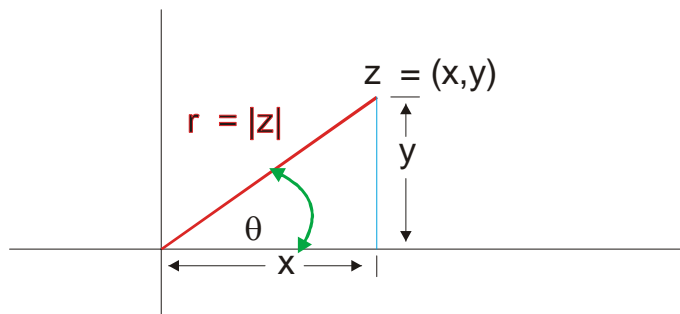
PRUEBA. Si $e^{z_1} = e^{z_2}$, entonces $e^{z_1 - z_2} = 1$ y de 17.4.5 se tiene $z_1 - z_2 = 2\pi in$.

Inversamente si $z_1 - z_2 = 2\pi in$ entonces $e^{z_1 - z_2} = e^{2\pi in} = 1 \Rightarrow e^{z_1} = e^{z_2}$

□

17.5 ARGUMENTO DE UN NÚMERO COMPLEJO

Si el punto $z = (x, y) = x + yi$ se representa en coordenadas polares r y θ , podemos escribir $x = r \cos \theta$ y $y = r \sin \theta$, es decir



$$z = r \cos \theta + i \sin \theta$$

Los dos números r y θ determinan unívocamente a z . Inversamente el número positivo r viene determinado unívocamente por z pues $r = |z|$. Sin embargo, z determina el ángulo θ salvo múltiplos de 2π . Existen una infinidad de valores de θ que satisfacen las ecuaciones

$$x = |z|\cos \theta, \quad y = |z|\sin \theta$$

pero, naturalmente, dos cualesquiera de ellos difieren en un múltiplo de 2π . Cada uno de estos valores de θ es un *argumento* de z pero uno de ellos se distingue y se llama el *argumento principal* de z .

17.5.1 DEFINICIÓN. Sea $z = x + iy$ un número complejo no nulo. El número real único θ que satisface las condiciones

$$x = |z|\cos \theta, \quad y = |z|\sin \theta \quad -\pi < \theta \leq +\pi$$

se llama el argumento principal de z , y se representa por

$$\theta = \arg(z)$$

La anterior discusión origina inmediatamente el siguiente teorema.

17.5.2 TEOREMA. Todo número complejo $z \neq 0$ puede ponerse en la forma $z = re^{i\theta}$, donde $r = |z|$ y $\theta = \arg(z) + 2\pi n$, siendo n un número entero.

NOTA. Tal método de representación de los números complejos es especialmente útil en relación con la multiplicación y la división, pues tenemos

$$(r_1 e^{i\theta_1})(r_2 e^{i\theta_2}) = r_1 r_2 e^{i(\theta_1 + \theta_2)}$$

y

$$\frac{r_1 e^{i\theta_1}}{r_2 e^{i\theta_2}} = \frac{r_1}{r_2} e^{i(\theta_1 - \theta_2)}$$

17.5.3 TEOREMA. Si $z_1 z_2 \neq 0$, se verifica

$$\arg(z_1 z_2) = \arg(z_1) + \arg(z_2) + 2\pi n(z_1, z_2)$$

donde

$$n(z_1, z_2) = \begin{cases} 0 & \text{si} & -\pi < \arg(z_1) + \arg(z_2) \leq \pi \\ 1 & \text{si} & -2\pi < \arg(z_1) + \arg(z_2) \leq -\pi \\ -1 & \text{si} & \pi < \arg(z_1) + \arg(z_2) \leq 2\pi \end{cases}$$

PRUEBA. Pongamos $z_1 = |z_1|e^{i\theta_1}$, $z_2 = |z_2|e^{i\theta_2}$, donde $\theta_1 = \arg(z_1)$ y $\theta_2 = \arg(z_2)$. Entonces $z_1 z_2 = |z_1 z_2|e^{i(\theta_1 + \theta_2)}$. Puesto que $-\pi < \theta_1 \leq \pi$ y $-\pi < \theta_2 \leq \pi$, tenemos

$$-2\pi < \theta_1 + \theta_2 \leq 2\pi$$

Este entero n es precisamente el entero $n(z_1, z_2)$ (existe n tal que $-\pi < \theta_1 + \theta_2 + 2\pi n < \pi$) dado en el enunciado del teorema, y para él tenemos

$$\arg(z_1, z_2) = \theta_1 + \theta_2 + 2\pi n.$$

□

17.6 POTENCIAS ENTERAS Y RAICES DE NÚMEROS COMPLEJOS

17.6.1 DEFINICIÓN. Dados un número complejo y un entero n , definimos la potencia n -ésima de z así

$$\begin{aligned} z^0 &= 1, & z^{n+1} &= z^n z & \text{si } n \geq 0 \\ z^{-n} &= (z^{-1})^n & & & \text{si } n > 0 \text{ y } z \neq 0 \end{aligned}$$

17.6.2 TEOREMA. Dados dos enteros m y n , tenemos

$$z^n z^m = z^{n+m} \quad \text{y} \quad (z_1 z_2)^n = z_1^n z_2^n$$

17.6.3 TEOREMA. Si $z \neq 0$, y n es un entero positivo, existen exactamente n números distintos z_0, z_1, \dots, z_{n-1} (llamados raíces n -ésimas de z). tales que

$$z_k^n = z, \quad \text{para } k = 0, 1, 2, \dots, n-1$$

Además, estas raíces se obtienen utilizando las fórmulas

$$z_k = R e^{i\theta_k} \quad \text{donde } R = |z|^{\frac{1}{n}} \quad \text{y} \quad \theta_k = \frac{\arg(z)}{n} + \frac{2\pi k}{n} \quad (k = 0, \dots, n-1)$$

NOTA. Las n raíces n -ésimas son los vértices de un polígono regular inscrito en el círculo de radio $r = |z|^{\frac{1}{n}}$ y centro en el origen.

PRUEBA. Los n números complejos $R e^{i\theta_k}$, $0 \leq k \leq n-1$, son distintos y cada uno es una raíz n -ésima de z , ya que

$$(R e^{i\theta_k})^n = R^n e^{in\theta_k} = |z| e^{i[\arg(z)+2\pi k]} = z$$

Demostremos ahora que no existen otras raíces n -ésimas de z . Admitamos que $w = A e^{i\alpha}$ es un complejo tal que $w^n = z$.

En tal caso $|w|^n = |z|$, y por lo tanto $A^n = |z|$, $A = |z|^{\frac{1}{n}}$. Por consiguiente, de $w^n = z$ se deduce

$$e^{in\alpha} = e^{i[\arg(z)]}, \quad \text{que implica } n\alpha - \arg(z) = 2\pi k$$

luego

$$\alpha = \frac{\arg(z) + 2\pi k}{n}$$

Pero mientras k va recorriendo todos los valores enteros, w toma sólo los valores distintos z_0, z_1, \dots, z_{n-1} .

□

17.7 LOGARITMOS COMPLEJOS

Según hemos visto e^z nunca es cero. Es natural preguntar si existen otros valores que e^z no pueda alcanzar. El próximo teorema demuestra que el único valor excepcional es el cero.

17.7.1 TEOREMA. Si z es un número complejo distinto de cero existen números complejos w tales que $e^w = z$. Uno de tales w es el número complejo

$$\log|z| + i\arg(z)$$

y todos los demás tienen la forma

$$\log|z| + i\arg(z) + 2n\pi i \quad (n \in \mathbb{Z})$$

PRUEBA. Ya que

$$e^{\log|z|+i\arg(z)} = e^{\log|z|}e^{i\arg(z)} = |z|e^{i\arg(z)} = z$$

vemos que

$$w = \log|z| + i\arg(z)$$

es una solución de la ecuación $e^w = z$. Pero si w_1 es alguna otra solución, entonces

$$e^w = e^{w_1} \Leftrightarrow e^{w_1-w} = 1 \Leftrightarrow w_1 - w = 2n\pi i$$

así

$$w_1 = \log|z| + i\arg(z) + 2n\pi i.$$

□

17.7.2 DEFINICIÓN. Sea $z \neq 0$ un número complejo dado. Si w es un número complejo tal que $e^w = z$, entonces w es llamado un logaritmo de z . El valor particular de w dado por

$$w = \log|z| + i\arg(z)$$

se denomina el logaritmo principal de z , y se representará simplemente por

$$w = \text{Log}(z)$$

17.7.3 TEOREMA. Si $z_1 z_2 \neq 0$, se verifica que

$$\text{Log}(z_1 z_2) = \text{Log}(z_1) + \text{Log}(z_2) + 2\pi in(z_1, z_2)$$

PRUEBA. $\text{Log}(z_1 z_2) = \log|z_1 z_2| + i\arg(z_1 z_2)$

$$\stackrel{\uparrow}{=} \log|z_1| + \log|z_2| + i[\arg(z_1) + \arg(z_2) + 2\pi n(z_1, z_2)]$$

17.5.3

$$= \{\log|z_1| + i\arg(z_1)\} + \{\log|z_2| + i\arg(z_2)\} + 2\pi in(z_1, z_2)$$

$$= \text{Log}(z_1) + \text{Log}(z_2) + 2\pi in(z_1, z_2).$$

□

17.8 POTENCIAS COMPLEJAS

Utilizando logaritmos complejos podemos ahora dar una definición de potencias complejas de números complejos.

17.8.1 DEFINICIÓN. Si $z \neq 0$ y si w es cualquier número complejo definimos

$$z^w = e^{w\text{Log}(z)}.$$

EJEMPLOS (1) $i^i = e^{i\text{Log}(i)} = e^{i(i\frac{\pi}{2})} = e^{-\frac{\pi}{2}}$

(2) $(-1)^i = e^{i\text{Log}(-1)} = e^{i(i\pi)} = e^{-\pi}$

(3) Si n es un número entero, entonces

$$z^{n+1} = e^{(n+1)\text{Log}(z)} = e^{n\text{Log}(z)} e^{\text{Log}(z)} = z^n z$$

17.8.2 TEOREMA. $z^{w_1} z^{w_2} = z^{w_1+w_2}$

PRUEBA. $z^{w_1+w_2} = e^{(w_1+w_2)\text{Log}(z)} = e^{w_1\text{Log}(z)} e^{w_2\text{Log}(z)} = z^{w_1} z^{w_2}$

□

17.8.3 TEOREMA. $(z_1 z_2)^w = z_1^w z_2^w e^{2\pi i n(z_1, z_2)}$

donde $n(z_1, z_2)$ es el entero dado en 17.5.3

PRUEBA. $(z_1 z_2)^w = e^{w\text{Log}(z_1 z_2)} = e^{w[\text{Log}(z_1) + \text{Log}(z_2) + 2\pi i n(z_1, z_2)]}$
 $= e^{w\text{Log}(z_1) + w\text{Log}(z_2) + 2\pi i w n(z_1, z_2)} = e^{w\text{Log}(z_1)} e^{w\text{Log}(z_2)} e^{2\pi i w n(z_1, z_2)}$
 $= z_1^w z_2^w e^{2\pi i n(z_1, z_2)}$

□

17.9 EJERCICIOS.

(1) Halle $\text{Log}(i)$

(2) Halle $\text{Log}(-i)$

(3) Demuestre que $\text{Log}(-1) = \pi i$

(4) Demuestre que si $x \in \Re$ y $x > 0$ entonces $\log x = \text{Log}(x)$

(5) Pruebe que $\text{Log}(1+i) = \log\sqrt{2} + \frac{\pi}{4}i$

(6) Demostrar que

a) $|z|^2 = z \cdot \bar{z}$

b) $\frac{z + \bar{z}}{2} = \text{Re}z$

c) $z - \bar{z} = 2\Im z$

d) $\overline{z+w} = \bar{z} + \bar{w}$

e) $\sum_{k=1}^n z_k = \sum_{k=1}^n \bar{z}_k$

f) $e^{i\theta} = e^{-i\theta}, \theta \in \Re$

g) $\bar{\bar{z}} = z$

h) $|\bar{z}| = |z|$

i) $|e^{i\theta}| = 1, \theta \in \Re$

j) $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$

k) $\left(\prod_{k=1}^n z_k\right) = \prod_{k=1}^n \bar{z}_k$

l) $\overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}$

ll) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

m) $\left|\prod_{k=1}^n z_k\right| = \prod_{k=1}^n |z_k|$

n) $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}, w \neq 0$

ñ) $|z+w| \leq |z| + |w|$

o) $|z-w| \leq |z \mp w| \leq |z| + |w|$

p) Si $|z| > |w|$ entonces $\frac{1}{|z \mp w|} \leq \frac{1}{|z| - |w|}$

q) $\left|\sum_{k=1}^n z_k\right| \leq \sum_{k=1}^n |z_k|$ (por inducción)

r) $\sqrt{|z|^2 + |w|^2} \leq |z| + |w|$

s) $|z-w|^2 + |z+w|^2 = 2(|w|^2 + |z|^2)$

(7) Encuentre los vértices de un polígono regular de n lados, si su centro está en $z = 0$ y uno de sus vértices es z_0 .

(8) Calcular:

a) $\sqrt[4]{1}$

b) $\sqrt[4]{-1}$

c) $(5 + 12i)^{100}$

d) $\left(\frac{5+12i}{4-3i}\right)^{100}$

e) $\sqrt[4]{i}$

f) $\sqrt[4]{(2+4i)}$

g) $\log(-e^2)$

h) $\log(-e^i)$

i) $(5 + 12i)^{6+7i}$

j) $(5 - 12i)^{6+7i}$

k) $(-5 + 12i)^{6+7i}$

$$l) (-5 - 12i)^{6+7i} \quad m) \log(5 + 12i) \quad n) i^{\frac{1}{i}}$$

$$\tilde{n}) (2i)^{\frac{1}{2}} \quad o) \pi^i$$

(9) Resolver las ecuaciones:

$$a) \log z = \frac{\pi i}{2} \quad b) \log z = 1 + 3\pi i \quad c) e^z + i = 0$$

$$d) e^{\bar{z}} + i = 0 \quad e) \cosh z = 6 \quad f) \sin z = 2$$

(10) Hallar el conjunto de puntos del plano que determinan cada una de las siguientes relaciones:

$$a) \operatorname{Re} z^2 \leq 0 \quad b) \frac{\pi}{3} \leq \arg z \leq \frac{2\pi}{3} \quad c) |z - 3i| = 5 \quad d) |z - 3i| = 5$$

$$e) |z - 3i| > 5 \quad f) |z - 3| + |z + 3| = 8 \quad g) |z - a| = r, a \in \mathbb{C}, r > 0$$

$$h) \operatorname{Im} z^{-1} < -3 \quad i) z + z^2 = 1 \quad j) 5 \leq |z - 3i| \leq 8$$

$$k) z = 3i + 5e^{i\theta}, \quad \theta \in [0, 2\pi] \quad l) |z - 3| - |z + 2| > 8$$

$$ll) \operatorname{Im} z^2 \geq 0 \quad o) 0 < \operatorname{Im} z < 3 \quad p) \operatorname{Re} z^{-1} < 0$$

(11) Resolver las ecuaciones

$$a) z^3 - 3z^2 + 3z + 8 = 0 \quad b) z^4 + 4z^3 + 6z^2 + 4z + 10 = 0$$

$$c) \cos x + i \sin x = \sin x + i \cos x, \quad \text{para } x \in \mathbb{R}$$

(12) ¿En qué vector (número) se transforma el vector (número) $2 + i\sqrt{3}$ después de una rotación de (1) $\frac{\pi}{2}$, (2) de $-\frac{\pi}{2}$?

(13) Demostrar que si $z = x + iy$ entonces $x = \frac{z+\bar{z}}{2}$, $y = \frac{z-\bar{z}}{2i}$

(14) Escribir en forma compleja y determinar el conjunto de puntos dado por cada una de las siguientes relaciones:

$$a) y = x \quad b) y = mx + b, \quad m, b \in \mathbb{R}, \text{ fijos, } x, y \in \mathbb{R}$$

$$c) x^2 + y^2 = a^2, \quad x, y \in \mathbb{R}, a \text{ real fijo}$$

$$d) x^2 + y^2 - 2ax = 0, \quad x, y \in \mathbb{R}, a \text{ real fijo}$$

$$e) \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \quad x, y \in \mathbb{R}, a > 0, b > 0$$

(15) Demostrar que

$$1 + z + z^2 + z^3 + \dots + z^n = \begin{cases} \frac{z^{n+1}-1}{z-1}, & z \neq 1 \\ n+1, & z = 1 \end{cases}$$

(16) A partir del ejercicio 15, demostrar que

$$1 + \cos\theta + \cos 2\theta + \dots + \cos n\theta = \frac{\cos \frac{n}{2}\theta \sin(n+1)\frac{\theta}{2}}{\sin \frac{\theta}{2}}, \quad \theta \neq 2k\pi, k \in \mathbb{Z}$$

(17) Demostrar que

$$a) \arcsin z = i \log \left(iz + \sqrt{1 - z^2} \right)$$

$$b) \arccos z = -i \log \left(z + \sqrt{z^2 - 1} \right)$$

$$c) \arctan z = \frac{i}{2} \log \left(\frac{i+z}{i-z} \right)$$

$$d) \operatorname{arccosh} z = \log \left(z + \sqrt{z^2 - 1} \right)$$

$$e) \operatorname{arcsinh} z = \log \left(z + \sqrt{z^2 + 1} \right)$$

$$f) \operatorname{arctanh} z = \frac{1}{2} \log \left(\frac{1+z}{1-z} \right)$$

$$g) |\cos^2 z| = \cos^2 x + \sinh^2 y, \quad z = x + iy.$$

(18) Si $1, w, w^2$ son raíces cúbicas de 1, probar que

$$i) (1 + w^2)^4 = w, \quad \text{con } w \neq 1$$

ii) $(1 - w)(1 - w^2)(1 - w^4)(1 - w^5) = 9, \quad w \neq 1$

(sugerencia $1 + w + w^2 = 0, \quad w \neq 1$)

(19) Probar o refutar cada una de las siguientes afirmaciones (justifique la respuesta).

(a) $|e^{iz}| = 1, \quad z \in \mathbb{C}$ (b) $\overline{e^{iz}} = e^{iz}, \quad z \in \mathbb{C}$

(c) $\overline{\cos^2 z} + \sin^2 z = 1, \quad z \in \mathbb{C}$ (d) $|\sin z| \leq 1, \quad z \in \mathbb{C}$

(e) $\overline{\sin z} = \sin \bar{z}, \quad z \in \mathbb{C}.$

(20) Probar que $\cos 5\theta = 6\cos^5\theta - 20\cos^3\theta + 5\cos\theta$

(21) La distancia entre dos números complejos z y w se define por $d(z, w) = |z - w|$. Demostrar que d es una métrica sobre \mathbb{C} , esto es, para todo $w, z, t \in \mathbb{C}$

(a) $d(w, z) = d(z, w)$

(b) $d(w, z) \leq d(w, t) + d(t, z)$

(c) $d(w, z) \geq 0$, y $d(w, z) = 0$, cuando $w = z$

(22) Demostrar que en general $(a^m)^{\frac{1}{n}} \neq \left(a^{\frac{1}{n}}\right)^m$. Si m y n son números primos relativos se tiene que $(a^m)^{\frac{1}{n}} = \left(a^{\frac{1}{n}}\right)^m$ y por lo tanto

$$(a^m)^{\frac{1}{n}} = \left(a^{\frac{1}{n}}\right)^m e^{i\frac{m}{n}(\theta+2k\pi)}, \quad 0 \leq k \leq n$$

Sugerencia : Tome $a = (-1)^{\frac{2}{4}}$

(23) Demostrar que para el valor principal en general se tienen las siguientes desigualdades:

(a) $(wz)^a \neq w^a z^a$ (b) $\left(\frac{w}{z}\right)^a \neq \frac{w^a}{z^a}, \quad z \neq 0$

(c) $\log z^a \neq a \log z$ (d) $(z^a)^b \neq z^{ab}$

(24) Supóngase que z_1, z_2, z_3 son tres números complejos tales que $|z_1| = |z_2| = |z_3| = 1$ y $z_1 + z_2 + z_3 = 0$. Demostrar que z_1, z_2, z_3 son los vértices de un triángulo equilátero inscrito en la circunferencia unitaria.

(25) Determinar los puntos $z = x + iy$ del plano complejo que satisface la desigualdad $|z - 1| \leq 2|z + 1|$.

(26) Sea $P(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \dots + a_n$ un polinomio de grado $n \geq 1$ y de coeficientes reales. Demostrar, que si α es una raíz de $P(z) = 0$, entonces $\bar{\alpha}$ lo es también.

(27) Demostrar que los puntos $z = x + iy$ que satisfacen $|z + 1| \leq 4 - |z - 1|$ son los puntos, interiores a la elipse $\frac{x^2}{4} + \frac{y^2}{3} = 1$ o pertenecen a ella.

(28) Probar que si z_0 es una raíz cúbica de un número z , y si $1, w, w^2$ son las raíces cúbicas de la unidad, entonces $z_0, z_0 w, z_0 w^2$ son las raíces cúbicas de z . Pártase de este resultado para determinar las raíces cúbicas de -8 .

(29) Encuentre la ecuación de la elipse con focos $\pm i$ que pasa por el punto $1 + i$. En geometría analítica, ¿cuál es la fórmula correspondiente?.

(30) Encuentre la hipérbola con focos 1 e i que pasa por el origen. ¿Cuál es la fórmula correspondiente en geometría analítica?.

- (31) Encuentre la parábola de foco $1 + i$ y con la resta $Re z + \Im z = 0$ como directriz.
- (32) Escriba en forma compleja la ecuación general de una hipérbola con focos a y b .
- (33) Pruebe que $|z| \leq |Re z| + |\Im z| \leq \sqrt{2}|z|$

BIBLIOGRAFIA

- [1] Allendoerfer C. and Oakley C.O., *Principles of Mathematics*. McGraw-hill book Company. (1963)
- [2] Apostol Tom.M., *Analisis Matemático*. Editorial Reverté. (1957)
- [3] Apostol Tom.M., *Introduction to Analytic Number Theory*. Springer-Verlag. New York Heidelberg Berlin.
- [4] Birkhoff y MacLane, *Algebra Moderna*. Editorial Teide. Barcelona, (1960)
- [5] Burnett R. Toskey. *College Algebra a Modern Approach*. Addison-Wesley P.C. (1962)
- [6] Mariño Rafael, *Fundamentos de Matemáticas*. Universidad Nacional de Colombia. (1966)
- [7] Muñoz. J.M., *Introducción a la teoría de conjuntos*. Universidad Nacional de Colombia. (1994)
- [8] Muñoz.J.M y Sánchez.J.D., *Precálculo*. Universidad Nacional de Colombia.(1992)
- [8] Neal H. McCoy, *Introduction to Modern Algebra*. Boston. Allyn and Bacon. Inc. (1961).

.ДАЖЙ ЛЛЭЮ

Espero que el lector haya obtenido algún provecho de este trabajo en el aprendizaje de la matemática avanzada. En esta forma se completa la parte del Álgebra propuesta en este proyecto de aprendizaje en matemática avanzada. Exitos y bienvenidos a la investigación por internet. Cualquier comentario favor hacerlo llegar a:

danojuanos@hotmail.com,
danojuanos@tutopia.com

Agradezco a Esperanza y Nohora el tiempo que dedicaron a revisar el castellano para que no se fueran tantos errores ya que el programa que uso para la escritura no tiene corrector .

Copyright© Darío Sánchez Hernández