Álgebra

Cuaderno 1

Victor Wall

Comentario.

El presente trabajo tiene como objetivo, presentar al estudiante una guía de estudio, constituída por notas teórico-práctico de las clases dadas. Pero, bajo ningún concepto intenta substituir a la bibliografía existente sobre este tema, que el alumno deberá consultar permanentemente para lograr un efectivo aprendizaje.

Está dirigido a los alumnos que cursan regularmente la Asignatura Álgebra1, correspondiente al primer cuatrimestre del primer año de la Carrera del Profesorado en Matemática de la Facultad de Ciencias Exactas, Químicas y Naturales de la Universidad Nacional de Misiones tiene como objetivo fundamental desarrollar los conceptos básicos y propiedades de las estructuras algebraicas y de los conjuntos numéricos, de acuerdo a los contenidos mínimos establecidos y por los docentes de las asignaturas de los años siguientes de la Carrera.

Se cree que el alumno tendrá, de ésta manera un elemento de trabajo, que le facilitará el estudio de Álgebra en el Primer Año. Los temas presentados en este cuaderno, son los que se desarrollarán en las clases teóricas, prácticas y trabajos complementarios y, se corresponden con las Unidades que conforman el Programa vigente de la Carrera mencionada y constituyen (las clases), entonces, el complemento necesario para una buena comprensión del texto.

Este material impreso expone los temas que forman parte de los contenidos de la asignatura, y que son desarrollados en las clases expositivas y presentando el criterio del Profesor para el estudio del mismo y que además se encuentran dispersos en una bibliografía muy variada o de muy difícil acceso para el alumno.

Consisten, esencialmente, en la presentación y desarrollo, metodológicamente ordenado, de lo fundamental de cada unidad y, que es producto de una labor docente de síntesis y recopilación.

Se propone que la asignatura considere y estudie los temas relativos a :

- Aplicaciones y Relaciones;
- Estructuras algebraicas y conjuntos numéricos;
- Ennumeramientos
- Funciones reales elementales
- Resolución de ecuaciones y desigualdades con una indeterminada

propuestos en los contenidos básicos para la Formación Docente en Matemática del actual Plan de Estudios de la carrera.

Se parte de la premisa fundamental, de que en las Universidades se debe enseñar ciencia de buen nivel, no importa si pura o aplicada, pero si óptima; (no se debe sacrificar la formación básica en aras de la información tecnológica, ya que ésta, envejece con mucha facilidad y sólo un sólido dominio de los conceptos básicos, otorga la flexibilidad necesaria para incorporar y adaptarse a las nuevas tecnologías.

El curso, sin pérdida del rigor y de su nivel de excelencia deberá concentrarse en ideas, aplicaciones y capacitación para una mayor y efectiva participación en actividades de discusión de problemas didácticos relacionados con la futura participación profesional.

La selección de los temas y su ordenamiento, deberá mostrar las conexiones entre ellos y con modelos reales, así como las técnicas de resolución concreta, y además teniendo en cuenta los contenidos mínimos de la Carrera.

Se pretende que el cursado de la asignatura sirva para que los alumnos, futuros docentes de Matemática:

Incrementen, actualicen y fortalezcan su formación específica mediante el conocimiento de los fundamentos, métodos y aplicaciones de:

- Aplicaciones o funciones y Relaciones,
- Ennumeramientos
- Estructuras ordenadas de los conjuntos numéricos.

Desarrollen una mejor disposición a:

Redescubrir conceptos básicos e incorporar conocimientos nuevos de manera continua;

Resignificar los conocimientos previamente adquiridos a partir de:

a) la reflexión y el análisis histórico y epistemológico sobre el descubrimiento y desarrollo de los conceptos.
b) La comparación de diferentes propuestas didácticas;

Adoptar una actitud decididamente actual en la presentación e interpretación de temas problemas y resultados tradicionales;

Relacionar sus propios conocimientos y experiencias con el desarrollo de la investigación científica.

Introducción

El Álgebra, que desde su origen y durante muchos años fue la rama de la matemática que trataba de números y de ecuaciones, amplía su campo a finales del siglo XIX hacia nuevos objetos matemáticos, como son los vectores, los polinomios, las matrices,...,etc y, se separa del estudio de la solución de ecuaciones dirigiéndose hacia las estructuras abstractas. Al igual que con los números, con los vectores, polinomios, matrices, ..., etc, se realizan operaciones que, en muchos casos, se denominan con los mismos nombres que las operaciones clásicas, suma, producto,..., definidas y delimitadas por propiedades análogas a las de la suma, producto, ... de números, tales como la asociatividad, conmutatividad ..., que forman las reglas del juego con los nuevos objetos. El Álgebra pasa a ser la ciencia que estudia las estructuras, es decir, conjuntos con operaciones verificando ciertas propiedades que determinan qué tipo de estructura es, recibiendo nombres como grupo, anillo, álgebra de Boole,.... Más aún, el Álgebra estudia hoy día cualquier estructura o, mejor aún, ninguna en concreto, siendo un procedimiento lógico que en muchos casos puede adaptarse al mundo físico, de manera que es la base de muchas ciencias actuales como la inteligencia artificial o la mecánica cuántica.

En el estudio de matemáticas, en general se utilizan signos, se define el universo o colección de términos de la teoría, se enuncian axiomas, reglas, propiedades, se hacen demostraciones, se hacen ejemplos. Para que el estudio sea eficaz, es necesario lograr que todas las formulaciones, se hagan con precisión, sin ambigüedades y con claridad.

Si bien, es complicado lograr un lenguaje matemático, que sea útil y práctico, es necesario lograr una aproximación a éste, y para ello haremos uso de algunos elementos de la lógica proposicional, sin mayores pretensiones.

Para ello, se debe estudiar el problema de establecer cuáles deben ser las condiciones que debe reunir un enunciado, para que pueda ser considerado como una conclusión derivada de otros enunciados, llamadas premisas. Se puede decir que para una correcta argumentación, se debe tener en cuenta:

a)- Si las premisas son verdaderas, la conclusión es verdadera.
b)- Si las premisas son falsas, la conclusión puede ser verdadera o falsa.-

Lo que nunca puede suceder en una argumentación correcta es que las premisas sean verdaderas y la conclusión falsa.

En síntesis, interesa aprender el modo de reconocer formas correctas e incorrectas, y la manera de construirlas. También, buscar medios de derivar desde formas fundamentales, otras formas correctas.

Se trata a continuación, de informar con más precisión al lector, sobre la manera de construir enunciados, relaciones y sobre los razonamientos lógicos más importantes que serán herramientas para usar, en forma continua.

Nociones Elementales de Conjuntos y Vocabulario Básico

Comentario

Se hace aquí un breve recordatorio de algunos elementos básicos del lenguaje a utilizar durante el curso y que, por otra parte son desarrollados en toda su extensión en otras Asignatura de la Carrera.

De manera que este capítulo denominado Unidad 0 no forma parte del Programa Oficial de la Asignatura.

0. - Vocabulario básico

0.1.- Conjuntos y elementos.

Es naturalmente preferible, decir que se considera a la noción de conjunto como una noción primitiva, que no se define, y realizar un estudio intuitivo de conjuntos, no es correcto realizar definiciones como ésta: "Se llama conjunto a toda colección de objetos de la misma naturaleza". En esta "definición", se reduce la palabra conjunto a la de colección, pero resulta que significan lo mismo.

El hecho de que se pueda interpretar a los objetos matemáticos como colecciones o conjuntos no tiene, por supuesto, nada que ver con el problema que consiste en definir matemáticamente la noción de conjunto, este problema se resuelve solamente a través del desarrollo de una teoría axiomática de conjuntos, que sobrepasa largamente nuestro propósito.

En el desarrollo de una teoría matemática, se tienen tres procesos fundamentales: 1) construír objetos matemáticos, 2) relacionar estos objetos entre ellos y 3) demostrar mediante razonamientos adecuados los teoremas, es decir aquellas relaciones entre objetos que son verdaderas.

En matemática, se estudian objetos de diferentes tipos: por ejemplo, puntos, números, vectores. Estos objetos formados de *elementos* en virtud de ciertas propiedades, son colecciones o *conjuntos*-.

Las teorías que se presentan, concernientes cada una al estudio de una cierta colección se denomina *conjunto base* de la teoría. Por ejemplo en Geometría, el elemento de base es el *punto* y el conjunto de base, la colección de todos los puntos.

En aritmética, el elemento de base es el *número natural* y el conjunto de base, conjunto de todos los números naturales, denotado N. Se notará, en general, un elemento por una letra minúscula (el elemento a) y a un conjunto por una letra mayúscula (el conjunto A).

0.2.- Relaciones.

Los elementos de un conjunto son susceptibles de tener entre ellos, o con los de otro conjunto, ciertas relaciones.

Por ejemplo, la ***relación de pertenencia***, que se enuncia "a pertenece al conjunto A" y se denota $a \in A$.

La negación de esta relación es otra relación que se enuncia "a no pertenece al conjunto A" y se denota $a \notin A$.

La ***relación de igualdad*** se enuncia "a es igual b" y se denota $a = b$.

La negación de esta relación se enuncia "a es distinto de b" y se denota $a \neq b$.

La ***relación de inclusión de conjuntos*** se enuncia: "El conjunto A está incluido en el conjunto B"; o también "A es parte de B"; o "A es subconjunto de B" y se denota $A \subset B$. A esta relación la definiremos más adelante. Podríamos decir por ahora es que esta relación, compara tamaños de Conjuntos.

La igualdad de conjuntos: A es igual a B, se escribe $A = B$

La negación de ésta relación se enuncia. "Existe, en uno de los dos conjuntos, un elemento que no pertenece al otro", y se denota $A \neq B$ que se lee "A es diferente de B".

0.3.- Símbolos lógicos.

Proposiciones. Conectivos.-

1°.-Proposiciones.- Se entiende por proposición, a un enunciado susceptible de tomar o uno o el otro de los valores lógicos, el verdadero - V- o el falso -F-.

¿Cómo se sabe si una proposición es cierta o falsa?.

Las proposiciones verdaderas, son en una teoría matemática, los axiomas, enunciados de una vez para siempre; entendiéndose a éstos, como las propiedades más "evidentes" de los objetos matemáticos que se estudien.-

2°.-Conectivos lógicos.- Sean p y q dos proposiciones. Se constata que las tablas de más abajo (llamadas Tablas de Verdad), nos permiten asociar seis nuevas proposiciones (son las necesarias para nuestro estudio) que son denotadas:

$$\sim p;\quad p \wedge q\ ;\quad p \vee q;\quad p \Rightarrow q\ :\ p \Leftrightarrow q;\ p \veebar q$$

que se lee:

No p; p y q; p o q; p implica q; p equivale lógicamente a q; o bien p o bien q.-

p	~p
V	F
F	V

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

Los símbolos $\sim$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\veebar$ son llamados conectivos lógicos de negación, de conjunción, de disjunción, de implicación, de equivalencia lógica y disjunción excluyente respectivamente.-

La escritura $\sim p$ se escribe sin paréntesis, es así que $\sim p \wedge q$ significa $(\sim) p \wedge q$.

Nota 1.- Si p es una proposición falsa entonces $p \Rightarrow q$ es una proposición verdadera.-

Generalización.- Dadas las proposiciones p, q, r, ... , los conectivos lógicos permiten construir nuevas proposiciones, llamadas compuestas y denotadas $P_{(p,q,r,\ldots,)}$, cuyo valor lógico se conoce, gracias a las tablas de verdad y al conocimiento de los valores lógicos de las proposiciones p, q, r,..., .-

Nota 2.- La negación de $p \Leftrightarrow q$, que se escribe $(p \Delta q)$, o tambien $p \veebar q$ se la denomina diferencia simétrica o disjunción excluyente. La construcción de su tabla de verdad queda para que la haga el lector.-

Tomemos un ejemplo: Sea el conjunto A parte del conjunto B, es decir simbólicamente escribimos: $A \subset B$. Se deberá decir que todo elemento de A pertenece a B. Se denota entonces

$$(\forall\, a) \qquad a \in A \;\Rightarrow\; a \in B$$

El símbolo $\forall$ es un cuantificador que se lee "cualquiera que sea".

El símbolo $\Rightarrow$ representa una implicación: de la hipótesis $(\forall a)\ a \in A$, se deduce la consecuencia $a \in B$ (que permite afirmar $A \subset B$). De una manera general, una implicación es una relación entre una proposición p, denominada hipótesis, y una proposición q, denominada consecuencia

(se lee: "p implica q").

El proceso de deducción lógica queda caracterizado por la transitividad de la implicación:

Si ($p \Rightarrow q$ y $q \Rightarrow r$) entonces $p \Rightarrow r$. Si se tiene, a la vez $p \Rightarrow q$ y $q \Rightarrow p$, se denota $p \Leftrightarrow q$ y se lee " p es equivalente a q ".

La implicación $(p \Rightarrow q)$ es la relación fundamental del razonamiento lógico, describe una situación típica en matemática, el *condicional*: "Si p entonces q".

La proposición p también se denomina *antecedente* y la proposición q *conclusión.*

La implicación $p \Rightarrow q$ equivale lógicamente a la negación del antecedente en disyunción con el consecuente. es decir: $p \Rightarrow q \quad \Leftrightarrow \quad \sim p \vee q$.

La tabla de verdad correspondiente es:

	p	~p	q	$p \Rightarrow q$	$\sim p \vee q$
1	V	F	V	V	V
2	V	F	F	F	F
3	F	V	V	V	V
4	F	V	F	V	V

En la fila 1, se parte de una hipótesis verdadera que lleva a una conclusión verdadera, el razonamiento ha sido correcto y la implicación es verdadera.

En la fila 2, una hipótesis verdadera lleva a una conclusión falsa, el razonamiento no es válido y la implicación es falsa.

Ejemplo.

La proposición:

$-2 < 3$ (hipótesis verdadera) $\Rightarrow$ $-5 = 0$ (conclusión falsa) es falsa.

En la fila 3, una hipótesis falsa conduce a una conclusión verdadera, se ha razonado correctamente, y la implicación es verdadera.-

Ejemplo.

La proposición:

$2 = 3$ (hipótesis falsa)
entonces: $3 = 2$
sumando $5 = 5$ (conclusión verdadera);
y la implicación es verdadera..-

En la fila 4, una hipótesis falsa nos lleva a una conclusión falsa, se ha razonado correctamente y la implicación es verdadera.

Ejemplo.

La hipótesis falsa $2 = -2$; nos lleva sumando 2 a ambos miembros de la igualdad, a que $4 = 0$ (conclusión falsa). El razonamiento ha sido correcto.

A la doble implicación $p \Leftrightarrow q$ se la lee:

p *es condición necesaria y suficiente para* q ,

o también:

p *sí y sólo sí* q

Tomemos otro ejemplo: Sabemos que la proposición "Existe en A un elemento "a", que no pertenece a B" implica la proposición "A no está incluído en B". Esta propiedad se denota:

$$(\exists a,\ a \in A;\ a \notin B) \ \Rightarrow\ A \not\subset B.$$

El símbolo $\exists$ es un *cuantificador* que se lee: "Existe al menos uno"

Para probar la implicación A $\Rightarrow$ B, se puede utilizar lo que se denomina, bien impropiamente, el *razonamiento por el absurdo*: Se toma por hipótesis la negación de la consecuencia B (denotado no B) y se deberá mostrar que ésta negación implica la negación de la hipótesis A (denotado no A). En otros términos:

(A $\Rightarrow$ B) equivale lógicamente a (no B $\Rightarrow$ no A).

0.4.- Inclusión de conjuntos.

Definición.

Dados dos conjuntos A y B, decimos que el conjunto A está incluído en el conjunto B, si y solamente si:

$$\forall x \qquad (x \in A) \ \Rightarrow (x \in B)$$

Se denota A$\subset$ B y se lee "A está incluído en B". Esta relación es sinónima de la relación B $\supset$ A que se lee "B contiene A". También se puede decir que A es parte de B, o que A es subconjunto de B.

La relación $\subset$ entre conjuntos es una relación de orden (concepto que estudiaremos mas adelante); es decir que, se verifican las siguientes:

a)- $\forall A$ $\qquad A \subset A$ *(Reflexividad)*

b)- $\forall A, B$ $\qquad (A \subset B \ \wedge \ B \subset A) \ \Rightarrow \ A = B$ *(Antisimetría)*

c)- $\forall A, B, C$ $\qquad (A \subset B \ \wedge \ B \subset C) \ \Rightarrow \ A \subset C$ *(Transitividad)*

Estas propiedades, se demuestran a partir de la definición.

La relación de igualdad de dos conjuntos se define como sigue:

Igualdad de conjuntos.

Definición-

Se dice que el conjunto A es igual al conjunto B (y se denota A = B), sí y solamente sí,

$$\forall x \quad (x \in A) \quad \Leftrightarrow \quad (x \in B)$$

Se debe observar que ésta definición es equivalente a:

$$A = B \quad \Leftrightarrow \quad (A \subset B) \ \wedge \ (B \subset A)$$

La negación de ésta relación se enuncia. "Existe, en uno de los dos conjuntos, un elemento que no pertenece al otro", y se denota $A \neq B$ que se lee "A es diferente de B".

NOTA .- Muchos autores, distinguen la inclusión en amplia y estricta. La inclusión amplia definen como la inclusión que hemos definido nosotros, y la denotan como $A \subseteq B$, (El conjunto A está incluido en el B) y la *inclusión estricta*, que se define a partir de ésta como:

$$A \subset B \quad \Leftrightarrow \quad (A \subseteq B \quad \wedge \quad A \neq B).$$

Nosotros en lo que sigue, haremos referencia a la inclusión amplia, como hemos definido más arriba y lo denotaremos como $A \subset B$.

0.5.- Parte de un conjunto. Conjunto de partes.

Definición.

Sea E un conjunto. Se llama parte de E (sub-conjunto de E) todo conjunto A que verifique $A \subset E$.

Por ejemplo, en el conjunto N de los números naturales, la propiedad de divisibilidad por 2 define una parte de N, el conjunto A de los números pares. Un número natural x pertenece a A, si existe un número y tal que $x = 2y$.

Se denota entonces:

$$A = \{x \in N / \exists\, y \in N \ \wedge \ x = 2y\}.$$

Toda parte A de un conjunto E es definida por una cierta propiedad P. Se denota, de manera general; $A = \{x \in E / P\}$.

Asimismo E es una parte de E definida en particular por

$$E = \{x \in E / \ x = x\}.$$

La parte de E que no tiene ningún elemento se denomina parte vacía de E y se denota Φ. Como no existe ningún elemento distinto de sí mismo, se tiene:

$$\Phi = \{ x \in E / x \neq x \}.$$

Todas las parte de E constituyen un nuevo conjunto, que se le denota P(E) y que se denomina conjunto de las partes de E.

Es decir:

$$P(E) = \{X / X \subset E\}$$

Ejemplo.

Si E = {1,2,3} entonces P(E) = {Φ; E; {1};{2};{3};{1,2};{1,3};{2,3}}.

Se tienen las siguientes equivalencias lógicas:

$$A \in P(E) \Leftrightarrow A \subset E,$$
$$\{a\} \in P(E) \Leftrightarrow a \in E.$$

Observemos también que: $E \in P(E)$ y $\Phi \in P(E)$.

Par ordenado.

Definición.

Sean a y b dos objetos.

Al conjunto $\{\{a\};\{a,b\}\}$ *se le llama par ordenado o pareja o cupla formado de a y b; se lo denota (a, b).*

En otros términos: a dos objetos cualesquiera a y b, se puede asociar un nuevo objeto, el par ordenado (a, b). A éstos dos objetos, a y b, se las denomina coordenadas: abscisa y ordenada, o también primer proyector y segundo proyector. El primer objeto "a" está tomado de un conjunto cualquiera E, el segundo objeto "b" de un conjunto cualquiera F. Estos pares (a, b) son los elementos de un nuevo conjunto, que se denomina conjunto producto de E por F.

Para la igualdad de dos pares, se tiene la siguiente equivalencia lógica:

$$(a, b) = (c, d) \Leftrightarrow (a = c \text{ y } b = d).$$

Ejemplo.

Si (a, 2) = (3, b) entonces será: (a = 3 e b = 2)

0.6. - Producto de dos conjuntos.

Definición.

Sean E y F dos conjuntos. Se llama conjunto producto de E por F (se denota ExF), al conjunto de pares (a, b), con $a \in E$ *y* $b \in F$.

Es decir: $E \times F = \{(a, b) / a \in E \ \wedge \ b \in F\}$

Ejemplo.

Sean $E = \{a, b\}$ y $F = \{1, 2, 3$, entonces $E \times F = \{(a,1); (a,2); (a,3); (b,1); (b,2); (b,3)\}$ y $F \times E = \{(1,a); (1,b); (2,a); (2,b); (3,a); (3,b)$.

Se tiene también, a toda evidencia,

$$E \times F = \Phi \ \Leftrightarrow \ (E = \Phi \ \vee \ F = \Phi),$$
$$E \times F \neq \Phi \ \Leftrightarrow \ (E \neq \Phi \ \wedge \ F \neq \Phi).$$

En el caso donde $E = F$, el producto $E \times F$ se denota E^2. Entonces los pares (a, b) y (b, a) son simultáneamente admisibles para dos elementos cualesquiera a y b de E y se tiene

$$(a, b) = (b, a) \ \Leftrightarrow \ a = b.$$

Se llama diagonal de E^2 al conjunto de pares (a, a) con $a \in E$.

0.7. -Intersección. Unión. Complementario

Consideremos un conjunto E. Vamos a definir en P(E) dos leyes de composición internas (ver mas adelante):

Intersección.-

A todo par $(A, B) \in P(E) \times P(E)$, asociamos una parte de E, denominado intersección de A y B, denotada $A \cap B$ y definida por

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

Es decir:

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

Ejemplo.

Sean $A = \{1,2,3,5,7\}$ y $B = \{0,2,3,7,9\}$, entonces $A \cap B = \{2,3,7\}$.

Dos partes A y B se dicen *disjuntas* si $A \cap B = \Phi$.

Unión:

A todo par $(A, B) \in P(E) \times P(E)$, asociamos una parte de E, denominada unión de A y B, denotada $A \cup B$ y definida por

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

Es decir:

$$\forall x \in E, \qquad x \in A \cup B \quad \Leftrightarrow \quad (x \in A \vee x \in B)$$

Ejemplo.

Sean $A = \{1,2,3,5,7\}$ y $B = \{0,2,3,7,9\}$, entonces $A \cup B = \{0,1,2,3,5,7,9\}$.

Se tiene evidentemente

$$A \cup B = \Phi \Rightarrow (A = \Phi \wedge B = \Phi).$$

Las dos leyes son *conmutativas:*

$$A \cap B = B \cap A \qquad y \qquad A \cup B = B \cup A.$$

Las dos son *asociativas:*

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

Son *distributivas una respecto la otra:*

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

Complementario*:*

Sean A y B en P (E) tales que $A \subset B$. Se llama complementario de A en B y se le denota B - A, la parte de E definida como sigue:

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

Es decir:

$$\forall x \in E \qquad (x \in B - A) \quad \Leftrightarrow \quad (x \in B \wedge x \notin A).$$

Ejemplo.

Sean $A = \{1,2,3,5,7\}$ y $B = \{0,2,3,7,9\}$, entonces $B - A = \{0,9\}$ y $A - B = \{1,5\}$.

Si se supone $B \subset A$, se tienen las siguientes relaciones:

$$B \cup (A - B) = A, \qquad A - A = \Phi,$$
$$B \cap (A - B) = \Phi, \qquad A - \Phi = A.$$

Sea E el conjunto de referencia y A una parte de E, al complementario de A en E se le denomina el complemento de A y se lo denota A' o también A^c. Es decir:

$$A' = E - A = \{x \in E / \ x \notin A\}$$

Es decir:

$$\forall x \in E \qquad (x \in A') \quad \Leftrightarrow \quad (x \notin A)$$

Ejemplo.

Si E = **Z** (números enteros) y A es el conjunto de los números estrictamente positivos, es decir, $A = \{x \in \mathbf{Z} / \ x > 0\}$, entonces $A' = \{x \in \mathbf{Z} / \ x \leq 0$.

0.8.- Leyes de DeMorgan.

1.-El complementario (o complemento) de la unión es igual a la intersección de los complementarios. Para dos partes cualquiera A y B de E, se tiene

$$E - (A \cup B) = (E - A) \cap (E - B), \qquad \text{o también:} \qquad (A \cup B)' = A' \cap B'$$

2.-El complementario de la intersección es igual a la unión de los complementarios:

$$E - (A \cap B) = (E - A) \cup (E - B), \qquad \text{o también} \qquad (A \cap B)' = A' \cup B'$$

Estas dos propiedades se demuestran usando algunas leyes lógicas y las definiciones anteriores

Es conveniente, a esta altura que el alumno pruebe la validez de la distributividad del producto escalar respecto a la intersección, a la unión y a la diferencia de conjuntos. Es decir:

a.- $A \times (B \cap C) = (A \times B) \cap (A \times C)$
b.- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
c.- $A \times (B - C) = (A \times B) - (A \times C)$

0.9.- Diferencia Simétrica.

A todo par $(A, B) \in P(E) \times P(E)$, asociamos una parte de E, denominada *diferencia simétrica* de A y B, denotada $A \Delta B$ y definida por:

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

Es decir:

$$\forall x \in E, \qquad x \in (A \Delta B) \quad \Leftrightarrow \quad (x \in A \ \underline{\vee} \ x \in B)$$

Ejemplo.

Sean $A = \{1,2,3,5,7\}$ y $B = \{0,2,3,7,9\}$, entonces $A \Delta B = \{1,5,9\}$.

A partir de la definición, surge que:

$$\begin{aligned} A \Delta B &= (A \cup B) - (A \cap B) \\ &= (A - B) \cup (B - A) \\ &= (A \cap B') \cup (B \cap A') \end{aligned}$$

Expresiones que el lector las puede probar, usando la definición dada. Además se pueden establecer las siguientes relaciones:

$$A \Delta B = [A - (A \cap B)] \cup [B - (A \cap B)],$$

$$(A \Delta B) \cap A = A - (A \cap B),$$

$$E - (A \Delta B) = (A \cap B) \cup [E - (A \cup B)].$$

La diferencia simétrica de conjuntos es conmutativa y asociativa, en particular la asociatividad, su demostración, es un buen ejercicio para el alumno en éste punto de la lectura.

0.10.- Grafo.

Definición.

Dados los conjuntos A, B *y* AxB. *Se llama grafo* Γ *a una parte de* AxB.

Es decir, es un conjunto de pares ordenados (x, y) de A x B.

Ejemplo .-

Si A = {a, b, c}; B = {1, 2}; Γ = {(a, 1); (b, 1); (c, 1); (c, 2)} es un grafo, dado que $\Gamma \subset A \times B$

Axioma

Sea Γ *un grafo. Existe uno y sólo un conjunto, denotado* $pr_1\Gamma$ *(respectivamente* $pr_2\Gamma$, *poseyendo la propiedad siguiente:*

$$\forall x \quad (x \in pr_1\Gamma) \Leftrightarrow [\exists y \ (x, y) \in \Gamma]$$
$$\{\text{resp. } \forall y \quad (y \in pr_2\Gamma) \Leftrightarrow [\exists x \ (x, y) \in \Gamma]\}$$

OBSERVACIÓN-

a) Todo grafo donde una de sus proyecciones es vacía, es, así mismo el conjunto vacío.

b) Todo grafo Γ es parte de un conjunto producto (a saber $pr_1\Gamma \times pr_2\Gamma$ o, en forma más general, A x B con $A \supset pr_1\Gamma$ y $B \supset pr_2\Gamma$). Inversamente, es evidente que una parte de un conjunto producto es un grafo.

Proyección de un grafo.

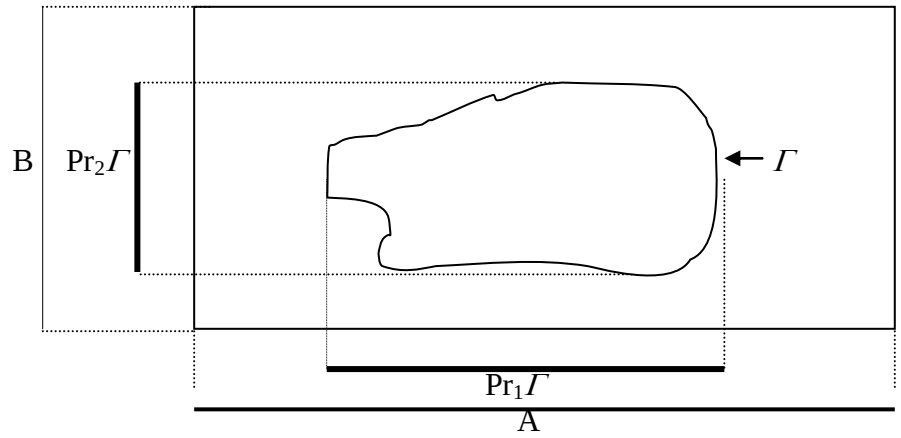
Definición.

Se llama primer proyector del grafo $\Gamma \subset A \times B$, *al conjunto de los elementos* x *de* A *tales que el par ordenado* $(x, y) \in \Gamma$

$$Pr_1\Gamma = \{x \in A / (x, y) \in \Gamma\}$$

De la misma manera se define la *segunda proyección del grafo* Γ *como el conjunto de los elementos* $y \in B$, *tales que punto* $(x, y) \in \Gamma \subset A \times B$.

$$Pr_2\Gamma = \{ y \in B/ (x, y) \in \Gamma\}$$



OBSERVACIÓN-

a)Todo grafo donde una de sus proyecciones es vacía, es, así mismo el conjunto vacío.

b) Todo grafo Γ es parte de un conjunto producto (a saber $pr_1\Gamma \times pr_2\Gamma$ o, en forma más general, $A \times B$ con $A \supset pr_1\Gamma$ y $B \supset pr_2\Gamma$). Inversamente, es evidente que una parte de un conjunto producto es un grafo.

Corte de un Grafo.

Definición.

Sea x_0 *un elemento de* A. *Se llama corte del grafo* Γ, *según el elemento* x_0, *al conjunto de los pares ordenados* (x_0 , y) *que pertenecen a* Γ.

$$C(x_0) = \{(x_0, y) \in ExF / (x_0, y) \in \Gamma \}$$

Es evidente que $C(x_0) \neq \phi$ si $x_0 \in Pr_1\Gamma$ y $C(x_0) = \phi$ si $x_0 \in (Pr_1\Gamma)'$

De la misma manera se define el corte del grafo Γ, según y_0 como el conjunto de pares ordenados (x, y_0) de Γ.

$$C(y_0) = \{(x, y_0) \in ExF / (x, y_0) \in \Gamma \}$$

Representación de los grafos.

Los grafos se representan por diferentes esquemas:

1.- Cuando la primera y segunda componente del par ordenado son la abscisa y ordenada del punto representado por el par, referido a dos ejes.

2.- Tabla de doble entrada. Los elementos de E se escriben horizontalmente y los de F verticalmente. Con una cruz se marcan los elementos que pertenecen al Grafo.

3.- Diagrama cartesiano. Está formado por un reticulado de rectas que indican los elementos de cada conjunto. Las verticales corresponden al conjunto de partida E y las horizontales al conjunto de llegada F.

4.- Diagrama sagital. Los elementos de cada conjunto son puntos, y una flecha une la primera componente con la segunda.

5.- Diagrama de Euler o Venn. Los conjuntos E y F se representan por puntos encerrados por una curva

Los subconjuntos de RxR y su representación gráfica en el plano son muy importantes en matemáticas. No solamente permiten analizar las relaciones numéricas en forma sistemática, sino que también dan una idea intuitiva de las relaciones.

El estudio de esta Unidad, se debe realizar conjuntamente con la guía de trabajos prácticos correspondiente, más los ejemplos y problemas que se desarrollan en las clases teóricas.

Damos a continuación una lista de ejercicios de aplicación

.

Ejercicios y Problemas propuestos.

1.- Colocar el signo $\in$ o $\notin$, según corresponda en las situaciones siguientes:
a) $(1- i)^2$ _ **R;** b) -1 _ **C**; c) $(1 - i)^3$ _ {3 + 4i , 4 +4i , -i}; d) $(2)^{1/2}$ _ **Q** ; 1- i _ **R**.

2.- Denotar los siguientes conjuntos.
a) El conjunto de enteros impares; b) El conjunto de naturales pares, divisibles por 7 y menores que 30; c) El conjunto de todos los enteros negativos cuyos cuadrados son menores que 50; d) Los números reales positivos no mayores que $2^{1/2}$.

3.- Determinar los conjuntos de números reales que hacen verdaderas las siguientes proposiciones.
a) $2x + 4 = 12$; b) $3x^2 - 4 = 23$; c) $6x^2 - 7x - 3 = 0$; d) $-3x^2 + 12x = 0$;

e) $x^2- 4 < 0$ f) $\sqrt{4 - 3x} = x + 2$; g) $\frac{x^2 - 4}{x - 2} = x + 2$; h) $\log_{10}\{x(x - 1)\} < 0$;

4.- Para los conjuntos $A = \{a , b, c, d\}$ y $B = \{b, d, e\}$, haga una lista de los conjuntos C que tienen la propiedad de que:

$$C \subset A \quad y \quad C \subset B.$$

5.- Si $A = \{1, 2, 3, 4\}$. ¿Cuáles son los conjuntos B tales que $\{1, 2\} \subset B$ y $B \subset A$?.

6.- Fijando un conjunto referencial E, exhiba cuatro conjuntos A, B, C y D tales que:

$$A \subset B ; \quad C \subset D ; \quad A \not\subset C ; \quad C \not\subset A ; \quad B \not\subset D \quad y \quad D \not\subset B .$$

7.- Sea el conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \subset \mathbf{Z}$. Determinar los siguientes sub-conjuntos de A:

a) $\{x/x^2 \in A\}$; b) $\{x/ 1+x \in A\}$; c) {x/x es cuadrado perfecto en A};
d) {x/x es primo}; e) $\{x / x < 5\}$; f)$\{x/3x = 1\}$; g) $\{x/x^2 < 16\}$;
h) {x/x es producto de primos distintos}; i) $\{x/ 1 + x + x^2 \in A\}$;
k) $\{x/x = 2^k, k \in \mathbf{N}\}$; l) $\{x/ x^3 < 100\}$; ll) $\{x/x^2 = 0\}$; m) $\{x/x - 1 \notin A\}$;

8.- Determine todos los elementos de P(E) si $E = \{1, 2, 3\}$.

9.- Determine P(E) y P(P(E)), para un conjunto E con un elemento.

10.- Si $A = \{2, 3, 4\}$; ¿Qué valores de verdad tienen las siguientes proposiciones?

a) $\varnothing \subset A$; b) $\varnothing \in A$; c) $\varnothing \in P(A)$; d) $\varnothing \subset P(A)$; e) $\{2, 3\} \in P(A)$;
f) $2 \in P(A)$; g) $A \in P(A)$; h) $A \in A$; i) $A \subset A$.

11.- Si $A = \{1, \{\varnothing\}, 2, \{1\}\}$. Colocar el signo que corresponda en las siguientes situaciones:

a) $\varnothing$ _ A; b) $\varnothing$ _ P(A); c) $\{\varnothing\}$ _ A; d) $\{\varnothing\}$ _ P(A);
e) $\{\{\varnothing\}\}$ _ A; f) $\{\{\varnothing\}\}$ _ P(A); g) 1 _ A; h) {1} _ P(A);
i) {1} _ P(A); j) $\{\{1\}\}$ _ A; k) $\{1, \{1\}\}$ _ A; l) $\{\{1, \{1\}\}$ _ P(A);
ll) $\{2, \{1\}\}$ _ P(A); m) {1, 2} _ A; n) $\{1, \{\varnothing\}\}$ _ A ; o) 2 _ P(A).

12.- Dados $E = \{a, b, c, d\}$; $A = \{a, c, d\}$; $B = \{b, c\}$.
Determinar: a) $A \cap B$; b) $A \cup B$; c) A'; d) B'.

13.- Si $A = \{a, b, c, d\}$ y $B = \{b, d, e\}$; determine:
$A \cap B$, $A \cup B$, $A \cap A$, $B \cap B$, $B \cup B$, $A \cap \varnothing$, $A \cup \varnothing$, $B \cup \varnothing$.

14.Si E = N; A = {números naturales divisibles por 2}; B ={números naturales divisibles por 3}. Halle: $A \cap B$; $A \cup B$; A'; B'.

15.- Si E = R ; A = {números reales mayores que -1}; B = {números menores o iguales a 1}. Halle:

$$A \cap B; \quad A \cup B; \quad A'; \quad B'.$$

16.- Construya diagramas de Venn para cada uno de los siguientes conjuntos:

a) $(A \cap B) \cup (C \cap B)$; b) $(A \cap B \cap C) \cup [A - (B \cup C)]$; c) $E - [C - (A \cup B)]$;
d) $[(A \cap B) - C] \cup [(B \cap C) - A] \cup [(A \cap C) - B]$; e) $(A \cup C) - B$;

f) $[(A\ C) - B] \cup [(B \cap C) - A]$; g) $[C - (A \cap B)] \cup (A \cap B \cap C)]$;
h) $\{(A\Delta C) - [(B \cap C) \cup (A \cap B)]\} \cup [B - (A \cup C)]$.

17.- Demostrar:

a) $(A \subset B \wedge A \subset C) \Rightarrow A \subset (B \cap C)$; b) $A \subset \varnothing \Rightarrow A = \varnothing$;
c) $A - B = A - (A \cap B) = (A \cup B) - B$; d) $(A \cup C) - C = (A - C) \cup (B - C)$;
e) $(A \cap B) - C = (A - C) \cap (B - C)$; f) $(A - B) - C = A - (B \cup C)$;
g) $A - (B - C) = (A - B) \cup (A \cap C)$; h) $A \cup (B - C) = (A \cup B) - (C - A)$;
i) $A - (A - B) = A \cap B$; j) $A \cup (B - A) = A \cup B$.

18.- Determine los elementos de los subconjuntos A y B contenidos en E sabiendo que:
$A' = \{f, g, h, l\}$; $A \cup B = \{a, b, d, e, f\}$; $A \cap B = \{d, e\}$.

19.- Determine E y sus subconjuntos A, B, C sabiendo que:
$(A \cup B \cup C) = \{1, 8, 12\}$; $B \cap C = \varnothing$; $A \cap C = \{5\}$;
$A \cup B = \{2, 3, 4, 5, 7, 9\}$; $A \cup C = \{2, 3, 4, 5, 6, 10, 11\}$; $B' = \{1, 2, 5, 6, 8, 10, 11, 12\}$.

20.- Determine los elementos de A y B sabiendo que:
$A\Delta B = \{1, 2, 3, 4, 5\}$; $B' = \{1, 4, 7\}$; $A' = \{2, 3, 5, 7\}$; $E = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

21.- En la edición de un libro han resultado 120 ejemplares con fallas: fallas en el papel, fallas en la impresión o fallas de encuadernación.

Si se sabe que:

68 libros tienen la primera falla por lo menos.
32 libros tienen la segunda falla por lo menos.
40 libros tienen la primera falla solamente.
5 libros tienen la primera y la segunda falla, pero no la tercera.
17 libros tienen la segunda y tercera, pero no la primera
4 libros tienen las tres fallas.

¿Cuántos libros tienen sólo la tercera falla? ¿cuántos tienen la tercera falla por lo menos?.

22.- 100 personas respondieron a un cuestionario formado por 3 preguntas. Cada pregunta debía contestarse por sí o por no y una sola de estas respuestas era correcta. Si sabemos que:

8 personas contestaron bien las tres preguntas.
9 personas contestaron bien solo la primera y la segunda.
11 personas contestaron bien solo la primera y la tercera.
6 personas contestaron bien solo la segunda y la tercera.
55 personas contestaron bien solo la primera pregunta, por lo menos.
32 personas contestaron bien solo segunda pregunta, por lo menos.
49 personas contestaron bien solo la tercera pregunta , por lo menos.

23.- Sea A el conjunto de rosas de una florería y B el conjunto de flores amarillas de ese negocio.

a) Determine los conjuntos $A \cup B$; $A \cap B$; $A - B$ y $B - A$.

b) Si el negocio no tiene flores amarillas; determine $A \cap B$.

c) ¿Podría usted determinar el conjunto $A - B$ en el caso en que todas las flores fueran amarillas?.

d) ¿Cómo expresaría que todas las flores amarillas del negocio son rosas? ¿Qué puede afirmar en este caso, del conjunto $B - A$?.

24.- Una encuesta llevada a cabo en un conjunto de 100 pacientes con enfermedades pulmonares dió los resultados siguientes: 45 fumadores que vivían en áreas urbanas, 37 de los cuales no tenían tareas insalubres; 20 personas con tareas insalubres, de las cuales 10 viven en el área urbana y 10 fuman; 5 personas que no fuman, viven en el área urbana y no tienen trabajos insalubres; 10 que no fuman ni tienen tareas insalubres ni viven en área urbana y por último 75 fumadores.

a) ¿Cuántos pacientes con tareas insalubres ni fuman ni viven en área urbana?

b) ¿Cuántos pacientes viven en área urbana?

c) ¿Cuantos pacientes fuman y tienen tareas insalubres?

d)¿Cuántos pacientes que fuman, se ocupan en tareas insalubres y viven en área urbana?

25.- Sean $A = \{1, 2, 3\}$; $B = \{2, 4\}$ y $C = \{3, 4, 5\}$. Determine:

a) $A \times B$; b) $A \times C$; c) $(A \times B) \times C$; d) $A \times (B \cap C)$;

e) $A \times (B \cap C)$; f) $(A \times B) \cap C$; g) $(A \times B) \cap (A \times C)$; h) $(A \times B) \cap (A \times C)$.

26.- Si A y B son conjuntos, demuestre las siguientes relaciones:

a) $A \times B = \varnothing \Leftrightarrow (A = \varnothing \vee B = \varnothing)$; b) $A \times B \subset C \times D \Leftrightarrow (A \subset C \wedge B \subset D)$;

c) $(AxB) \cap (CxD) = (A \cap C) \times (B \cap D)$; d) $[(AxB) \cup (C \times D)] \subset [(A \cup C) \times (B \cup D)]$

27.- Si $S \subset T$ explique porqué $S \times T \subset T \times T$; $S \times S \subset S \times T$.

28.- Si $E = \{1, 2, 3, 4, 5, 6, \}$: $A = \{2, 4, 6\}$; $B = \{4, 5, 6, 7, 8\}$.

Dé los elementos de $A \times B$; $(A \times B)'$

29.- Representar en R^2 (mediante un gráfico) los siguientes conjuntos:

a) $A = \{(x, y) / y = x\}$; b) $B = \{(x, y) / x + y = 5\}$; c) $C = \{ (x, y) / x = 2\}$;

d) $D = \{(x, y) / y = 3\}$; e) $E = \{(x, y) / y < x\}$; f) $F = \{(x, y) / y \geq x\}$;

g) $G = \{(x, y) / x \in [0,1] \wedge y \in]-1, 1[\}$ h) $H = \{(x, y) / x \in [0, 1] \wedge y \in [-1, 1]\}$;

i) $I = \{(x, y) / y \leq x^2 \}$; j) $J = \{ x, y) / y \geq \text{sen } x\}$.

30.- Hallar $A \cap B$ y representar en R^2 si:

$A = \{(x, y) / -1 < x + y < 1 \wedge -1 \leq x - y \leq 1\}$ y $B = \{(x, y) / -1 \leq x + y < 1 \wedge x^2 \leq 1\}$

31.- Dados $A = \{(x, y) / 2x - 3y + 6 \geq 0\}$; $B = \{(x, y) / 2x - y \leq 0\}$; $C = \{(x, y) / x^2 + y^2 \leq 1\}$;

$D = \{(x, y) / 6y - 2x \leq 3\}$; determine todas las intersecciones posibles.

32.-Sean $S = \{(x, y)/ x \in R, \ y \in R, \ y \geq x^2\}$ y $T = \{(x, y) / x \in R, \ y \in R, \ y \leq x + 2\}$.

a) Haga un dibujo de $S \cap T$; b) Halle el conjunto primera proyección de $S \cap T$; c) Halle el conjunto segunda proyección de $S \cap T$.

Además se pueden resolver los siguientes:

1. Sea A una parte cualquiera de E, de el resultado de cada una de las siguientes operaciones:

$A \cup A$; $A \cap A$; $A \cup \varnothing$; $A \cap \varnothing$; $A \cup E$; $A \cap E$; $A \cup (E-A)$; $A \cap (E-A)$.

2. Sea A y B dos partes cualesquiera de E, probar que las siguientes relaciones son equivalentes:

$$A \subset B; \quad (E-A) \supset (E-B); \quad A \cup B = B; \quad A \cap B = A.$$

La misma pregunta para las siguientes relaciones:

$$A \cap B = \varnothing ; \quad A \subset (E-B); \quad B \subset (E-A).$$

La misma pregunta para las siguientes relaciones:

$$A \cup B = E; \quad (E-A) \subset B; \quad (E-B) \subset A.$$

3. Probar las siguientes relaciones:

$(\forall\, A \in P(E))$ $E-(E-A) = A$,
$(\forall\, A \in P(E),\ \forall B \in P(E))$ $E-(A \cup B) = (E-A) \cap (E-B)$, $E-(A \cap B) = (E-A) \cup (E-B)$.

4. Sean A, B y C tres elementos de P(E). Probar que:

$$[(A \cup B) \subset (A \cup C) \text{ y } (A \cap B) \subset (A \cap C)] \Rightarrow B \subset C.$$

5. 1° Sean E y F dos conjuntos cualesquiera. Probar que
$$(A \subset E \text{ y } B \subset F) \Leftrightarrow A \times B \subset E \times F.$$

2° Sean E,F y G tres conjuntos cualesquiera. Probar que
$$(E \times G) \cup (F \times G) = (E \cup F) \times G.$$

3° Sean E,F,G y H cuatro conjuntos cualesquiera. Probar que
$$(E \times F) \cap (G \times H) = (E \cap G) \times (F \cap H).$$

1.- Aplicaciones o funciones y relaciones

INTRODUCCIÓN

En el desarrollo de la Unidad, se supone que el alumno tiene conocimientos elementales de Conectivos Lógicos, Conjuntos y de las operaciones entre conjuntos. De cualquier manera el Profesor, en las primeras clases explicará los conceptos fundamentales necesarios y mostrará la notación que usará en el desarrollo de la asignatura.

1.1.- Correspondencias.

Definición 1.

Sean E y F *dos conjuntos. se llama correspondencia de* E hacia F*, toda terna ordenada de la forma* (Γ, E, F) *donde* Γ *es una parte de* $E \times F$.

Dada la correspondencia; (Γ, E, F), se dice que E es el *conjunto de partida*; F es el *conjunto de llegada*:

OBSERVACIÓN.- Sean E y F dos conjuntos. A toda relación binaria $\Re$ de E hacia F, se le puede asociar la correspondencia (Γ, E, F) que admite por grafo el sub-conjunto de $E \times F$:

$$\Gamma = \{(x, y) \in E \times F / \Re(x, y)\}$$

Se dice que Γ es el *grafo de la relación* $\mathcal{R}$.

Al conjunto de las primeras componentes de los elementos Γ se le denomina de el *conjunto de definición (dominio)*, y se la denota $pr_1\Gamma$; al conjunto de las segundas componentes se le denomina *conjunto de los valores (imagen)* y se le donota $pr_2\Gamma$.

Es decir, se llama ***conjunto de definición*** de la relación $\mathcal{R}$ a la parte D de E definida como sigue:

$$D = pr_1\Gamma = \{x \in E / \exists y \in F;\ x\ \mathcal{R}\ y\}$$

Inversamente, a toda correspondencia (Γ, E, F) se puede asociar una relación binaria $\Re$ de E hacia F, conviniendo que $\Re(x, y)$ significa que $(x, y) \in \Gamma$.

Se puede así, "identificar" la relación de E hacia F y la correspondencia de E hacia F.

Se llama ***conjunto imagen*** de la relación $\mathfrak{R}$ a la parte $Im_{\mathfrak{R}}$ de F definida como sigue:

$$Im_{\mathfrak{R}} = pr_2\Gamma = \{y \in F / \exists x \in E;\ x\ \mathfrak{R}\ y\}$$

En definitiva, podemos decir ahora que:

Sean E y F dos conjuntos y Γ una parte no vacía de ExF. Consideremos todos los pares (a, b) que verifiquen $(a, b) \in \Gamma$. A tal par se la denotará a $\mathfrak{R}$ b , es decir:

$$(a, b) \in \Gamma \subset (E \times F) \quad \Leftrightarrow \quad a\ \mathfrak{R}\ b.$$

$\mathfrak{R}$ se denomina relación de E hacia F y Γ grafo de la correspondencia de E hacia F. $\Gamma \subset ExF$ se le denomina *grafo* de la relación $\mathfrak{R}$. E es *conjunto de partida* y F el *conjunto de llegada* de la relación $\mathfrak{R}$.

Definición 2

Sea un conjunto E. *Se llama relación binaria sobre* E *toda correspondencia de* E *hacia* E. Ya, hemos visto algunos ejemplos de relaciones binarias sobre un conjunto.

1. La *relación de igualdad* $a = b$ sobre un conjunto E donde el grafo Γ es la diagonal de E, conjunto de los pares (a, a) cuando a recorre E. El conjunto de definición A y el conjunto imagen $\mathfrak{R}$(a) coinciden con E.

2. La *relación de inclusión* $A \subset B$ es una relación binaria en P(E). El conjunto de definición y el conjunto imagen coinciden con P(E).

1. 2. - Aplicaciones

Definicion 3

Se califica de funcional todo grafo Γ tal que, para todo x, existe al menos un y que verifique $(x, y) \in \Gamma$

Aplicación. Definición 4.

Sean E y F dos conjuntos. Una aplicación de E en (o hacia) F es una correspondencia f = (Γ, E, F) tal que

$$\forall x \in E, \quad \exists! \, y \in F \qquad (x, y) \in \Gamma \qquad (1)$$

Sea f una aplicación de E en F (que nosotros escribiremos abreviadamente (Sea f: E $\rightarrow$ F). Estando dado x $\in$ E, al único elemento asociado por (1) se denota f(x). Se dice que x es un antecedente – no forzosamente único- de este elemento de F.
Es decir:

1. El *dominio de definición* de f es el conjunto E,
2. A todo x de E, f hace corresponder un y único en F.

A éste "y", se le llama ahora la *imagen* de x, se denota y = f(x).

El *conjunto imagen* de la aplicación es

$$f(E) = \{ y \in F / \; x \in E; \; y = f(x) \}.$$

Se denota también f(E) = Im f.
Todo elemento de F no es necesariamente la imagen de un elemento de E.

El *grafo de la función* es el conjunto de los (x, f(x)) cuando x recorre E. Es una parte de E x f(E).
O sea:

$$\Gamma_f = \{ (x, y) \in ExF \; / \; y = f(x) \}.$$

Si todo elemento x de E tiene la misma imagen a en F, la aplicación se dice constante.

$$(\forall x \in E) \qquad f(x) = a.$$

Supongamos, E = F. La relación f(x) = x, define una aplicación de E en E que se denomina aplicación idéntica o coincidencia y se la denota i. El grafo de esta aplicación es la diagonal de E^2

1.2.1- Igualdad. Restricción. Extensión

Definición 5.

Sean (E, F, f) y (E`, F`, g) dos aplicaciones. Se dirá que estas aplicaciones son iguales si se verifican las tres condiciones siguientes:

$$E` = E, \qquad F` = F \quad y \quad (\forall x \in E), \quad f(x) = g(x).$$

Se debe notar que una aplicación queda definida por la terna constituida por el conjunto de definición E, el conjunto de llegada F y la correspondencia unívoca f.

Definición 6

Sea (E, F, f) una aplicación y A una parte de E. Se llama restricción de la aplicación a A, a la aplicación (A, F, g) tal que

$$(\forall x \in A) \qquad g(x) = f(x).$$

Inversamente, dada una aplicación (A, F, g), se llama *extensión* de esta aplicación con $E \supset A$, toda aplicación (E, F, f) tal que $(\forall x \in E)$ $f(x) = g(x)$.

1. 2. 2.- Sobreyección. Inyección. Biyección

Definición 7.

Una aplicación (E, F, f) es sobreyectiva si f(E) = F.

Se dice entonces que f aplica E sobre F.

Ejemplos.

1. Si F contiene más de un elemento, toda aplicación constante de E en F no es sobreyectiva.

2. La aplicación $f: E \times F \rightarrow E$ (denominado *primer proyector*) $f(a, b) = a$ es sobreyectiva.

3. La aplicación (N, Z, f) definida por (a tomado de Z)

$$(\forall x \in N) \qquad f(x) = a + x$$

no es sobreyectiva.

4. La aplicación (Z, Z, f) definida por (a tomado de Z)

$$(\forall x \in Z) \qquad f(x) = a + x$$

es sobreyectiva.

Definición 8

Una aplicación (E, F, f) es inyectiva si

$$(\forall x, x' \in E) \qquad f(x) = f(x') \Rightarrow x = x'.$$

O la definición equivalente:

$$(\forall x, x' \in E) \qquad x \neq x \Rightarrow f(x) \neq f(x')\text{-}$$

Ejemplos.

1. El primer proyector $f : ExE \rightarrow E$ no es inyectiva, si E contiene más de un elemento. En efecto, para $b \neq b'$, se tiene:

$$f(a, b) = f(a, b') = a.$$

2. Sea a dado en N distinto de 0. La aplicación (N, N, f) definida por:

$$(\forall x \in N) \qquad f(x) = ax$$

es inyectiva (pero no es sobreyectiva si $a \neq 1$).

3. Sea a tomado de Z. La aplicación (N, Z, f) definida por:

$$(\forall x \in N) \qquad f(x) = a + x$$

es inyectiva.

Definición 9.

Una aplicación (E, F, f) es biyectiva si es sobreyectiva e inyectiva a la vez.

En otros términos, (E, F, f) es biyectiva si :

1. f(E) = F ;
2. $(\forall x, x' \in E) \quad f(x) = f(x') \Rightarrow x = x'$.

La propiedad (1) significa: "Todo y de F es la imagen de al menos un x de E".

La propiedad (2) significa además "Todo y de F es la imagen de un *solo* x de E". Se define así una aplicación (F, E, f^{-1}) tal que:

$$(y \in F) \qquad x = f^{-1}(y) \qquad \Leftrightarrow \qquad y = f(x) \qquad (x \in E).$$

Esta aplicación f es así mismo una biyección de F sobre E. Se la denomina la ***aplicación recíproca*** **de f .**

1.2.3. Composición de aplicaciones

Sean E, F, y G tres conjuntos y dos aplicaciones: (E, F, f) y (F, G, g) tales que el conjunto dominio de definición de la segunda coincida con el conjunto de llegada de la primera.

A todo x de F le corresponde un solo $y = f(x)$ en F.
A este y de F le corresponde un solo $z = g(y)$ en G.

Por consiguiente, a todo x de E le corresponde un único z en G que es $z = g[f(x)]$. Queda definida así una aplicación de E en G que se denota g o f y que se denomina *compuesta de f y g.*

Ejemplo.- La aplicación (Z, N, f) definida por:

$$(\forall x \in Z) \qquad f(x) = x^2$$

puede ser compuesta con la aplicación (N, N, g) definida por:

$$(\forall x \in N) \qquad g(x) = x + 2$$

para dar la aplicación compuesta $(Z, N, g \circ f)$ definida por:

$$(\forall x \in Z) \qquad (g \circ f)(x) = x^2 + 2.$$

Por la definición misma, la composición de aplicaciones es asociativa.

Sea $E \to F \to G \to H$.

Entonces, $(h \circ g) \circ f = h \circ (g \circ f)$.

La compuesta de dos sobreyecciones es una sobreyección

Si (E, F, f) e (F, G, g) son sobreyectivas, entonces $f(E) = F$ y $g(F) = G$ implica evidentemente $(g \circ f)(E) = G$.

La compuesta de dos inyecciones es una inyección.

Si (E, F, f) y (F, G, g) son inyecciones, entonces

$$g[f(x)] = g[f(x')] \quad \Rightarrow \quad f(x) = f(x') \quad \Rightarrow \quad x = x'.$$

Luego $(E, G, g \circ f)$ es inyectiva.

De ello resulta entonces que la compuesta de dos biyecciones es una biyección.

En particular, la compuesta de una biyección:

$f : E \to F$ y su recíproca $f^{-1} : F \to E$ es la aplicación idéntica sobre E.

$$f^{-1} \circ f = I_E.$$

Además, tenemos que:

$$f \circ f^{-1} = I_F.$$

Ejemplo 1.-
Se consideran tres conjuntos E, F, G y dos aplicaciones: $f : E \to F$ y $g : F \to G$.

a) Demostrar que $g \circ f$ inyectiva $\Rightarrow$ f inyectiva.
b) Demostrar que $g \circ f$ sobreyectiva $\Rightarrow$ g sobreyectiva.

Solución: a) Consideramos dos elementos cualesquiera del conjunto E, x' y x'' con la condición de que f(x') = f(x''), entonces se deduce de la definición de composición de funciones y de la condición de inyectividad que:

$$g[f(x')] = g[f(x'')] \Rightarrow (g \circ f)(x') = (g \circ f)(x'') \Rightarrow x' = x'',$$

por consiguiente f tendrá que ser inyectiva.

Solución: b) Consideremos las imágenes de las aplicaciones. Se tiene:

$$f(E) \subset F \Rightarrow g[f(E)] \subset g(F) \subset G,$$

por hipótesis, $(g \circ f)(E) = G$, por lo tanto $g(F) = G$ y g es sobreyectiva.

Ejemplo 2.- Sea f una aplicación de E en F.

a) Demostrar que f es inyectiva si, y solamente si, existe una aplicación g de F en E tal que $g \circ f = i_E$ (identidad sobre E).
b) Demostrar que f es sobreyectiva si, y solamente si, existe una aplicación g de F en E tal que $f \circ g = i_F$ (identidad sobre F).

Solución: a) Si existe g tal que $g \circ f = i_E$; entonces f es inyectiva por el ejemplo anterior, dado que i_E es inyectiva.
Inversamente, si f es inyectiva, con imagen f(E); todo $y \in f(E)$ es imagen de un solo x de E; supongamos g(y) = x. Para $y \in F - f(E)$, se elige arbitrariamente g(y); por ejemplo $g(y) = x_0$, donde x_0 es un elemento determinado de E. La aplicación g de F en E, así obtenida es tal que $g \circ f = i_E$. Es única si f es sobreyectiva.

Solución: b) Si existe g tal que $f \circ g = i_F$, dado que i_F es sobreyectiva, tenemos que f es sobreyectiva según se demostró en el Ejemplo 1.

Inversamente, supongamos f sobreyectiva: $\forall y \in F, \exists x, y = f(x)$. Admitamos que es posible asignar para cada y un x. La aplicación g así obtenida de F en E es tal que $f \circ g = i_F$. Será única si f es inyectiva.

Definición 10: Aplicación recíproca (Función inversa).

Dadas dos funciones biyectivas f y g y si $f \circ g = i$, (identidad sobre el dominio de g) decimos que la función g es la función recíproca de f y la denotamos $f^{-1} = g$; o también que f es la recíproca de g, es decir será $g^{-1} = f$.

Es decir toda vez que hacemos la composición de una función con su recíproca el resultado es una función identidad.

O sea, tendremos:

$f \circ f^{-1} = i$, (identidad sobre Df^{-1}) y
$f^{-1} \circ f = i$ (identidad sobre Df).

Muchas veces el problema que se plantea es determinar la función recíproca de una dada. Para que la función tenga recíproca tendrá que ser biyectiva.

OBSERVACIÓN.

No existe un procedimiento único para determinar a la función recíproca de una función dada, si bien, existen estrategias. Una estrategia muy útil en el caso de que la función se exprese analíticamente mediante una expresión explícita, $y = f(x)$, consiste en "despejar" la variable "independiente x" desde la expresión $y = f(x)$, e intercambiar la variable "dependiente y" por la variable x en la expresión obtenida.

Ejemplos.

1. La aplicación (Z, Z, f) definida por $(\forall x \in Z)$ $f(x) = a + x$ es una biyección .

La aplicación recíproca (Z, Z, f) definida por:

$$(\forall y \in Z) \qquad f(y) = y - a.$$

2. Sea A el conjunto de los números naturales pares. La aplicación (N, A, f):

$$(\forall x \in N) \qquad f(x) = 2x \text{ es una biyección.}$$

Para resolver el siguiente ejercicio, el alumno deberá apelar a sus conocimientos adquiridos sobre el conjunto de números reales, **R**, en etapas previas a su ingreso a la Facultad.

3.Determinar la función recíproca de la función dada por : $f(x) = \dfrac{x+5}{x+2}$

Solución:

* La expresión $\dfrac{x+5}{x+2}$ no tiene sentido si $x + 2 = 0$, por lo tanto,

$$Dom(f) = \mathbf{R} - \{-2\}$$

$$f : \mathbf{R} - \{-2\} \rightarrow \mathbf{R}$$

Para determinar su inversa se considera la expresión:

$$y = \frac{x+5}{x+2}$$

y se despeja x en términos de y

$$y = \frac{x+5}{x+2} \quad \Rightarrow \quad y\cdot(x+2) = x+5 \quad \Rightarrow \quad y\cdot x + 2y = x+5 \quad \Rightarrow \quad y\cdot x - x = 5 - 2y \quad \Rightarrow$$

$$\Rightarrow x = \frac{5-2y}{y-1}$$

así pues, se considera la función:

$$g : \mathbf{R} - \{1\} \rightarrow \mathbf{R}$$
$$x \rightarrow g(x) = \frac{5-2x}{x-1}$$

Dado que g no está definida en $x = 1$, se debe observar que $f(x)$ nunca toma el valor 1.

El alumno deberá verificarlo y además deberá probar que $(f \circ g)(x) = x$ y que $(g \circ f)(x) = x$.

1.2.4.- Permutación. Involución

Definición.

Se llama permutación de un conjunto E toda biyección de E sobre si mismo.

Ejemplo.- La aplicación (Z, Z, f) definida por:

$(\forall x \in Z)$ $\qquad f(x) = a + x$ es un permutación de Z.

Definición.

Se llama involución de E toda permutación de E que coincide con su recíproca.

Ejemplo.

1. La aplicación (Z, Z, f) definida en el ejemplo precedente no es una involución de Z.

2. La aplicación (Q^*, Q^*, f) definida por:

$$(\forall x \in Q^*) \qquad f(x) = 1/x$$

es una involución de Q^*. (Se recuerda que $Q^* = Q - \{0\}$.)

3. La aplicación (P(E), P(E), f): $f(X) = E - X$ es una involución de P(E).

1.2.5.-Monotonía de una función.

Sea f una función numérica definida sobre todo el conjunto D. Tenemos a los conjuntos I, J , K y G partes de D:

Si $\forall x_1 \in I$ y $x_2 \in I$ $(I \subset D)$, $x_1 < x_2 \Rightarrow f(x_1) \leq f(x_2)$; decimos, f es **creciente** sobre I.

Si $\forall\ x_1 \in J$ y $x_2 \in J$ $(J \subset D)$, $x_1 < x_2 \Rightarrow f(x_1) \geq f(x_2)$, decimos, f es **decreciente** sobre J.

Si $\forall x_1 \in K$ y $x_2 \in K$ $(K \subset D)$, $f(x_1) = f(x_2)$; decimos, f es **constante** sobre K.

Una función creciente (o decreciente) sobre un intervalo G de D se dice **monótona sobre G**

Por ejemplo:

La función lineal $x \to ax$ es creciente sobre **R** si $a > 0$ y decreciente sobre **R**, si $a < 0$.

La función afin $x \to ax + b$ es creciente sobre **R** si $a > 0$ y decreciente sobre **R**, si $a < 0$.

La función $x \to 1/x$, es decreciente sobre $\mathbf{R}_-^*$ y sobre $\mathbf{R}_+^*$.

La función $x \to \operatorname{sen} x$ es creciente en $[0; \pi/2]$ y decreciente en $[\pi/2; \pi]$.

1.2.6.-Paridad y periodicidad.

Definiciones:

Sea f definida $\forall x \in D$, $(D \subset \mathbf{R})$

- si $\forall x \in D$, $f(-x) = f(x)$; f se dice **par.**
- si $\forall x \in D$, $f(-x) = -f(x)$; f se dice **impar.**
- si $\exists\ t \in \mathbf{R}$ tal que $\forall x \in D$, $f(x + t) = f(x)$; f se dice **t-periódica.**

Por ejemplo:

1) $x \to x^2 + 4$ es una función par definida sobre **R**.

2) $x \to 5x^3 - 7x$ es una función impar definida sobre **R**.

3) $x \to x^3 - 5x^2 + 2x + 1$ es una función definida sobre **R** que no es ni par ni impar. (la imparidad no es la negación de la paridad).

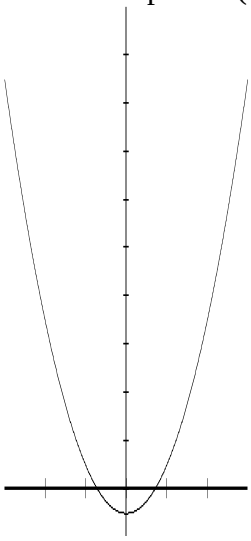
4) $x \to$ sen x es una función impar, 2π - periódica definida sobre **R**.

5) $x \to$ cos x es una función par, 2π - periódica definida sobre **R**.

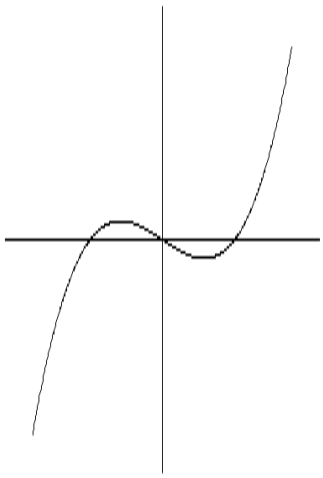
6) $x \to$ tan x es una función impar, π - periódica definida sobre $\mathbf{R} - \left\{\frac{\pi}{2} + k\pi, k \in \mathbf{Z}\right\}$.

Propiedades de la gráfica:

- si **f es par**, el eje **Oy** es eje de simetría de la gráfica
- si **f es impar**, el origen **O** es centro de simetría de la gráfica
- si **f es t-periódica**, y (x, f(x)) es un punto de la gráfica, entonces el punto (x + t, f(x)) también es un punto de la gráfica, pues f(x+t) = f(x).



Función par



Función impar

Consecuencias prácticas:

La paridad o la periodicidad de una función simplifica su estudio:

- Si f es par, se estudia sus variaciones sobre $\mathbf{R}_+$ y se completa su estudio por simetría respecto al eje **Oy**;
- Si f es impar, se estudia sus variaciones sobre $\mathbf{R}_+$ y se completa su estudio por simetría respecto al origen de coordenadas **O**;
- Si f es t-periódica, se estudia sus variaciones sobre un intervalo de amplitud t.

1.2.7.- Propiedades.

P_1 *Sea (E, F, f) una aplicación y A y B dos partes de E. Entonces:*

$$A \subset B \quad \Rightarrow \quad f(A) \subset f(B).$$

Prueba:

En efecto, sea $y \in f(A)$. Entonces existe $x \in A$ tal que $y = f(x)$. Pero $x \in A$ implica $x \in B$, Luego $y = f(x) \in f(B)$.

P_2 *Sea (E, F, f) una aplicación y A y B dos partes de E. Entonces:*

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

Prueba:

Es evidente que:

$$x \in (A \cup B) \quad \Rightarrow \quad f(x) \in [f(A) \cup f(B)],$$

luego

$$f(A \cup B) \subset [f(A) \cup f(B)].$$

Ahora,

$$A \subset (A \cup B) \quad \Rightarrow \quad f(A) \subset [f(A \cup B)] \qquad \text{(P1)},$$

$$B \subset (A \cup B) \quad \Rightarrow \quad f(B) \subset [f(A \cup B)],$$

Luego

$$[f(A) \cup f(B)] \subset f(A \cup B),$$

P_3 *Sea (E, F, f) una aplicación y A y B dos partes de E. Entonces*

$$f(A \cap B) \subset [f(A) \cap f(B)].$$

Prueba:

La igualdad se da si f es inyectiva.

La inclusión es evidente. La igualdad no se verifica si la aplicación no es inyectiva. Es suficiente, por ejemplo, considerar una aplicación constante $f(x) = a$ con $A \cap B = \phi$. Se tiene entonces

$$f(A \cap B) = \phi \quad y \quad f(A) \cap f(B) = \{a\}$$

si A y B no son vacíos. Pero si f es inyectiva, se prueba que

$$f(A) \cap f(B) \subset f(A \cap B).$$

-Sea $y \in [f(A) \cap f(B)]$. Existe entonces $x \in A$ y $x' \in B$ tales que: $y = f(x) = f(x')$ y como f es inyectiva, se deduce $x = x' \in [A \cap B]$, entonces $y \in f(A \cap B)$, que completa la demostración.

1.2.8.- Diversas maneras de definir una función.

a) A partir de una tabla de valores.

Ej. Alargamiento de un resorte en términos del peso colgado en uno de sus extremos..

Carga (N)	50	100	150	200	250
Alargamiento	20	41	59	80	95

La construcción gráfica de esta función está constituída por puntos aislados ya que la variable (carga) no puede tomar mas que valores aislados. En éste ejemplo no se conoce la expresión analítica de la función.

b) A partir de una fórmula explícita.

$t \rightarrow i(t) = A \text{ sen } \omega t$ nos dá la intensidad de una corriente alterna sinusoidal de amplitud A y de frecuencia ω dada.

c) A partir de una relación algebraica

$x \rightarrow f(x) = \frac{x^4 - 16}{x - 2}$; ésta función está definida sobre $D = \mathbf{R} - \{2\}$, pero además se puede observar que la expresión analítica se puede simplificar, siempre que x sea distinto a 2 y reescribirla como $f(x) = (x + 2)(x^2 + 4)$ (para $x \neq 2$).

d) A través de una curva representativa.

Por ejemplo la traza de un registrador de la presión atmosférica o de la temperatura en término del tiempo. Estas curvas en general no se van a corresponder con una expresión simple.

e) A partir de una construcción geométrica.

Por ejemplo, las funciones trigonométricas.
etc.

1.2.9.- Álgebra de las funciones reales.

Vamos a denotar $F(\mathbf{R})$, al conjunto de todas las funciones definidas de **R** a **R,** en ese conjunto se pueden considerar las siguientes operaciones o leyes de composición internas en $F(\mathbf{R})$.

1. Suma de funciones.

Sean dos funciones cualesquiera $f, g \in F(\mathbf{R})$, o sea:

$f : \mathbf{R} \to \mathbf{R}$, con $x \to f(x)$
$g : \mathbf{R} \to \mathbf{R}$, con $x \to g(x)$; se define la función suma como:

$f + g : \mathbf{R} \to \mathbf{R}$, con $x \to (f + g)(x) = f(x) + g(x)$; (ver mas adelante el estudio de los dominios)

2. Producto de funciones

Sean dos funciones cualesquiera $f, g \in F(\mathbf{R})$, o sea:

$f : \mathbf{R} \to \mathbf{R}$, con $x \to f(x)$
$g : \mathbf{R} \to \mathbf{R}$, con $x \to g(x)$; se define la función producto como:
$f \cdot g : \mathbf{R} \to \mathbf{R}$, con $x \to (f \cdot g)(x) = f(x) \cdot g(x)$

3. Composición de funciones

Sean dos funciones cualesquiera $f, g \in F(\mathbf{R})$, o sea:

$f : \mathbf{R} \to \mathbf{R}$, con $x \to f(x)$
$g : \mathbf{R} \to \mathbf{R}$, con $x \to g(x)$; se define la compuesta como:

$f \circ g : \mathbf{R} \to \mathbf{R}$, con $x \to (f \circ g)(x) = f[g(x)]$

Asimismo, se define una ley de composición externa (producto por un escalar)

4. Producto de un escalar (número real) por una función.

Sea una función cualquiera de $F(\mathbf{R})$, y un escalar cualquiera λ (número real), es decir:

$f : \mathbf{R} \to \mathbf{R}$, con $x \to f(x)$; se define una nueva función denotada:
$\lambda f : \mathbf{R} \to \mathbf{R}$, con $x \to (\lambda \cdot f)(x) = \lambda \cdot f(x)$

Para funciones cuyo dominio no es todo $\mathbf{R}$ también se pueden definir las anteriores leyes de composición de igual manera.

Ha de tenerse cuidado al determinar el dominio de la función resultante en cada operación. Así pues, se destacan las siguientes consideraciones:

- Los dominios de las funciones $f + g$ y $f \cdot g$ coinciden y son las intersecciones de los dominios de f y g.

- Una función f y su opuesta $(-f)$, tienen el mismo dominio.

- El dominio de la función f / g respecto al producto de $f \cdot g$ es el dominio de $f \cdot g$ menos los valores donde g se anula.

- El dominio de la función g o f es el de la función f menos los valores $x_0 \in D_f$ tales que $f(x_0) \notin D_g$.

1.3. Familia de partes. Partición de un conjunto. (ANEXO)

El estudio de este ítem, puede obviarse en una primer lectura. Para comprenderlo correctamente son necesarios algunos conceptos que se estudian más adelante.

Sea L un conjunto cualquiera de elementos, que serán denominados *índices.*

Un primer ejemplo está dada por $L = \{0,1,2, ..., n\} \subset N$ que es un conjunto *finito* de índices. Por lo contrario, $L = N$ es un ejemplo de conjunto *infinito* de índices. Más precisamente, se dirá por definición, que N es *infinito numerable*. Un tercer ejemplo está dado por $L = R$, conjunto de números reales, que es *infinito no numerable*.

Sea ahora E un conjunto cualquiera. Se llama *familia de partes* de E toda aplicación $\lambda \rightarrow A_\lambda$ de L en $P(E)$. La familia se denota $(A_\lambda)_{\lambda \in L}$.

Ejemplos.

1. En N, a todo $n \in N$ asociamos la parte

$$A_n = \{x \in N / x \leq n\}.$$

Se obtiene una familia numerable $(A_n)_{n \in N}$ de partes de N.

2. En el plano R^2, A todo $\lambda \in R$ asociamos la recta

$$D_\lambda : y = \lambda x.$$

Se obtiene una familia $(D_\lambda)_{\lambda \in R}$ (no numerable) de partes de R^2: Es la familia de las rectas del plano que contienen al origen, con la exclusión de la recta $x = 0$.

Para toda familia $(A_\lambda)_{\lambda \in L}$ se define la *unión:*

$$\bigcup_{\lambda \in L} A_\lambda = \{x \in E / \ \exists \lambda \in L; \ x \in A\}$$

y se define la *intersección:*

$$\bigcap_{\lambda \in L} A_\lambda = \{x \in E / \ \forall \lambda \in L; \ x \in A\}.$$

***Partición de un conjunto*.**

Sea E un conjunto. Se llama partición de E toda familia $(A_\lambda)_{\lambda \in L}$ *de partes no vacías de E tal que*

1. $\bigcup_{\lambda \in L} A_\lambda = E;$

2. $(\forall \lambda, \lambda' \in L), \quad A_\lambda \neq A_{\lambda'} \Rightarrow A_\lambda \cap A_\lambda = \Phi$.

En otros términos, una partición de E es una familia de partes no vacías de E, dos a dos disjuntas, donde la unión es igual a E.

Ejemplo.- Sea a un número fijo en R*. La familia de intervalos [ka, (k+1)a[cuando k recorre Z (que aquí es el conjunto de índices) es una partición de R.

Ejercicios propuestos.

1.- Sea la correspondencia (E, F, f) con E = {a, b, c, d}; F = {1, 2, 3} y definida por: f(a) = 2; f(a) = 3; f(c) = 2; f(c) = 3. Determine:
a) el conjunto de partida; b) el conjunto de definición; c) el conjunto de llegada; d) el conjunto de valores; e) haga un diagrama de la correspondencia.

2.- a) Sea E = {a, b, c, d} y f(a) = b; f(b) = c; f(c) = b; f(d) = a; Halle el grafo de la correspondencia f y dibújelo en un sistema de coordenadas.
b) Sea E = {a, e, i, o, u, v, w}. Supongamos que g es la relación que a cada letra de E le hace corresponder la letra siguiente según el orden alfabético. Halle el grafo de la relación g.

3.- Sea A = {1, 2} y B = {p, q}. Enumérense todas las relaciones posibles de A en B.

4.- Sea A = {a, b, c}. a) Halle P(A). b) Halle en P(A) x P(A) la relación de $\subset$ (inclusión).

5.- Sean dos conjuntos, E = {3, 5, 7} y F = {1, 3, 11, 17}. a) ¿Cuál es el grafo de la relación $x + y < 15$; con $x \in E$ y $y \in F$. b) Determine el dominio de la relación. c) Determine el conjunto imagen de la relación.

6.- Sean E = {1, 2, 3, 4] y F = {1, 3, 5}, y la relación definida por "x es menor que y".
a) Escriba el grafo de la relación. b) Dibuje el grafo. c) Halle la relación recíproca.

7.- Sean las relaciones f y g definidas por los grafos: $F \subset A \times B = \{(a, a); (b, e); (d, e)\}$; $G \subset B \times C = \{(a, u); (a, v); (e, w); (f, w)\}$; con A = {a, b, c, d}; B = {a, e, f}; C = {u, v, w}. Determinar el grafo de g o f.

8.- Dada la relación definida por $\{(x, y) \in R \times R / x^2 + y^2 = 4\}$
a) Dibujar el grafo de la relación.
b) Determinar el conjunto dominio de la relación.
c) Determinar el conjunto imagen de la relación.

9.- Haga un dibujo aproximado en R x R de las siguientes relaciones.(si se acuerda de lo aprendido previamente al curso).

a) $y \leq x^2$; b) $y < 3 - x$; c) $y > \log x$; d) $y \geq \text{sen } x$.

10.- Sea $S = \{(x, y) / x \in R, y \in R, 4x^2 + 9y^2 = 36\}$. Construya un dibujo de S en R x R y halle: a) el dominio de S; b) el conjunto imagen de S; c) el grafo de la relación inversa.

11.- Obtener las gráficas y decir cuáles de las siguientes relaciones son funciones. Dar una razón para las respuestas.

a) {(5, 2); (0,4); (3, 5); (8, 20); (9, 15)}; b) {(5, -24); (0,30); (3, 6); (7, 11); (8,9)};
c) {(3, 4); (6, 5); (3, 7); -2, 1); (8, 9)}; d) {(5, -4); (0,6); (3, 3); (8, 9); (7, 10); (11, 6)}

12.- Construya todas las aplicaciones distintas del conjunto $E = \{1, 2, 3\}$ al conjunto $F = \{1, 0\}$.

13.- Sea $f : \mathbf{R} \rightarrow \mathbf{R}$, definida por : $f(x) = \begin{cases} 3x - 1, & \text{si } x > 3 \\ x^2 - 2, & \text{si } -2 \leq x \leq 3 \\ 2x + 3, & \text{si } x < -2 \end{cases}$

i) Halle: a) f(2); b) f(4); c) f(-1); d) f(-3).
ii) Dibuje su gráfico.

14.- Si $h = \{(5, 6); (4, 3); (2, 1); (7, 9)\}$; a) dar el dominio de h; b) el conjunto imagen.

15.- Decir si las siguientes relaciones son o no funciones y dar una razón para su respuesta. En cada ejercicio obtener su gráfica y dar su dominio y conjunto imagen.

a) $\{(x, y) / y^2 = 25x\}$; b) $\{(x, y) / x^2 + y^2 = 16\}$; c) $\{(x, y) / y = -3x + 4\}$;
d) $\{(x, y) / y = (9 - x)^{1/2}\}$; e) $\{(x, y) / y = 5/x\}$; f) $\{(u, v) / u = v^2\}$.

16.- Si f es la función dada por $f(x) = 2x^3$, determinar:

a) f(-2); f(-1); f(0); f(1); f(2); b) $f(x_1)$; $f(x_2)$; $f(x_2 - x_1)$; $f(x_2) - f(x_1)$.

17.-Si f está dada por $f(x) = \sqrt{9 - x}$; determinar: f(x) + f(h) y probar si $f(x + h) \neq f(x) + f(h)$.

18.- Si $f(x) = x^2 + 4$, determinar 9 puntos de la gráfica de f. Construir la gráfica de f y dar el dominio y conjunto imagen.

19.- Idem del 8, pero con $f(x) = - x^2 + 4$.-

20.- Si $g(x) = \dfrac{x^2 + 3x + 2}{x + 5}$, determinar g(1); g(1/2); g(-1); g(0). ¿Existe g(-5)?. Explicar su repuesta.

21.- Determine el dominio de las funciones dadas por:

a) $f(x) = ax + b$; b) $f(x) = ax^2 + bx + x$ con $a \neq 0$; c) $f(x) = 1/ x$;
d) $f(x) = \sqrt{x + 2}$; e) $f(x) = \sqrt{x^2 - 4}$; f) $f(x) = \dfrac{x}{(x + 2)(x - 3)}$; g) $f(x) = \dfrac{1}{x^2 + 4}$
h) $f(x) = \dfrac{x}{x^2 - 9}$; i) $f(x) = \ln x$; j) $f(x) = \ln(x + 2)$; k) $f(x) = \text{sen } x$;

l) $f(x) = \ln (x^2 + 2)$; m) $f(x) = \ln (x^2 - 9)$.

22.- Si $E = \{a, b, c, d, e\}$, la función $f: E \to E$ definida por:
Grf = {(a, c); (b, e); (c, e); (d, e); (e, c)}. Diga : a) si es aplicación; b) si es inyectiva;
c) si es sobreyectiva; d) haga un diagrama.

23.- Dado $E = \{-2, -1, 0, 1, 2\}$ y la función $f: E \to \mathbf{R}$, dada por $f(x) = x^2 + 1$. Halle el conjunto imagen de f. ¿ Es inyectiva, es sobreyectiva?.

24.- Sean $A = [-1, 1]$; $B = [1, 3]$ y $C = [-3, -1]$ y sean las funciones $f_1: A \to \mathbf{R}$; $f_2: B \to \mathbf{R}$; $f_2 : C \to \mathbf{R}$; definidas por la siguiente regla: a cada número se le asigna su cuadrado.
a) ¿Cuáles de las funciones son inyectivas? y ¿cuáles sobreyectivas?.
b) i) Halle el intervalo máximo D, en el cuál la fórmula $f(x) = x^2$, define una función inyectiva. ii) El codominio máximo para que la función sea sobreyectiva.

25.- Sea $E = [-1. 1]$ y las funciones g y h definidas de E en **R** por:
$g(x) = x^3$ y $h(x) = \text{sen } x$.
Diga si son inyectivas y/o sobreyectivas.

26.- a) Diga para que conjuntos la función idéntica es biyectiva.
b) Dé el codominio de una función constante que sea sobreyectiva.

27.- Pruebe que la función $f : \mathbf{R} \to \mathbf{R}$ dada por $f(x) = 2x - 1$ es biyectiva.-

28.- Sean $E = \{1, 2, 3, 4, 5\}$ y las funciones $f: E \to E$; $g : E \to E$ definidas por:
Grf = {(1, 3); (2, 5); (3, 4); (4, 1); (5, 2)}; Grg = {(1, 4); (2, 1); (3, 5); (4, 2); (5, 3)}.
Halle gof y fog.

29.- Sean $f: \mathbf{R} \to \mathbf{R}$ y $g: \mathbf{R} \to \mathbf{R}$ definidas por: $f(x) = x^2 - 2|x|$, $g(x) = x^2 + 1$.
Halle (fog)(x); (gof)(x); (gof)(3); (fog)(-2); (gof)(-4); (fog)(5).

30.- Demuestre que:
a) Si $f : A \to B$ y $g : B \to C$ son inyectivas entonces gof es inyectiva
b) Si $f : A \to B$ y $g : B \to C$ son sobreyectivas entonces gof es sobreyectiva.
c) Si $f : A \to B$ y $g : B \to C$ son biyectivas entonces gof es biyectiva
d) Si gof es inyectiva entonces f es inyectiva.
e) Si gof es sobreyectiva entonces g es sobreyectiva.

31.- Si f es una biyección de un conjunto E sobre F, probar que: a) $f \circ f^{-1} = i_F$;
b) $f^{-1} \circ f = i_E$

32.- Sea $\Im$ el conjunto de las aplicaciones de E en F y $\wp$ el conjunto de aplicaciones de F en E. Si existe una aplicación $g \in \wp$ tal que $g \circ f = i_E$, entonces la aplicación $f \in \Im$ es inyectiva.

33.- Sean $s(x) = x^2$; $p(x) = 2^x$ y $t(x) = \text{sen } x$. Determinar los siguientes valores:
a) $(s \circ p)(y)$; b) $(s \circ t)(y)$; c) $(s \circ p \circ t)(u) + (t \circ p)(u)$; d) $t(u^3)$.

34.- Expresar cada una de las siguientes funciones en términos de s, p, t usando solamente:

$+$, $\cdot$ y $\circ$.

a) $f(x) = e^{\text{sen } x}$; b) $f(x) = \text{sen } 2^x$; c) $f(x) = \text{sen } x^2$; d) $f(x) = \text{sen}^2 x$;
e) $f(t) = 2^{2t}$; f) $f(u) = \text{sen } [2^u + (2^u)^2]$; g) $f(a) = 2^{\text{sen } a} + \text{sen}(a^2)$.

35.- Sean $f : \mathbf{R} \to \mathbf{R}$, con $f(x) = 2x - 3$ y $g : \mathbf{R} \to \mathbf{R}$, con $g(x) = x^3 + 5$.
a) Diga si f y g son biyectivas. b) Determine f^{-1} y g^{-1}. c) Halle: $g \circ f$; $f \circ g$; $g \circ g^{-1}$; $f \circ f^{-1}$

36.- De ejemplos de funciones reales que:
a) No sea inyectiva ni sobreyectiva. b) Sea inyectiva pero no sobreyectiva. c) Sea inyectiva y sobreyectiva. d) Sea sobreyectiva pero no inyectiva.

37.- Si f y g son aplicaciones biyectivas , probar que:

$(f : A \to B \text{ y } g : B \to C) \Rightarrow (gof)^{-1} == f^{-1} \text{ o } g^{-1}$.

38.- Dadas las funciones reales determinar la inversa:
a) $f(x) = x^2 - 5$; b) $f(x) = \sqrt[3]{x^3 + 1}$; c) $f(x) = \dfrac{3x - 5}{-x - 2}$; d) $f(x) = \ln(x + 2)$.

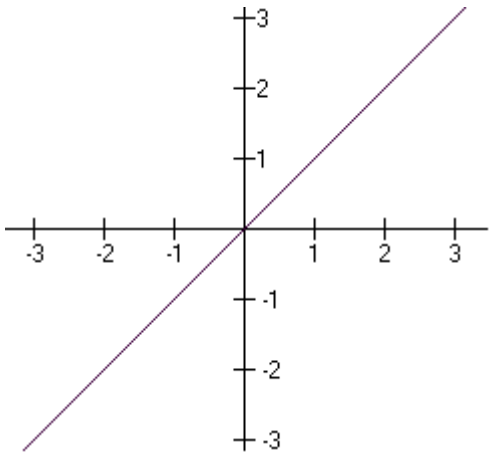
39.- Dadas las funciones, determinar las que la componen:

a) $f(x) = \text{sen}^3 \ln(3x + 2)^2$; b) $f(x) = e^{\text{sen}(2x + 5)}$; c) $f(x) = \sqrt[5]{\text{sen}^3(e^{3x^2 - 2})}$.

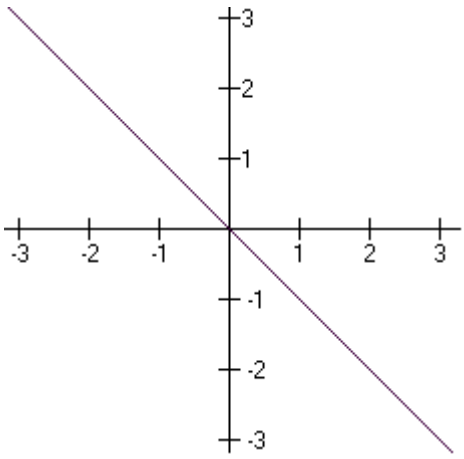
40.- Sea $f: E \to F$ una aplicación monótona.
1° Si f es inyectiva, probar que f es estrictamente monótona.
2° Si f es estrictamente monótona y E totalmente ordenado. probar que f es inyectiva.

Anexo B.-

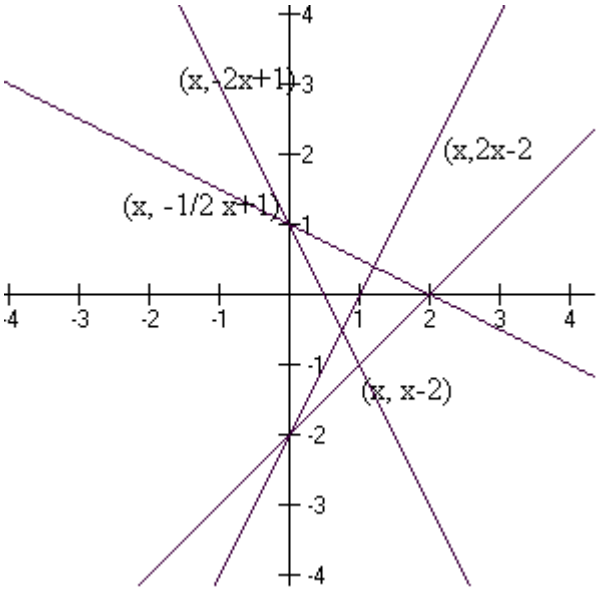
Es necesario, que el alumno empiece a reconocer a los gráficos de funciones reales elementales. Se representan aquí algunas de ellas.

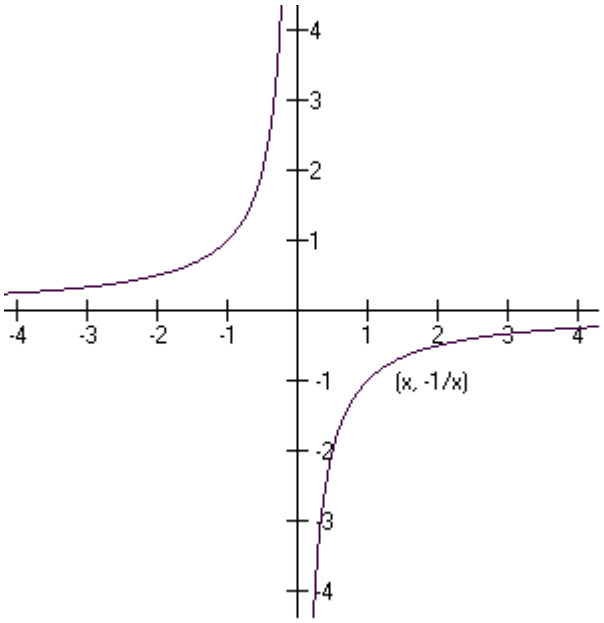


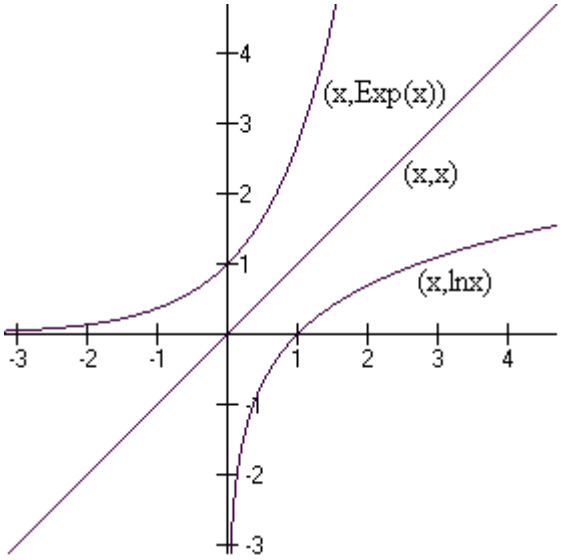
f(x) = x

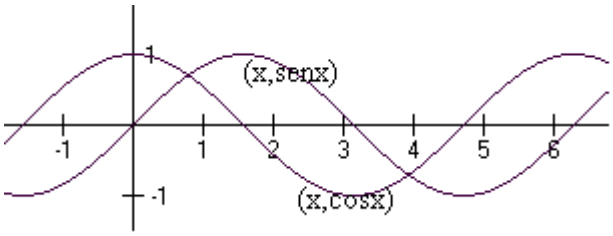


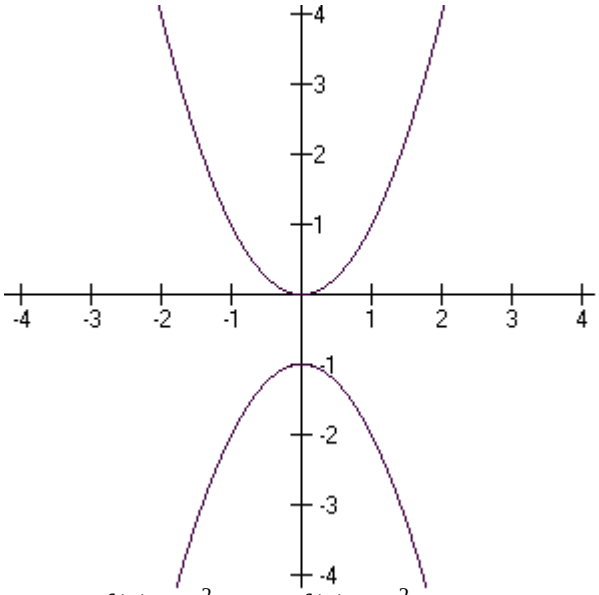
f(x) = -x



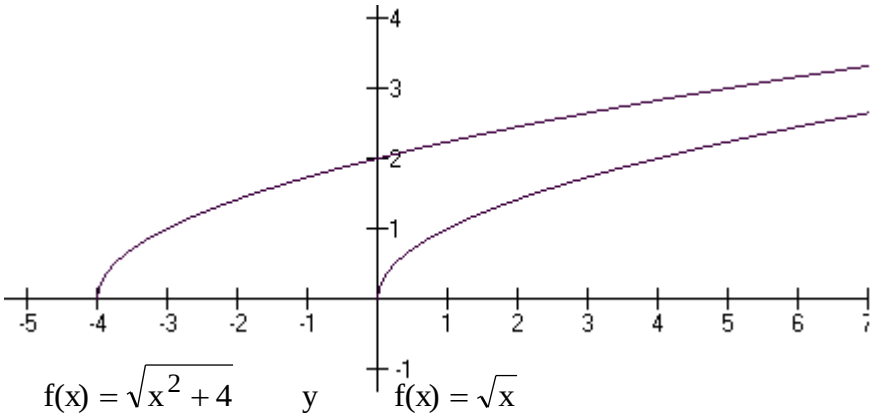




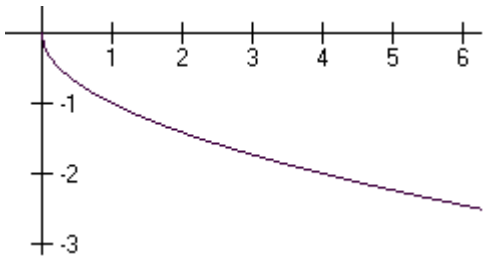




$f(x) = x^2$ y $f(x) = x^2 - 1$



$f(x) = \sqrt{x^2 + 4}$ y $f(x) = \sqrt{x}$



$f(x) = -\sqrt{x}$

Bibliografía

-Ayres, F.: Algebra Moderna.
-Doneddu, A.: Algebra y Geometría.
-Gentile, E.: Notas de Álgebra.
-Lentin-Rivaud: Álgebra Moderna
-Pecastaigns, F.: Chemins vers l'Algèbre
-Pinzón, A. Conjuntos y estructuras.
-Queysanne, M.: Algebra Básica.
-Taylor, H- Wade, T.: Matemáticas Básicas.

2.- Relaciones definidas en un conjunto.-

2.1.- Relaciones de equivalencia

Sea E un conjunto y consideremos una relación binaria $\mathfrak{R}$ sobre E. Esta relación puede presentar cualidades particulares que nos interesen. La relación de equivalencia que es la más natural que se puede definir en un conjunto, origina en éste una partición asociada, y nos permite clasificar a los elementos del conjunto.

2.1.1.- Reflexividad

Definición.

Se dice que una relación binaria $\mathfrak{R}$ sobre E es reflexiva si

$$(\forall x \in E) \qquad x \ \mathfrak{R} \ x.$$

En otros términos, $\mathfrak{R}$ es reflexiva si la diagonal de E^2 está incluída en el grafo de $\mathfrak{R}$.

Ejemplos.

1. La igualdad es reflexiva: $(\forall a \in E) \quad a = a$.

2. La inclusión en P(E) es reflexiva: $(\forall A \in P(E)) \quad A \subset A$.

3. En el conjunto de las rectas del plano euclidiano, la relación "D es perpendicular a D´ " (denotado $D \perp D'$) no es reflexiva. Una recta no es perpendicular a sí misma.

2.1.2.- Simetría

Definición.

Se dice que una relación binaria $\mathfrak{R}$ sobre E es simétrica si

$$x \ \mathfrak{R} \ y \ \Rightarrow \ y \ \mathfrak{R} \ x.$$

Ejemplos.

1. La igualdad es simétrica: $a = b \ \Rightarrow \ b = a$.

2. La relación $D \perp D'$ es simétrica: $D \perp D' \ \Rightarrow \ D' \perp D$.

3. La relación de inclusión no es simétrica: $A \subset B$ no implica, en general, $B \subset A$. Solo se puede cambiar A y B en el caso donde A = B.

2.1.3.- Antisimetría

Definición.

Se dice que una relación binaria $\mathcal{R}$ sobre E es antisimétrica si

$$(x \mathcal{R} y \quad e \quad y \mathcal{R} x) \Rightarrow x = y.$$

Ejemplos.

1. La relación de inclusión es antisimétrica:

2. La relación de divisibilidad en N es antisimétrica.

Recordemos que "a divide b" (denotado a/b) si existe un entero natural q tal que b = aq. Esta relación cumple la propiedad

$$(a/b \text{ y } b/a) \Rightarrow a = b.$$

2.1.4.- Transitividad

Definición.

Se dice que una relación binaria $\mathcal{R}$ sobre E es transitiva si

$$(x \mathcal{R} y \quad e \quad y \mathcal{R} z) \Rightarrow x \mathcal{R} z.$$

Ejemplos.

1. La inclusión es transitiva:

$$(A \subset B \text{ y } B \subset C) \Rightarrow A \subset C.$$

2. La relación $D \perp D'$ no es transitiva en el conjunto de las rectas del plano euclidiano.

En efecto $D \perp D'$ y $D' \perp D''$ implica $D \,//\, D''$ (D es paralela a D´´) y no puede ser $D \perp D''$.

2.2.- Relación de equivalencia

Definición.

Se dice que $\mathcal{R}$ es una relación de equivalencia sobre E si es a la vez reflexiva, simétrica y transitiva.

Por ejemplo, en el conjunto E de las rectas del plano euclidiano, se dice que D es paralela a D' (y se la denota $D//D'$) si $D \cap D' = \phi$ o $D = D'$. Esta relación es una equivalencia sobre E:

$$(\forall\, D \in E) \qquad D//D,$$

$$D//D' \quad \Rightarrow \quad D'//D.$$

$$(D//D' \text{ y } D'//D'') \quad \Rightarrow \quad D//D''.$$

Se va a clasificar a todas las rectas de E como sigue:

a) Dos rectas D y D' que estén relacionadas son de la misma clase.

b) Dos rectas D y D' que no estén relacionadas , son de clases distintas.

Todas las rectas, entonces quedan clasificadas; cada clase se denomina una "dirección". Una recta cualquiera de una clase puede ser elegida como la *representante de la dirección.*

Definición

Sea $\mathfrak{R}$ una relación de equivalencia sobre E. Para todo $a \in E$, se llama clase de equivalencia de a el sub-conjunto de E:

$$\mathcal{C}(a) = \{x \in E / x\, \mathfrak{R}\, a\}.$$

Se tiene entonces la siguiente equivalencia lógica:

$$a\, \mathfrak{R}\, b \quad \Leftrightarrow \quad \mathcal{C}(a) = \mathcal{C}(b).$$

a) Tomemos primero la implicación $\Rightarrow$. Sea $x \in \mathcal{C}(a)$. Entonces,

$$(x\, \mathfrak{R}\, a \text{ y } a\, \mathfrak{R}\, b) \Rightarrow x\, \mathfrak{R}\, b \Rightarrow x \in \mathcal{C}(b) \Rightarrow \mathcal{C}(a) \subset \mathcal{C}(b).$$

Por simetría, se ve a sí mismo que $\mathcal{C}(b) \subset \mathcal{C}(a)$.

b) *Recíprocamente,* por reflexividad, $a \in \mathcal{C}(a) = \mathcal{C}(b)$, de donde $a\, \mathfrak{R}\, b$.

Mostraremos ahora que la familia $(\mathcal{C}(a))_{a \in E}$ constituye una **partición** de E.

$(\forall a \in E) \qquad \mathcal{C}(a) \neq \Phi,$ pues $a \in \mathcal{C}(a)$, ya que $\mathfrak{R}$ es reflexiva.

$$\bigcup_{a \in E} \mathcal{C}(a) = E \quad \text{es evidente.}$$

$$\mathcal{C}(a) \neq \mathcal{C}(b) \quad \Rightarrow \quad \mathcal{C}(a) \cap \mathcal{C}(b) = \Phi.$$

En efecto, si se supone que existe un $x \in [\mathfrak{C}(a) \cap \mathfrak{C}(b)]$, entonces $x \,\Re\, a$ y $x \,\Re\, b$ implican $a \,\Re\, b$, de donde $\mathfrak{C}(a) = \mathfrak{C}(b)$, contrariando a la hipótesis.

Recíprocamente, sea E un conjunto y $(A_\lambda)_{\lambda \in L}$ una partición de E. Definimos una relación binaria sobre E de la siguiente manera:

$$a \,\Re\, b \;\Leftrightarrow\; (\exists \lambda \in L;\ a \in A_\lambda \ \text{ y } \ b \in A_\lambda).$$

• Se puede mostrar que $\Re$ es una relación de equivalencia sobre E.

1. Es reflexiva. En efecto,

$$(\forall a \in E) \qquad (\exists \lambda \in L) \qquad a \in A_\lambda \ .$$

2. Es simétrica de forma evidente.

3. Es transitiva. En efecto, sea $a \,\Re\, b$ y $b \,\Re\, c$. Entonces

$$(\exists\, \lambda \in L) \qquad a \in A_\lambda \qquad \text{y} \qquad b \in A_\lambda,$$

$$(\exists \lambda' \in L) \qquad b \in A_{\lambda'}, \qquad \text{y} \qquad c \in A_{\lambda'}.$$

Como $b \in A_\lambda \cap A_{\lambda'}$, entonces $A_\lambda \cap A_{\lambda'} \neq \Phi$, luego $A_\lambda = A_{\lambda'}$, y por consiguiente $a \,\Re\, c$.

Las clases de equivalencia son evidentemente los elementos A_λ de la familia propuesta; se ha demostrado el siguiente resultado:

Teorema 1.

A toda relación $\mathfrak{R}$ de equivalencia sobre un conjunto E le corresponde una partición de E en clases de equivalencia y recíprocamente, toda partición de E define sobre E una relación de equivalencia $\mathfrak{R}$ donde las clases coinciden con los elementos de la partición dada.

Definiciones.

1. El conjunto de las clases de equivalencia se denomina conjunto cociente de E por $\Re$ y se denota $E/\Re$.

2. La aplicación $g: E \to E/\mathfrak{R}$ que a todo elemento de E hace corresponder su clase $g(x) = \mathfrak{C}(x)$ se denomina aplicación canónica.

2.3.- Relaciones de orden

2.3.1.- Conjunto ordenado.

Definición.

Se llama relación de orden sobre un conjunto E a una relación binaria reflexiva, antisimétrica y transitiva.

$\mathcal{R}$ es una relación de oden sobre E si

1. $(\forall\, x \in E)$ $\quad x\ \mathfrak{R}\ x$ (reflexividad),

2. $(x\ \mathfrak{R} y \quad e \quad y\ \mathfrak{R}\ x)$ $\quad x = y$ (antisimetría),

3. $(x\ \mathfrak{R} y \quad e \quad y\ \mathfrak{R}\ z)$ $\quad x\ \mathfrak{R}\ z$ (transitividad).

Se dice entonces que E está *ordenado* por $\mathfrak{R}$

Ejemplos.

1. La igualdad sobre E $(x = y)$ es una relación de orden sobre E que se denomina orden trivial. En todo lo siguiente de este apunte, cuando se considere un conjunto ordenado, será admitido implícitamente que su orden no es el trivial. Un conjunto no trivialmente ordenado contiene al menos dos elementos.

2. La relación de inclusión en P(E) verifica

$$(A \subset B \quad y \quad B \subset A) \Leftrightarrow A = B,$$
$$(A \subset B \quad y \quad B \subset C) \Rightarrow A \subset C.$$

P(E) queda entonces ordenado por la relación de inclusión.

2.3.2.- Orden parcial. Orden total

En P(E) ordenado por $\subset$, dos partes cualesquiera A y B no están necesariamente incluídas una en la otra. Por ejemplo, es suficiente considerar dos partes A y B que verifiquen

$$(\exists a \in A) \quad a \notin B \quad y \quad (\exists\, b \in B) \quad b \notin A.$$

Las partes A y B así consideradas no son *comparables* por la relación de inclusión. Se dice que la inclusión es una relación de *orden parcial.*

La relación de orden natural en N se define como sigue:

$$a \leq b \quad (\exists\, x \in N, \ a + x = b).$$

Para todo par $(a, b) \in N^2$ se tiene, ya sea $a \leq b$, o $b \leq a$. Dos elementos cualesquiera son comparables, Se dice que la relación de orden es total.

Definición.

Una relación de orden $\mathcal{R}$ en E se dice relación de orden total si dos elementos cualesquieras son comparables:

$$\forall (x, y) \in E^2, \quad \text{se tiene} \quad x \mathcal{R} y \quad o \quad y \mathcal{R} x.$$

En el caso contrario, el orden es parcial.

El orden es parcial si existe al menos un par $(x, y) \in E^2$ de elementos no comparables.

Ejemplo.-

La relación de divisibilidad en N es una relación de orden parcial. En efecto, primero, es una relación de orden pues

$$(a / b \quad y \quad b / a) \quad \Leftrightarrow \quad a = b,$$
$$(a / b \quad y \quad b / c) \quad \Rightarrow \quad a / c.$$

Por último, este orden es parcial, pues dos enteros cualesquieras no son necesariamente comparables. Por ejemplo.

$$5 \ \# 12 \qquad y \qquad 12 \ \# \ 5.$$

2.3.3.- Relación de orden estricto

Definición.

Una relación binaria $\mathcal{R}$ sobre un conjunto E se dice relación de orden estricto si

1. *Es transitiva:*
   $$(x \ \mathcal{R} \ y \quad e \quad y \mathcal{R} \ z) \ \Rightarrow \ x \mathcal{R} \ z;$$
2. *Se verifica:*
   $$x \mathcal{R} \ y \ \Rightarrow \ x \neq y.$$

El conjunto E se dice entonces *estrictamente ordenado* por $\Re$.

Ejemplo.

1. La relación natural de orden estricto en N se define como sigue:

$$a < b \ \Leftrightarrow \ (\exists x \in N^*; \ a + x = b),$$

es una relación de *orden estricto total*.

2. La inclusión estricta en $P(E)$ se define por

$$A \mathfrak{R} B \Leftrightarrow (A \subset B \text{ y } A \neq B),$$

Es una relación de *orden estricto parcial.*

P_4 *Si $\mathfrak{R}$ es una relación de orden estricto sobre un conjunto E, entonces $x \mathfrak{R} y$ e $y \mathfrak{R} x$ jamás son simultáneamente verdaderas.*

En efecto, si suponemos que son simultáneamente verdaderas, esto nos conducirá a una contradicción. Por transitividad, $x \mathfrak{R} y$ e $y \mathfrak{R} x$ implica $x \mathfrak{R} x$, de donde $x \neq x$ (contradicción).

Teorema.

Sea E un conjunto ordenado en forma no trivial por una relación, denotada $\leq$. Entonces la relación binaria $\mathfrak{R}$ sobre E definida por

$$x \mathfrak{R} y \Leftrightarrow (x \leq y \text{ e } x \neq y)$$

es un orden estricto sobre E.

En efecto, se tiene a todas luces y en primer lugar

$$x \mathfrak{R} y \Rightarrow x \neq y.$$

Además, $\mathfrak{R}$ es transitiva pues:

$$(x \mathfrak{R} y \text{ e } y \mathfrak{R} z) \Rightarrow (x \leq y \leq z \text{ e } x \neq y \text{ e } y \neq z).$$

No puede ser $x = z$, porque sinó $x \leq y \leq x$ implicaría $x = y$ (contradicción).

Se dice que $\mathfrak{R}$ es el *orden estricto deducido* de $\leq$ y se la denota $<$.

Teorema.

Sea E un conjunto estrictamente ordenado por una relación, denotada $<$. Entonces la relación binaria $\mathfrak{R}$ sobre E definida por

$$x \mathfrak{R} y \Leftrightarrow (x < y \text{ o } x = y)$$

es un orden (no trivial) sobre E.

En efecto, $\mathfrak{R}$ es a todas luces evidentemente reflexiva. Es también antisimétrica pues las dos condiciones en forma simultánea s $(x < y \text{ o } x = y)$ e $(y < x \text{ o } y = x)$ exigen que $x = y$.

Por último $\Re$ es transitiva pues,

$(x < y \text{ o } x = y)$ e $(y < z \text{ o } y = z)$ implican $x < z$ o $x = y = z$.

Se dice que $\Re$ es el orden (no trivial) deducido de $<$ y se le denota $\leq$.

2.3.4.- Intervalos

Sea E un conjunto ordenado por una relación, denotada $\leq$. La relación de orden estricto que se deduce de ella será denotada $<$. Sea $a \leq b$.

Se denomina *intervalo cerrado* de origen a y de extremo b, al conjunto de los elementos x de E tales que $a \leq x \leq b$. Se denota

$$[a, b] = \{x \in E / a \leq x \leq b\}.$$

Sea $a < b$. El *intervalo abierto* de origen a y de extremo b se define como sigue:

$$]a, b[= \{x \in E / a < x < b\}.$$

El *intervalo semi-abierto a derecha* se define y denota como sigue

$$[a, b[= \{x \in E / a \leq x < b\}$$

y por último el intervalo *semi-abierto a izquierda*

$$]a, b] = \{x \in E / a < x \leq b\}.$$

2.3.5.- Mayorantes. Minorantes. (Cotas superiores Cotas inferiores).

Sea $(E, \leq)$ un conjunto ordenado y A una parte no vacía de E. Las relaciones $x \leq y$ e $y \geq x$ son sinónimos.

Definiciones.

1. Si existe $a \in E$ tal que:

$$(\forall x \in A) \qquad x \leq a,$$

se dice entonces que a es una cota superior o mayorante de A

2. Si existe $b \in E$ tal que:

$$(\forall x \in A) \qquad b \leq x,$$

se dice que b es una cota inferior o minorante de A.

Ejemplo.-

Sea el conjunto N ordenado por la relación de divisibilidad. Consideremos la parte A={a, b} constituida de dos números naturales. Por la relación x/y, todo *múltiplo común* de a y de b es una cota superior de A y toda cota superior de A es un múltiplo común de a y b.

Asimismo, el conjunto de las cotas inferiores de A coinciden, con el conjunto de los divisores comunes de a y b

.

Se debe notar que, para una parte cualquiera A de un conjunto ordenado, la existencia de cota superior no está necesariamente asegurada. Cuando existe una cota superior, se dice que A está *mayorada* o *acotado superiormente*. Cuando existe una cota inferior de A, se dice que A está *minorado* o *acotado inferiormente*. Si A está a la vez mayorado y minorado, se dice que A está *acotado.*

2.3.6.- Elemento máximo. Elemento mínimo.

Definiciones.

Sea $(E, \leq)$ un conjunto ordenado y A una parte no vacía de E.

1. Si existe una cota superior a de A que verifique: $a \in A$, se dice que a es elemento máximo de A. Se le denota a = máx A.

2. Si existe un minorante b de A que verifique: $b \in A$, se dice que b es elemento mínimo de A. Se le denota b = mín A.

Si el elemento máximo a existe, es único. Pues, si existiera otro a', se tendría

$$a' \geq a \quad \text{dado que } a' \text{ mayora } A \text{ y que } a \in A,$$
$$a \geq a' \quad \text{dado que } a \text{ mayora } A \text{ y que } a' \in A,$$

luego

$$a = a'.$$

Así mismo, si el elemento mínimo existe, el es único.

Ejemplos.

1. Para la relación de divisibilidad en N, la parte A = {a, b} admite un elemento máximo (y un elemento mínimo) si , y solamente si, a/b. Se tiene entonces que mín A = a y máx A = b.

2. Para la relación de orden natural $\leq$ en N, se tienen las siguientes propiedades que conviene recordar:

a) toda parte no vacía de N admite un elemento mínimo:

$(\forall A \subset N;\ A \neq \Phi\ ) \Rightarrow$ *mín A existe;*

b) toda parte no vacía y mayorada de N admite un elemento máximo:

$(\forall A \subset N;\ A \neq \Phi;$ *A mayorado)* $\Rightarrow$ *máx A existe.*

2.3.7.- Supremo. Infimo.

Sea $(E, \leq)$ un conjunto ordenado y A una parte no vacía de E.

Definiciones.

1. Si el conjunto M de las cotas superiores de A no es vacío y admite un elemento mínimo, este elemento se denomina supremo de A, y se denota

$$\sup A \quad (\sup A = \min M).$$

2. En el conjunto N de las cotas inferiores de A no es vacío y admite un elemento máximo, este elemento se denomina ínfimo de A, y se denota

$$\inf A \quad (\inf A = \max N).$$

Cuando el sup A y el inf A existen son únicos.

Cuando una cota superior de A pertenece a A, es a la vez máx A y sup A. Así mismo, una cota inferior de A que pertenece a A es a la vez min A e inf A.

Ejemplos.

1. Sea **N** ordenado por la relación de divisibilidad y A = {a,b} una parte de **N** constituida de dos elementos.

El conjunto M de los mayorantes de A es el conjunto de los múltiplos comunes al elemento "a" y al "b". Este conjunto M admite un elemento mínimo que es el común múltiplo de a y de b más chico. Luego

$$\sup \{a, b\} = \text{m.c.m. } (a, b).$$

El conjunto N de los minorantes de A es el conjunto de los divisores comunes de a y de b. Este conjunto N admite un elemento máximo, el común divisor más grande de a y de b, luego

$$\inf \{a,b\} = \text{M.C.D. } (a,b)$$

2.- Sea P(E) ordenado por la relación de inclusión y {A, B} una parte de P(E) constituída de dos elementos. El conjunto M de los mayorantes de {A, B} se define como sigue:

$$M = \{X \in P(E) / X \supset A \text{ y } X \supset B\}.$$

O sea, se tiene a la vez

$$(X \supset A \text{ y } X \supset B) \Rightarrow X \supset (A \cup B),$$

$$(A \cup B) \supset A \quad \text{y} \quad (A \cup B) \supset B.$$

En consecuencia, $A \cup B$ es el mayorante más pequeño de $\{A, B\}$, luego

$$\sup \{A, B\} = A \cup B.$$

Se puede ver de la misma manera que todo minorante de $\{A, B\}$, está incluído a la vez en A y en B, es decir está incluído en $A \cap B$ que es así mismo un minorante de $\{A, B\}$; luego

$$\inf \{A, B\} = A \cap B.$$

2.4.- Leyes de composición.

2.4.1.- Magma.

Definiciones.

Se llama ley de composición interna sobre un conjunto E toda aplicación de ExE en E.

A todo par ordenado $(a, b) \in E^2$, se le asocia un único elemento c en E: "a" se llama el *primer término*, "b" el *segundo término* y c el *resultado* o la *compuesta* de a y b.

Notaciones.

La notación aditiva, se escribe

$a + b = c$ (y se lee "a más b es igual c").

La notación multiplicativa, se escribe

$a \cdot b = c$ (y se lee "a por b es igual c").

Existen otras notaciones. Por ejemplo,

$a \, T \, b = c$ (a *truco* b es igual c);
$a \perp b = c$ (a *antitruco* b es igual c);
$a * b = c$ (a *asterisco* b es igual c).

Definición.

Un conjunto E munido de una ley de composición interna se denomina magma.

Ejemplos.

1.-La adición o la multiplicación en **N.**

2.-Sea E un conjunto cualquiera. El *primer proyector* $E^2 \to E$, es una ley de composición interna sobre E: a * b = a.

3.-La intersección y la unión son dos leyes de composición internas en P(E).

Si E es un conjunto finito, se puede dibujar la *tabla* de la ley de composición. Por ejemplo, sea E = {*a, b, c, d*} y la ley $\perp$ se define sobre el conjunto E por la siguiente tabla:

1er término \ 2do término	*a*	*b*	*c*	*d*
a	*d*	*d*	*a*	*b*
b	*a*	*b*	*b*	*a*
c	*c*	*c*	*c*	*d*
d	*d*	*a*	*b*	*c*

Se lee la compuesta $x \perp y$ en el caso de coordenadas x, y; con x 1er término e y 2do término. Así, por ejemplo:

$$b \perp d = a.$$

Para definir un magma, es suficiente reemplazar los casilleros arbitrariamente por elementos de E.

2.4.2.- Propiedades.

Sea (E, T) un magma. Esta ley de composición puede presentar ciertas cualidades, las mismas se estudian a continuación.

1° Asociatividad.

Definición.

Sea (E, T) un magma. La ley T se dice asociativa si

$$(\forall\ a, b, c \in E) \qquad (a\ T\ b)\ T\ c = a\ T\ (b\ T\ c).$$

se dice entonces que el magma es asociativo.

Ejemplos.

1. La adición y la multiplicación en **N** o **Z** son asociativas.
2. La unión y la intersección en P(E) son asociativas.
3. El primer proyector sobre E es asociativo:

$$(a * b) * c = a * (b * c)$$

$$a * c = a * b$$
$$a = a.$$

2° Conmutatividad.

Definición.

Sea (E, T) un magma. La ley T se dice conmutativa si

$$\forall (a, b \in E) \qquad a\ T\ b = b\ T\ a.$$

Se dice entonces que el magma es conmutativo.

Ejemplos.

1. La adición y la multiplicación en **N** son conmutativas.
2. La unión y la intersección en P(E) son conmutativas.
3. El primer proyector sobre E no es conmutativo. En efecto,

$$a * b = a \quad y \quad b * a = b.$$

Los resultados son diferentes si $a \neq b$.

3° Elemento neutro.

Definición.

Sea (E, T) un magma. Se dice que un elemento $e \in E$ es neutro para la ley T si, cualquiera que sea $a \in E$,

$$a\ T\ e = e\ T\ a = a.$$

Se dice entonces que el magma tiene elemento neutro.

OBSERVACIÓN.- Si la ley T es conmutativa, la primer igualdad siempre es verdadera.

P_1 *Si el elemento neutro existe, es único.*

En efecto, si se supone que el magma (E, T) tiene dos elementos neutros e y e'. Entonces, considerando que e es el elemento neutro y $e' \in E$, se tiene:

$$e'\ T\ e = e\ T\ e' = e'. \quad (1)$$

Y ahora que e' es elemento neutro y que $e \in E$, entonces será:

$$e\ T\ e' = e'\ T\ e = e; \quad (2)$$

luego de (1) y de (2) se deduce que e = e' y el elemento neutro es único.

Ejemplos.

1.-La adición en **N** posee el elemento neutro 0. La multiplicación a el elemento neutro 1.

2.-El primer proyector sobre E : a * b = a no tiene elemento neutro.

3.-La unión en P(E) a el elemento neutro $\varnothing$:

$$(\forall A \in P(E)) \qquad A \cup \varnothing = A.$$

4.-La intersección en P(E) tiene elemento neutro E:

$$(\forall A \in P(E)) \qquad A \cap E = A.$$

4° Elementos simplificables.

Definiciones.

Sea (E, T) un magma.

1. Se dice que un elemento $a \in E$ es simplificable a izquierda si

$$(\forall b, c \in E) \qquad a\ T\ b = a\ T\ c \Rightarrow b = c.$$

2. Se dice que "a" es simplificable a derecha si

$$(\forall b, c \in E) \qquad b\ T\ a = c\ T\ a \Rightarrow b = c.$$

Si "a" es simplificable a derecha y a izquierda se dice que es simplificable..

Para una ley conmutativa, un elemento simplificable de un lado es simplificable.

Ejemplos.

1. Todo número natural es simplificable para la adición:

$$(\forall x \in \mathbf{N}) \qquad a + x = b + x \Rightarrow a = b.$$

2. Todo número natural, salvo 0, es simplificable para la multiplicación:

$$(\forall x \in \mathbf{N}, x \neq 0) \qquad ax = bx \Rightarrow a = b.$$

3. Para el primer proyector, todo elemento es simplificable a derecha:

$$a * c = b * c \Rightarrow a = b.$$

Pero ningún elemento es simplificable a izquierda, pues

$$a * b = a * c$$ cualesquiera que sean a, b y c.

4. En P(E) ningún elemento, salvo E, es simplificable para la intersección y ningún elemento salvo ∅, es simplificable para la unión.

Si el magma es unífero, el elemento neutro es evidentemente simplificable.

5° Elementos simétricos.

Definiciones.

Sea (E, T, e) un magma unífero.

1. Se dice que un elemento $a \in E$ es simetrizable a derecha, si existe un elemento a' de E tal que a T a' = e.

Se dice que "a' " es simétrico a la derecha de "a".

2. $a \in E$ es simetrizable a izquierda si existe $a' \in E$ tal que a' T a = e. Se dice que a' es simétrico a la izquierda de a.

Para una ley conmutativa, un elemento simetrizable de un lado es simetrizable.

Si a' es simétrico de a de un lado, entonces a es simétrico de a' de el otro lado.

El elemento neutro es también simetrizable. El es el simétrico de sí mismo.

Ejemplos.

1. En **N,** ningún elemento, salvo 0, es simetrizable para la adición.

El problema de la simetrización de la adición en **N** conduce a la construcción de el conjunto **Z** de los enteros relativos.

2. En **N**, ningún elemento, salvo 1, es simetrizable para la multiplicación.

3. Para la unión o la intersección en P(E), ningún elemento, salvo el elemento neutro, es simetrizable.

-Para la unión, si se da $A \neq \emptyset$, no existe $B \in P(E)$ tal que

$$A \cup B = \emptyset .$$

-Para la intersección, si se da $A \neq E$, no existe B tal que

$$A \cap B = E.$$

6° Sub-magma de un magma.

Definición.

Sea (E, T) una magma y F una parte no vacía de E. Se dice que F es sub-magma de E si la restricción a FxF de la ley de composición de E es una aplicación en F.

En otros términos, F es sub-magma de E si

$$(a \in F \text{ y } b \in F) \Rightarrow aTb \in F.$$

2.4.3.- Monoide.

Definición.

Se llama monoide un magma unífero asociativo.

Si la ley es conmutativa, el monoide se dice conmutativo.

Ejemplos.

1. **N** es un monoide conmutativo para la adición y también lo es para la multiplicación.
2. P(E) es un monoide conmutativo para la unión y también para la intersección.
3. Sea E un conjunto. Designemos por $\mathbb{F}(E)$ el conjunto de las aplicaciones de E en E. La ley de composición de aplicaciones es una ley interna en $\mathbb{F}(E)$. Es asociativa. Admite por elemento neutro a I_E, la coincidencia sobre E. En consecuencia , $(\mathbb{F}(E), o, I_E)$ es un monoide. No es conmutativa cuando $\text{card}E \geq 2$.

P_2 *En un monoide, todo elemento simetrizable es simplificable.*

Sea (E, T, e) un monoide y a un elemento simetrizable de E. Existe entonces $a' \in E$ tal que

$$aTa' = a'Ta = e.$$

Se demuestra que, cualquiera que sean b y c en E,

$$bTa = cTa \Rightarrow b = c.$$

En efecto, operando por derecha miembro a miembro por a',

$$(bTa)Ta' = (cTa)Ta'.$$

Por asociatividad,

$$bT(aTa') = cT(aTa'),$$

queda

$$bTe = cTe, \text{ entonces } b = c.$$

P_3 *En un monoide, todo elemento simetrizable admite un simétrico único.*

Se supone que el elemento a tiene dos simétricos a' y a" en el monoide (E, T, e). Luego

$$a'Ta = a"Ta = e$$

y como a es simplificable, se obtiene:

$$a' = a".$$

OBSERVACIÓN.- En un monoide donde la ley es denotada aditivamente el simétrico de un elemento a se denomina el *opuesto* de a y se denota -a. Si la notación es multiplicativa, se denomina el *inverso* de a y se denota a^{-1}.

P_4 Sea M un monoide denotado multiplicativamente. Para todo par ordenado (a, b) de elementos inversibles de M, el compuesto ab es inversible y

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

En efecto

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e.$$

Así mismo,

$$(b^{-1}a^{-1})(ab) = e, \quad \text{y esto demuestra la propiedad.}$$

2.4.3.1.- Sub-monoide de un monoide

Definición.

Sea M un monoide y A una parte no vacía de M. Se dice que A es sub-monoide de M, si A es un sub-magma del magma M y si este sub-magma A es así mismo un monoide.

Todo sub-magma A del monoide M es evidentemente asociativo. Es suficiente entonces que el sub-magma A posea un elemento neutro para que el sea sub-monoide de M.

Hay que prestar atención a lo que sigue: El elemento neutro de un sub-monoide A puede ser distinto del elemento neutro del monoide M como se muestra en el siguiente ejemplo, del monoide $M=\{e,\omega,a,b\}$ de elemento neutro e y con un sub-monoide $A = \{\omega,a,b\}$ de elemento neutro ω:

	e	ω	a	b
e	e	ω	a	b
ω	ω	ω	a	b
a	a	a	b	ω
b	b	b	ω	a

Se tiene la siguiente propiedad:

P_5 *Si en un monoide M todo elemento es simplificable, todo sub-monoide de M tiene el mismo elemento neutro que M.*

En efecto sea e el elemento neutro de M y ω el elemento neutro de un sub-monoide cualquiera A de M. Entonces para todo $a \in A$

$$a\omega = ae = a \qquad \text{implica por simplificación} \qquad \omega = e.$$

2.5.- Morfismos

Definición.

Sean (E, T) y (F, #) dos magmas. Se llama morfismo de E en F, para las leyes T y #, toda aplicación f: E $\rightarrow$ F tal que

$$(\forall\, a, b \in E) \qquad f(aTb) = f(a) \# f(b).$$

Ejemplos.

1. Sea (E, #) un magma , se define en E^2 la ley T por

$$(a, b)\ T\ (a', b') = (a\#a', b\#b').$$

El primer proyector f: $E^2 \rightarrow E$ es un morfismo del magma (E^2, T) en el magma (E, #). En efecto, para todo (a, b) y (a', b') en E^2,

$$f[(a, b)T(a', b')] = f(a\#a', b\#b') = a\#a' = f(a, b) \# f(a', b').$$

2. La aplicación f(X) = E - X de P(E) en sí mismo es un morfismo del monoide $(P(E), \cup)$ en el monoide $(P(E), \cap)$. En efecto, para toda parte X e Y de E,

$$f(X \cup Y) = E - (X \cup Y) = (E - X) \cap (E - Y) = f(X) \cap f(Y).$$

Definición.

Un morfismo biyectivo se denomina isomorfismo.

En los ejemplos precedentes, el primer morfismo no es biyectivo. (Es simplemente sobreyectiva). Por consiguiente no es un isomorfismo.

El segundo morfismo es biyectivo: $f(X) = E - X$ es un isomorfismo del monoide $(P(E), \cup)$ sobre el monoide $(P(E), \cap)$. Es involutivo.

Caso en el que E y F coinciden, como así también las leyes T y #.

Sea (E, T) un magma y f una aplicación de E en si mismo. Si f es un morfismo del magma (E, T) en sí mismo, toma el nombre particular de ***endomorfismo*.** Si, además, es biyectiva, toma el nombre particular de ***automorfismo*.**

Ejemplos.

1. Para todo a dado en **N** la aplicación $f(x) = ax$ es un endomorfismo del monoide (**N**, +).

2. El isomorfismo $f(X) = E - X$ de $(P(E), \cup)$ sobre $(P(E), \cap)$ no es un automorfismo pues las leyes no son coincidentes.

3. Sea E un monoide donde la ley es denotada multiplicativamente y al elemento neutro se lo denota con e. Para todo elemento inversible a de E (de inverso denotado a^{-1}), la aplicación $f(x) = axa^{-1}$ de E en si mismo es un automorfismo del monoide. En efecto, es un morfismo pues, para todo x e y de E,

$$f(x)f(y) = (axa^{-1})(aya^{-1}) = ax(a^{-1}a)ya^{-1} = a(xy)a^{-1} = f(xy),$$

dado que la ley es asociativa y que $a^{-1}a = e$.

Además, f es biyectiva. En efecto, es sobreyectiva pues, para todo $y \in E$, existe $x = a^{-1}ya$ en E tal que $f(x) = y$.

Y por último es inyectiva pues

$$axa^{-1} = ax'a^{-1} \Rightarrow x = x',$$

ya que todo elemento inversible es simplificable.

Tal automorfismo se denomina *automorfismo interior (inducido por a)* del monoide E.

2.5.1.- Compatibilidad.

Definición

Sean E y F dos conjuntos y se consideran dos relaciones binarias, una $\mathcal{R}$ sobre E, la otra $\mathcal{R}'$ sobre F. Una aplicación $f: E \to F$ se dice compatible con $\mathcal{R}$ y $\mathcal{R}'$ si

$$(\forall a,b \in E) \qquad a \mathcal{R} b \quad \Rightarrow \quad f(a) \mathcal{R}' f(b).$$

Ejemplo.-

Sean E y F dos conjuntos ordenados por las relaciones denotadas, las dos relaciones por la relación de orden $\leq$. Por definición una aplicación f de E en F se dice *creciente* si

$$a \leq b \quad \Rightarrow \quad f(a) \leq f(b).$$

La aplicación creciente es compatible con las dos relaciones de orden.

Definición.

Sea (E, T) un magma y se considera una relación binaria $\mathcal{R}$ sobre E. Se dice que la ley T es compatible con $\mathcal{R}$ si, para todos a, b, a', b' de E:

$$(a \mathcal{R} a' \text{ y } b \mathcal{R} b') \Rightarrow (a\, T\, b)\, \mathcal{R}\, (a'\, T\, b').$$

Ejemplos.

1. Sea el monoide aditivo (**N**,+) con la relación de orden natural. Entonces, para todos a, b, a' y b' en **N**,

$$(a \leq a' \text{ y } b \leq b') \Rightarrow (a + b \leq a' + b').$$

La adición en **N** es compatible con el orden natural.

2. En el mismo monoide anterior, se considera la relación de divisibilidad. Entonces existen a, b, a', b' en **N** que verifican

$$a \mid a', \quad b \mid b' \quad \text{y} \quad (a + b) \perp (a' + b');$$

por ejemplo, 2 divide a 6, 5 divide a 10 pero 7 no divide a 16.

La adición no es compatible con la relación de divisibilidad.

3. Por lo contrario, si se toma el monoide multiplicativo (**N**, ·) la multiplicación es compatible con la relación de divisibilidad:

$$(a \mid a' \text{ y } b \mid b') \Rightarrow ab \mid a'b'.$$

*Compatibilidad de una ley con una relación de equivalencia***.**

Sea E un conjunto y se considera una relación de equivalencia $\mathfrak{R}$ sobre E. Se denotará $a \equiv a' \pmod{\mathfrak{R}}$ en lugar de $a\, \mathfrak{R}\, a'$.

Sea (E, T) un magma donde la ley T es compatible con la relación de equivalencia $\mathfrak{R}$. Entonces, para todos a, b, a', b' de E se tiene

$$(a \equiv a' \text{ y } b \equiv b' \bmod(\mathfrak{R})) \Rightarrow a\, T\, b \equiv a'\, T\, b' \pmod{\mathfrak{R}}.$$

Sea $E / \mathfrak{R}$ el conjunto -cociente de E por la relación de equivalencia $\mathfrak{R}$, la clase de a se denotará $\bar{a}$ Se muestra que la correspondencia de $(E / \mathfrak{R})^2$ en $(E / \mathfrak{R})$:

$$(\bar{a},\bar{b}) \mapsto \overline{aTb}$$

es una aplicación. En efecto, si a' y b' son dos representantes cualesquiera de la clases $\bar{a},\bar{b},$ se tiene

$$(a \equiv a' \quad y \quad b \equiv b' \ (\mathrm{mod}\ \Re)) \Rightarrow \overline{aTb} = \overline{a'Tb'}.$$

La imagen de $(\bar{a},\ \bar{b})$ no depende de los representantes elegidos de las clases $\bar{a}, y, \bar{b}$. La correspondencia entonces, es una aplicación de $(E / \Re)^2$ en $E / \Re$.

Esta aplicación es una ley de composición en el conjunto cociente $E / \Re$, Para toda clase $\bar{a}$ y $\bar{b}$ de $E / \Re$ se tiene

$$(1) \qquad \bar{a}\ \bar{T}\ \bar{b} = \overline{aTb}\ ;$$

Se lee; "clase de a operado clase de b es igual clase de (a T b)".

Esta ley $\bar{T}$ en $E/ \Re$ se denomina <u>*ley-cociente de T por la relación de equivalencia $\mathcal{R}$.*</u>

La aplicación canónica g(a) = clase del elemento a de E sobre $E / \Re$ es un <u>*morfismo sobreyectivo*</u> del magma (E, T) sobre el magma $(E / \Re, \bar{T})$. La relación (1) dice que, para todo elemento a y b de E:

$$g(a)\,\bar{T}\,g(b) = g(aTb).$$

Se obtiene el siguiente resultado:

<u>Teorema 1</u>

Sea (E, T) un magma. Para toda relación de equivalencia $\mathcal{R}$ sobre E, compatible con la ley T, la relación

$$(\forall \bar{a},\bar{b} \in E / \Re \qquad \bar{a}\ \bar{T}\ \bar{b} = \overline{aTb}$$

Define una ley de composición $\bar{T}$ en $E /\mathcal{R}$, denominada <u>ley-cociente.</u>

Además la aplicación canónica es un morfismo sobreyectivo del maga (E, T) sobre el magma $(E / \Re, \bar{T})$, *que se denomina <u>magma cociente.</u>*

Si el magma (E,T), es unífero, de elemento neutro e, entonces el magma-cociente es también, de elemento neutro clase de e.

En efecto

$$(\forall \bar{a} \in \mathrm{E} / \mathfrak{R}) \qquad \begin{array}{l} \bar{a}\,\bar{T}\,\bar{e} = \overline{aTe} = \bar{a}, \\ \bar{e}\,\bar{\mathrm{T}}\,\bar{a} = \overline{eTa} = \bar{a}. \end{array}$$

Si el magma (E, T) es asociativo, el magma cociente lo es también. En efecto, para todos $\bar{a}, \bar{b}\ y\ \bar{c}$ de E / $\mathfrak{R}$,

$$\bar{a}\,\bar{\mathrm{T}}\,(\bar{b}\,\bar{\mathrm{T}}\,\bar{\mathrm{c}}) \;=\; \overline{a\,T\,(b\,T\,c)} = \overline{(a\,T\,b)\,T\,c} \;=\; (\bar{a}\,\bar{\mathrm{T}}\,\bar{b})\,\bar{\mathrm{T}}\,\bar{c}.$$

Si el magma (E, T) es conmutativo, el magma cociente lo es también.
En efecto, para todos $\bar{a}, \bar{b}$ de E / $\mathfrak{R}$:

$$\bar{a}\,\bar{\mathrm{T}}\,\bar{b} \;=\; \overline{a\ T\ b} \;=\; \overline{b\,T\,a} \;=\; (\bar{b}\,\bar{\mathrm{T}}\,\bar{a})$$

El resultado particular es que el magma-cociente de un monoide es también un monoide, que se le denomina *monoide cociente*

A todo elemento a admitiendo el simétrico a' en el monoide (E, T) le corresponde un elemento $\bar{a}$ admitiendo el simétrico $\bar{a}'$ en el monoide-cociente pues

$$a\,T\,a' = a'\,T\,a \;=\; e \quad \Rightarrow \quad \bar{a}\ \bar{\mathrm{T}}\ \bar{a}' \;=\; \bar{a}'\ \bar{T}\ \bar{a}' = \bar{e}.$$

ANEXO 1.-

1.- Descomposición canónica de una aplicación

Sea $f : \mathrm{E} \to \mathrm{F}$ una aplicación. La relación binaria $\mathfrak{R}$ sobre E definida

$$\mathrm{x}\ \mathfrak{R}\ \mathrm{x}' \;\Leftrightarrow\; f(\mathrm{x}) = f(\mathrm{x}')$$

es evidentemente una relación de equivalencia (*figura 1).*

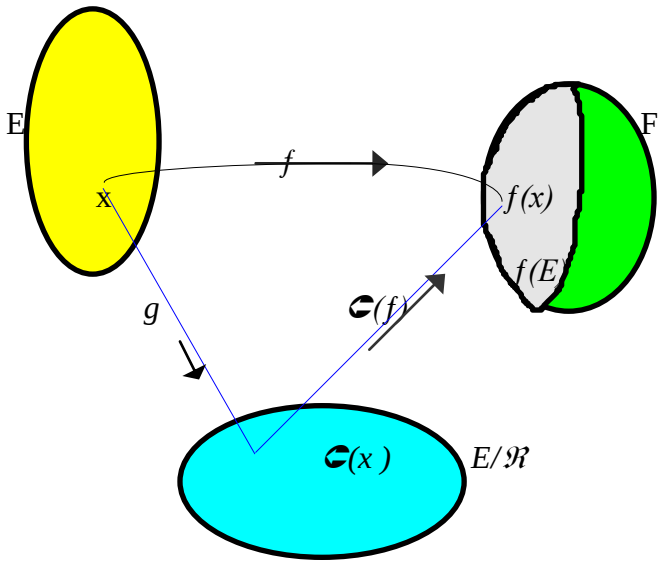


Figura 1.

Sea g: E → E/ℜ la aplicación canónica. (Se denota g(x) = ⊂(x) la clase de x ∈E.). Se muestra que la correspondencia ⊂(x) → f(x) de E/ℜ en *f*(E) es una aplicación. En efecto,

$$\subset(x) = \subset(x') \Rightarrow x \,\Re\, x' \Rightarrow f(x) = f(x')$$

(la imagen *f*(x) no depende del representante de la clase ⊂(x)).

Sea ⊂(f) : E/ ℜ → f(E), esta aplicación

$$[\forall \subset(x) \in E/\Re] \qquad \subset(f)[\subset(x)] = f(x).$$

Es evidentemente una sobreyección, y es también una inyección, pues

$$\subset(f)[\subset(x)] = \subset(f)[\subset(x')] \Rightarrow f(x) = f(x') \Rightarrow x \,\Re\, x' \Rightarrow \subset(x)=\subset(x').$$

⊂(f) es entonces una biyección de E/ℜ sobre f(E).

Sea j: f(E) → F la restricción a f(E) de la coincidencia sobre F. (Se la denomina *inyección canónica de la aplicación)* Se tiene entonces el esquema siguiente*:*

$$E \rightarrow E/\Re \rightarrow f(E) \rightarrow F \qquad \text{y}$$

$$f = j \circ \subset(f) \circ g.$$

Esta aplicación $\subset(f)$ es única, pues esta relación muestra que necesariamente $\subset[\subset(x)] = f(x)$. Se obtiene así la *descomposición canónica* de la aplicación $f : E \to F$.

Teorema.

Para toda aplicación $f: E \to F$ *la relación binaria* $\mathcal{R}$ *sobre* E*:*

$$x \ \mathcal{R} \ x' \quad \textit{si, y solamente sí,} \quad f(x) = f(x')$$

es una relación de equivalencia.

Si $g: E \to E/\mathcal{R}$ *es la aplicación canónica y* $j: f(E) \to F$ *la inyección canónica, entonces existe una aplicación, y una sóla,* $\subset(f) : E/ \to f(E)$ *que es biyectiva y verifica:*

$$f = j \ o \ \subset(f) \ o \ g.$$

Bibliografía

-Ayres, F.: Algebra Moderna.
-Doneddu, A.: Algebra y Geometría.
-Gentile, E.: Notas de Álgebra.
-Lentin-Rivaud: Álgebra Moderna
-Pecastaigns, F.: Chemins vers l'Algèbre
-Pinzón, A. Conjuntos y estructuras.
-Queysanne, M.: Algebra Básica.
-Taylor, H- Wade, T.: Matemáticas Básicas.

El Alumno deberá hacer los ejercicios propuestos que siguen a continuación.

Si bien es una larga lista de ejercicios, siempre se debe tener en cuenta que para aprender matemática, es necesario resolver la mayor cantidad de ejercicios y problemas.

Es decir, no existe ningún impedimento de buscar en la bibliografía, (de los libros que existen en las bibliotecas de las Facultades de la Universidad o de los libros que eventualmente el alumno pudiera comprar) ejercicios y problemas y tratar de resolverlos.

En general, uno debe saber que, se "aprende matemática", planteando y resolviendo problemas

Asimismo, resolviendo ejercicios, muchos ejercicios, se adquiere habilidad, destreza, manejo de la simbología, y criterios.

Una vez que uno logra un manejo apropiado de todos esos elementos el aprendizaje se hace cada vez, más sencillo, y lo que antes parecía muy difícil, se vuelve con el tiempo cada vez fácil.

Ejercicios propuestos.

1.- Sea $X = \{1, 2\}$. Clasifique las siguientes relaciones en X :

a) $X \times X$; b) $\{(1, 2); (2,1); (2, 2)\}$; c) $\{(1, 1); (2, 1); (2, 2)\}$; d) $\{(1,1); (1,2); (2,2)\}$; e) $\{(1,1); (1,2); (2,1)\}$; f) $\{(2,1; (2,2)\}$; g) $\{(1,2); (2,2)\}$; h) $\{(1,2); (2,1)\}$; i) $\{(1,1); (2,2)\}$; j) $\{(1,1); (2,1)\}$; k)$\{(1,1); (1,2)\}$; m) $\{(2,1)\}$; n) $(1,2)\}$; o) $\{(1,1)\}$.

2.- Dado $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$, construya las siguientes relaciones en A:
a) $\leq$, siendo $x \leq y \Leftrightarrow y - x \in A$; b) $<$, siendo $x < y \Leftrightarrow (y - x \in A \wedge y - x \neq 0)$;
c) $=$, siendo $x = y \Leftrightarrow y - x = 0$; d) $\sim$, siendo $x \sim y \Leftrightarrow y - x$ es un entero divisible por 2;
e) $*$, siendo $x * y \Leftrightarrow 4 < x - y$; f) $\&$, siendo $x \,\&\, y \Leftrightarrow y - x = 1$.

3.- Sea R la relación $\leq$ en N^*, es decir $(a, b) \in R$ ssi $a \leq b$. Determine r, s, a, t.

4.- Sea R la relación en $N^* \times N^*$ definido por $(a, b) = (c, d) \Leftrightarrow ad = bc$. Demuestre que R es una relación de equivalencia.

5.- Sea R una relación en $N^* \times N^*$ definida de la siguiente manera:

$(a, b)\, R\, (c, d) \Leftrightarrow (a + d = b + c)$. Pruebe que R es una relación de equivalencia.

6.- Sea $E = \{1, 2, 3, ..., 9\}$. En $E \times E$, se define la relación

$$(a, b) \equiv (c, d) \Leftrightarrow a - b = c - d, \text{ o si } b - a = d - c.$$

Muestre que es una relación de equivalencia, y señale las clases de equivalencia.

7.- El mismo estudio en $E \times E$ para la relación: $(a, b) \equiv (c, d) \Leftrightarrow a + b = c + d$.

8.- Halle todas las particiones de $X = \{a, b, c, d\}$.

9.- Sea $X = \{a, b, c, d, e, f, g\}$; decir si las siguientes son particiones de X:
a) $\{\{a, c, e\}; \{b\}; \{d, g\}\}$; b) $\{\{a, e, g\}; \{b,e, f\}; \{c, d, e\}\}$;
c) $\{ \{a, b, e, g\}; \{c\}; \{d, f\}\}$; d) $\{\{a, b, c, d, e, f, g\}\}$.

10.- Si $S = \{1, 2, 3, 4, 5\}$ se reparte de la siguiente manera; $S_1 = \{1\}$; $S_2 = \{2, 4\}$; $S_3 = \{3\}$; $S_4 = \{5\}$.
De las relaciones de equivalencia que inducen estos 4 sub-conjuntos.

11.- Sean Z; $m \in Z$; $m > 0$. Si p y q $\in$ Z definimos:

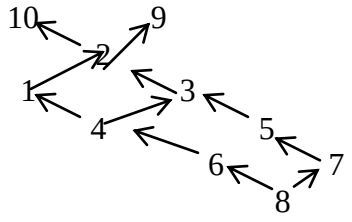
$$p \equiv q \pmod m \iff p - q = k \cdot m \qquad \text{para } k \in Z.$$

Pruébese que $\equiv \pmod m$ es una relación de equivalencia en Z , $\forall m \geq 1$.

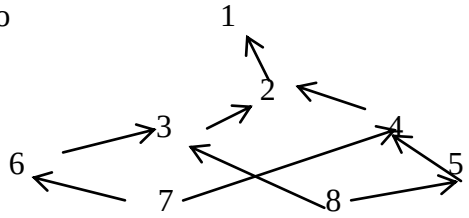
12.- Sea E = {1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84}. Considere la relación "divide a ". Muestre que es un orden parcial y construya un retículo.

13.- La relación "x divide a y" en N* es un orden parcial; ¿cuáles de los siguientes subconjuntos de N son totalmente ordenados?: a) {4, 3, 15}; b) {2,4, 8, 16}; c) {1, 2, 3, ...}; d) {5}.

14.- Sea E = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}, ordenado como lo lo indica el diagrama.
Sea X = {4, 5, 6}. a) Halle el conjunto de los mayorantes de X. b) Halle el conjunto de los minorantes. c) Halle Sup X. d) Halle Inf X



15.- Sea E = {1, 2, 3, 4, 5, 6, 7, 8}, ordenado como lo indica el diagrama de la derecha.
Sea X = {2, 3, 4} subconjunto de E.
a) Halle el conjunto de los mayorantes .
b) Halle el conjunto de los minorantes.
c) Halle el Sup X.
d) Halle el Inf X



16.- Si E = {a, b, c}, forme la tabla de composición de P(E) para las operaciones: $\cap$, $\cup$ y Δ.

17.- Complete las tablas, (E: referencial)

$\cup$	A	B	E
A		E	
B			
E			

$\cap$	A	B	$\varnothing$
A			
B	B		
$\varnothing$			

18.- Establezca la tabla de las biyecciones de E = {a, b, c} (son 6 biyecciones)

19.- En E = {1, 2, 3, 4, 5, 6}; Hacer una tabla de formación del mínimo común múltiplo. a) ¿ Es interna?; b) ¿ Qué puede decir al respecto del máximo común divisor?.

20.- Estudie las propiedades de las siguientes leyes en **R**.
a) $x * y = 3x + 2y$; b) $x * y = 2y^2$; c) $x * y = y$; e) $x * y = xy - x - y + 2$;
f) $x * y = x^2 - xy + y^2$.

21.- Estudie las propiedades de las siguientes leyes en **RxR.**
a) (a, b) * (c, d) = (a + c, b + d) y a(c, d) = (ac, ad); **b)** (a, b) * (c, d) = (a + c, b + d) y (a, b) o (c, d) = (ac - bd; ad + bc)

22.- Estudie las leyes de composición en R^+:
a) media aritmética: $m_a = ½ (a + b)$; b) media geométrica: $m_g = (ab)^{1/2}$.
c) media armónica: $m_h = 2ab(a + b)^{-1}$.

23.- Estudie la ley de composición de las resistencias en paralelo:

$$\frac{1}{R} = \frac{1}{R_1} + \frac{1}{R_2} \quad \text{con} \quad R = R_1 * R_2 = \frac{R_1 R_2}{R_1 + R_2}$$

¿Es ley asociativa? ¿Admite elemento neutro?.

24.- Dos lentes de distancias focales f_1 y f_2 están separadas por una distancia l. La distancia focal f del sistema está dado por:

$$\frac{1}{f} = \frac{1}{f_1} + \frac{1}{f_2} - \frac{1}{f_1 f_2} \quad \text{con} \quad f = f_1 * f_2 = \frac{f_1 f_2}{f_1 + f_2 - 1}$$

25.- En Q , ¿ es distributiva la ley T respecto a la ley + en los siguientes casos?
a) x * y = 2x + 2y ; x T y = ½ xy. b) x * y = x + y +1; x T y = xy.

26.- En N se define la operación * de la siguiente manera:
a, b N, a * b = a + b + ab. a) Calcule 1 * 2; 0 * 2; 3 * 4; (2 * 5) * 6.
b) Estudie las propiedades.

27.- En el conjunto Q* se define la operación * : a * b = ½ (1/a + 1/b).
Calcule a * b para: a= - 50 y b = 25; a = ¾ y b = 25/3.
¿Es asociativa?, ¿ tiene elemento neutro?, ¿es conmutativa?.

Los enteros naturales. Grupos

3.- Los enteros naturales

3.1.- Axiomas de Péano

El número natural (o entero natural) es el primer concepto matemático creado por el espíritu humano. Todas las ciencias matemáticas se han desarrollado a partir de este concepto que se desarrollará aquí mediante los axiomas dados por el matemático italiano **Péano** (1858-1932). Al conjunto de los números naturales se le denotará **N**.

Axioma 1.

Cero es un número natural.

El conjunto **N** es distinto de vacío. Contiene un elemento, el cero denotado 0. Se toma **N*= N -** {0}.

Axioma 2.

Existe una biyección φ *:* $\boldsymbol{N \rightarrow N^*}$ *que, a todo número natural x, asocia un número natural* x^{φ}*, denominado el* ***siguiente*** *de x.*

El siguiente de x se lo denota x^{φ} en lugar de $\varphi(x)$, como se haría habitualmente. Dado que φ es biyectiva, a todo entero natural $x \in \mathbf{N^*}$ $(x \neq 0)$ le corresponde un único entero natural y tal que $y^{\varphi} = x$. Este entero y se denomina el **precedente** de x.

Se denota $0^{\varphi} = 1$. Se tiene después 1^{φ} = dos, etc. Aplicando φ al último número obtenido, se obtiene uno nuevo, distinto de todos los anteriores que ya se han obtenidos.

Axioma 3, o axioma de recurrencia (inducción):

Sea A una parte de ***N*** *tal que A contiene al cero, y que, si A contiene a x, entonces A también contiene al siguiente* x^{φ}*. Entonces A coincide con el conjunto* ***N*** *de todos los números naturales.*

Este axioma se simboliza como sigue. Sea $A \subset \mathbf{N}$.

$$\left(\begin{array}{c} 0 \in A \\ x \in A \ \Rightarrow \ x^{\varphi} \in A \end{array} \right) \ \Rightarrow \quad A = \mathbf{N}.$$

La proposición $x \in A$ se denomina *hipótesis de recurrencia*.

3.2.- Adición de números naturales

Definición

A todo par ordenado $(x, y) \in \mathbf{N}^2$, *se asocia un número natural, denominado* ***suma*** *de* x *e* y, *denotado* $x + y$, *y definido por recurrencia como sigue:*

a) $x + 0 = x$;
b) supuesto definido $x + y$, *se define* $x + y^{\varphi}$ *de la siguiente forma*

$$x + y^{\varphi} = (x + y)^{\varphi}.$$

En esta definición, x es fijado arbitrariamente en $\mathbf{N}$. La recurrencia se hace sobre y. Si se designa por A al conjunto de los enteros naturales y tales que la adición $x + y$ esté definida, se puede ver por (a) que $0 \in A$ y por (b) que $y \in A$ implica $y^{\varphi} \in A$.

Luego $A = \mathbf{N}$ y la adición queda definida por recurrencia para todos los enteros naturales. Para todo $x \in \mathbf{N}$ y para $y = 0$

$$x + 0^{\varphi} = (x + 0)^{\varphi} = x^{\varphi}$$

de manera que

$$x + 1 = x^{\varphi}.$$

El siguiente de x es entonces $x + 1$.

Se demuestra que esta adición admite elemento neutro 0, que es asociativa y conmutativa. No es posible dar aquí todas las demostraciones. Se proponen algunos ejercicios para interesar al lector en el razonamiento por recurrencia que es de capital importancia en numerosas demostraciones matemáticas.

La ***inducción o recurrencia matemática*** es uno de los métodos de demostración más frecuentes en algunos campos de la matemática. La idea se entiende con facilidad. Se considera al axioma 3 , o axioma de inducción y se toma el siguiente ejemplo: Se supone que se tienen las 28 fichas de dominó. Se está seguro de que están colocadas de pie, en fila india, de forma que si cae una, cae, seguro la siguiente. Si un gracioso tira la primera hacia la segunda. ¿Qué pasará?¡Se caerán todas! Esto viene a ser la inducción. Se puede considerar los números 1,2,3,4,.. como fichas de dominó. Se supone

estar seguro en demostrar, que si uno cualquiera de estos números tiene cierta propiedad p, entonces también el siguiente la tiene. A continuación uno se debe asegurar que el primero, el 1, tiene la propiedad p. ¿Conclusión? Claramente *todos* los números naturales tienen la propiedad p. A veces se puede probar que el número 25 tiene la propiedad p, pero no el 1. Entonces, claro está se puede concluir que todos, a partir del 25, tienen la propiedad.

Como se ve, hay dos cosas importantes de las que uno se tiene que cerciorar:

(1)*Si h tiene la propiedad p, entonces también h +1 tiene la propiedad p.*
(2) El número 1 (o tal vez el 25), tiene la propiedad p.

La conclusión, es decir que todas las fichas hayan caído se expresa: "la proposición P(n) es verdadera para todo n".

La posibilidad de obtener tal conclusión a partir de (1) y (2) es una propiedad intrínseca de los números naturales que puede aplicarse a toda situación similar a la dada. El número de fichas de dominó que dimos como dato al principio, no desempeña ningún papel en este razonamiento, puede aumentarse tanto como se quiera. Con este ejemplo el lector habrá captado el soporte intuitivo del "principio de inducción o recurrencia", que damos a continuación.

Principio de Inducción o Recurrencia

Sea P(n) una proposición asociada a todo número natural n. Si se cumple:

1) la proposición P(0) es verdadera, eventualmente P(1).

2) si la proposición P(n) es verdadera, entonces también lo es P(n +1) para cualquier n,

Entonces P(n) es verdadera para cualquier número natural n.

Demostración:

Definamos $A = \{n/P(n)$ es *verdadera*$\}$. Queremos probar que $A = \mathbf{N}$. Notemos que

(i) $0 \in A$, (o $1 \in A$)

(ii) Si $n \in A$ entonces $(n + 1) \in A$

Sea $T = \mathbf{N} - A$. Es suficiente probar que $T = \varnothing$. Supongamos que $T \neq \varnothing$.

Entonces T contiene un menor elemento m. Por hipótesis $m \neq 0$ y entonces $m \geq 1$. Pero como $0 < 1$, $0 < m - 1 < m$. Como m es el menor elemento de T, se sigue que:

$$m - 1 \in A.$$

Pero entonces, por hipótesis $(m - 1) + 1 = m$ pertenece a A, lo cual es un absurdo.

OBSERVACIÓN.-

La existencia de este elemento mínimo (m) es consecuencia del principio de buena ordenación en los números naturales: "todo subconjunto no vacío de **N**, tiene menor elemento".

La validez de este principio es una de las propiedades fundamentales de los números naturales. Consideremos otras formas alternativas al Principio de Inducción:

Sea P(n) tal que:

a_1) P(p) es verdadera
a_2) $\forall k \geq p$ si P(k) es verdadera entonces P(k+1) es verdadera.

Entonces P(n) es verdadera cualquiera sea $n \geq p$.

Sea P(n) tal que:

b_1) P(1) es verdadera
b_2) $\forall k \in \mathbf{N}$ si P(m) es verdadera $\forall m \leq k$, entonces P(k+1) es verdadera.

Entonces P(n) es verdadera $\forall n \in \mathbf{N}$. A esta forma se la suele denominar "Principio de Inducción Completa".

Por ejemplo, 0 es elemento neutro. Por definición de la adición, 0 es ya elemento neutro a derecha. Se demuestra, por recurrencia sobre x, que:

(1) $0 + x = x$.

(1) es verdadera para $x = 0$, pues 0 es elemento neutro a derecha. Se supone (1) verdadera para x, y se debe demostrar que lo es para x^{φ}.

Se tiene

$$0 + x^{\varphi} = (0 + x)^{\varphi} \quad \text{(definición de adición)}$$
$$(0 + x)^{\varphi} = x^{\varphi} \quad \text{(hipótesis de recurrencia).}$$

(1) queda entonces demostrado por recurrencia para todo $x \in \mathbf{N}$.

N es un **monoide aditivo conmutativo.** Se puede demostrar también que todo elemento de **N** es simplificable para la adición.

3.3. Relación de orden

Definición

Sean dos números naturales a y b. Si existe un número natural x tal que:

$a + x = b$, se dice entonces que "a es al menos igual a b" y se denota $a \leq b$.

Al entero natural x se le denomina **diferencia** de a y b y se denota $x = b - a$.

Si tal número x existe, es único ya que todo entero es simplificable para la adición:

$$b = a + x = a + x' \Rightarrow x = x'.$$

Se puede demostrar que la relación $\leq$ es un ***orden total*** en **N**.

La relación es reflexiva, antisimétrica y transitiva. A modo de ejercicio, se demuestra que el orden es total, es decir:

$$\forall (a, b) \in \mathbf{N}^2, \text{ se tiene } \quad a \leq b \quad o \quad b \leq a.$$

Se fija "b" y se razona por recurrencia sobre "a". Sea A el conjunto de los números naturales "a" tales que $a \leq b$ o $b \leq a$.

1° Se tiene $0 \in A$, pues para todo $b \in \mathbf{N}$, $0 + b = b$ luego $0 \leq b$.
2° Se supone $a \in A$ y se demuestra $a^{\varphi} \in A$. La hipótesis de recurrencia $a \in A$ significa que se tienen $a \leq b$ o $b \leq a$.

- Si $a \geq b$, existe $x \in \mathbf{N}$ tal que $a = b + x$, de donde $a^{\varphi} = b + x^{\varphi}$ y por consiguiente $a^{\varphi} \geq b$ y $a^{\varphi} \in A$.

- Si $a \leq b$, se puede suponer $a \neq b$ (el caso $a = b$ ya ha sido examinado). Existe entonces $x \neq 0$ tal que $a + x = b$. Como $x \neq 0$, hay un precedente y $(y^{\varphi} = x)$. Luego

$$b = a + y^{\varphi} = (a + y)^{\varphi} = (y + a)^{\varphi} = y + a^{\varphi},$$

de donde

$$a^{\varphi} \leq b \quad y \quad a^{\varphi} \in A.$$

Orden estricto.

Definición.

Sean dos números naturales a y b. Si existe un $x \in \mathbf{N}$, $x \neq 0$, tal que:

$a + x = b$, se dice entonces que "a es estrictamente menor a b" y se denota

$$a < b.$$

Es fácil de ver que $a < b$ es una relación de orden estricto total en **N** y que las siguientes relaciones son válidas, para todo entero natural a, b, c:

$$a \leq b \Rightarrow a + c \leq b + c$$
$$a < b \Rightarrow a + c < b + c$$

3.4. Equipotencia

Definición.

Sean A y B dos conjuntos. Se dice que A es equipotente a B si existe una biyección de A sobre B. Se denota entonces $A \leftrightarrow B$.

Para todo conjunto A, se tiene evidentemente $A \leftrightarrow A$ (se toma la coincidencia).

Si $A \leftrightarrow B$ entonces $B \leftrightarrow A$. (Si $f: A \rightarrow B$ es la biyección de la hipótesis, entonces $f: B \rightarrow A$ es la de la consecuencia. Por último,

$$A \leftrightarrow B \quad y \quad B \leftrightarrow C \quad \text{implica} \quad A \leftrightarrow C$$

(pues la compuesta de dos biyecciones es una biyección).

Sea entonces una conjunto A. Todos los conjuntos equipotentes al A constituyen una clase que se denomina un ***cardinal*** y se lo denota card A.

Conjunto finito.

Un conjunto A se dice ***finito*** *si es equipotente a un intervalo [1, n] incluído en* ***N.*** *Se denota entonces card A = n.*

Conjunto infinito numerable.

Un conjunto A se dice ***infinito numerable*** *si es equipotente a* ***N.***

(card A = card ***N****.)*

Existen conjuntos infinitos que tienen una potencia superior a la de **N**. Por ejemplo, el conjunto **R** de los números reales. Esos conjuntos se dicen ***infinitos no numerables.***

P *Todo conjunto equipotente a una de sus partes estrictas es infinito.*

En efecto, si A está incluído estrictamente en B, y si A y B son finitos, entonces el card A es estrictamente menor al card B. Como resultado se puede ver que cuando A está estrictamente incluído en B y si B es infinito, el card A = card B.

Ejemplo.-

La aplicación f, de **N** sobre **N - {0},** f(x) = x + 1 es una biyección. Luego **N** es infinito.

Teorema.

*Sea A y B dos conjuntos **finitos** del mismo cardinal y f: A → B una aplicación. Las siguientes propiedades son equivalentes:*

(1) f es inyectiva;
(2) f es sobreyectiva;
(3) f es biyectiva.

Como la propiedad (3) es la conjunción de las propiedades (1) y (2), es suficiente establecer la equivalencia de (1) y (2).

- (1) ⇒ (2). Si f es inyectiva, es una biyección de A sobre f(A) y por consiguiente card f(A) es igual al card A, de donde card f(A) = card B y como f(A) B finito, se tiene f(A) = B.

- (2) ⇒ (1). Se utiliza la descomposición canónica de la aplicación f: A → B. La relación de equivalencia sobre A:

$$x \,\Re\, x' \Leftrightarrow f(x) = f(x')$$

parte al conjunto A en clases de equivalencia.

El conjunto cociente es denotado $A/\Re$. La aplicación

$\bar{f} : A/\Re \to f(A) = B$ (ya que f es sobreyectiva) es una biyección, de donde:
card $A/\Re$ = card B = card A. El número de clases de $A/\Re$ es igual al número de elementos de A, esto quiere decir, que toda clase es un singleton, de donde

$$f(x) = f(x') \Rightarrow x \,\Re\, x' \Rightarrow x = x',$$

y f es inyectiva.

3.5.- Recurrencia limitada

Sean a y b dos números naturales tales que a < b. Sea A una parte de **N** que verifique

$$A \subset [a,b] \subset \mathbf{N}.$$

Se designará por $\wp(n)$ una propiedad verdadera si, y solamente si, $n \in A$.

Se establecen las dos proposiciones siguientes:

Primera proposición: $\wp(a)$ es verdadera ($a \in A$).

Segunda proposición: la hipótesis "$\wp(n)$ es verdadera para $a \leq n < b$" implica la consecuencia " $\wp(n+1)$ es verdadera".

Se deduce entonces que $\wp(n)$ es verdadera cualquiera que sea el elemento n del intervalo cerrado [a, b].

La recurrencia limitada se simboliza como sigue:

$$A \subset [a,b] \subset \mathrm{N},$$

$$\left(\begin{array}{c} a \in A \\ \left(n \in A \text{ y } n \neq b\right) \Rightarrow n+1 \in A \end{array} \right) \Rightarrow A = [a,b].$$

Se dice que la *recurrencia queda limitada* al intervalo [*a, b*]

Teorema.

Todo conjunto no vacío, totalmente ordenado y finito, admite un elemento máximo y un elemento mínimo.

Sea E un conjunto no vacío, totalmente ordenado y finito. Se hace la demostración para el elemento más grande como ejemplo.

Sea card E = n ≥ 1. Se razona por recurrencia limitada a n. Sea A el conjunto de los enteros p tales que $1 \leq p \leq n$ y que toda parte de E que tenga p elementos admita un elemento máximo. Primero $1 \in A$ evidentemente. Por otra parte, se supone $1 \leq p < n$ y $p \in A$, y sea F una parte de E que tenga p + 1 elementos. Se toma $a \in F$ y G = F - {a}. Como G posee p elementos, la hipótesis de recurrencia permite afirmar que máx G = b existe, de donde máx {a,b} = máx F existe también.

Teorema.

Toda parte no vacía de ***N*** *admite un elemento mínimo.*

Sea $P \subset \mathbf{N}$ con $P \neq \varnothing$. Se toma $a \in P$. Si existen en P elementos inferiores al a, ellos pertenecen al intervalo [0, a] y constituyen el conjunto $J = P \cap [0,a]$. J no es vacío, pues contiene al a. Es finito dado que está incluído en [0,a]. Entonces admite un elemento mínimo (Teorema precedente) que es el mín P.

Ejemplos.

1.- Sean $n, m \in \mathbf{N}$, $n \neq 0$, $n < m$ entonces $n/m \notin \mathbf{N}$.

Dado que $0 \neq n < m \Rightarrow n/m < 1$, como no puede ser cero entonces se tiene que $n/m \notin \mathbf{N}$.

2.- No existe $m \in \mathbf{N}$, tal que $m^2 = 2$.

En efecto, si tal m existiese se tendría $1 \leq m$. Pero $m = 1$ no es posible, ya que $1^2 = 1$. Por consiguiente tendrá que ser $1 < m$, o sea $2 \leq m$ y entonces se tendrá que $4 \leq m^2 = 2$, que es un absurdo.
Esta situación surgió de suponer la existencia de m en **N** con $m^2 = 2$.

3.6.- Sucesiones.

3.6.1- Definición.

Sea un intervalo inicial [1, b] de números naturales. Se llama *sucesión finita en* **R** a toda aplicación

$$x: [1, b] \rightarrow \mathbf{R}$$

que se escribe en la forma tradicional $x_1, \ldots, x_b$ donde

$$x_1 = x(1), \ldots, x_i = x(i), \ldots, x_b = x(b)$$

Dicho de otra manera, una *sucesión* es una aplicación

$$x: \mathbf{N} \rightarrow \mathbf{R},$$

que a cada $n \in \mathbf{N}$ le asocia uno y sólo un $x(n) = x_n$; es decir, en una sucesión $x_0, x_1, \ldots, x_n, \ldots$ de elementos de **R**, cada elemento x_{n-1}, se corresponde con un número natural n; se dice que n es el elemento *n*-ésimo de la sucesión. La sucesión se denota poniendo

$$(x_n)_{n \in \mathbf{N}} \text{ o simplemente } (x_n).$$

En una sucesión, de un elemento interesa, no sólo su valor, sino también el lugar que ocupa en ella.

Ejemplos.
Son sucesiones las siguientes:

0, 0, 0, 0, 0
1, -1, 1, -1, 1
1, 2, 3, 4, 5
2, 4, 6, 8, 10
½, ¼, 1/8, 1/16, 1/32
1,½, 1/3,¼, 1/5

(Notar que al dar una sucesión se da un orden entre sus elementos).

3.6.2.- Suma y producto de sucesiones.

Para una sucesión de números reales $x_1, x_2, ..., x_n$, se define su *suma* y su *producto*.

Por ejemplo, si se trata de una sucesión de 3 términos x_1, x_2, x_3, la suma está definida en forma natural (gracias a la propiedad asociativa).
Esta es

$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ que se escribe simplemente por

$$x_1 + x_2 + x_3$$

De la misma manera se puede hacer el producto.

Definición.

Dada una sucesión $x_1, ... , x_n$, $n \in \mathbf{N}$ de números reales se denomina *suma* de la sucesión al número real denotado por

$$\sum_{i=1}^{i=n} x_i \text{ o también } \sum_{i=1}^{n} x_i \text{ tal que } \sum_{i=1}^{i=1} x_i = x_1,$$

$$\sum_{i=1}^{i=n+1} x_i = (\sum_{i=1}^{i=n} x_i) + x_{n+1}$$

De manera similar se denomina *producto* de la sucesión, al número real denotado por

$$\prod_{i=1}^{i=n} x_i \quad \text{tal que}$$

a) $\prod_{i=1}^{i=1} x_i = x_1$

b) $\prod_{i=1}^{i=n+1} x_i = \left(\prod_{i=1}^{i=n} x_i \right) \cdot x_{n+1}$

c) Dada una sucesión $a_o, a_1, \ldots, a_n$ de números reales, se define

$$\sum_{i=0}^{n} a_i = a_0 + \sum_{i=1}^{n} a_i$$

El principio de inducción asegura que tanto la suma como el producto quedan completamente definidos para todas las sucesiones finitas de números reales.

Ejemplos.

1) $\sum_{i=1}^{3} i = 1+2+3 = 6$ 2) $\sum_{i=1}^{4} i^2 = (1)^2 + (2)^2 + (3)^2 + (4)^2 = 1+4+9+16 = 30$

3) $\prod_{i=1}^{n} i = 1.2.3.4....(n-1)n = n!$ (factorial de n) 4) $\prod_{i=1}^{3} (i+1)^i = (1+1)^1.(2+1)^2.(3+1)^3$

3.6.2.1- Fórmulas de sucesión aritmética y sucesión geométrica.

Definición 1: Sucesión aritmética.

Sea (u_n) una sucesión numérica, de primer término u_0 y tal que, $\forall n \in \mathbf{N}$, $u_{n+1} = u_n + r$ (r una constante llamada *razón o diferencia* de la sucesión). Entonces decimos que (u_n) es una *sucesión aritmética*.

Por ejemplo: Si $u_0 = 1$ y $r = 2$

$u_0 = 1$; $u_1 = u_0 + 2 = 3$, $u_2 = u_1 + 2 = 5$, $u_3 = u_2 + 2 = 7$,

Propiedades.

1. $u_1 = u_0 + r$; $u_2 = u_1 + r = u_0 + 2r$; $u_3 = u_2 + r = u_0 + 3r$; ...;

$$\boxed{u_n = u_0 + nr, \forall n \in \mathbf{N},}$$

2. $u_n + u_0 = u_{n-1} + u_1 = u_{n-2} + u_2 = \ldots = u_{n-p} + u_p$;

3. con la excepción de u_0, cada término u_p es la media aritmética de los términos u_{p-1} y u_{p+1}; de lo que resulta:

$$u_p = \tfrac{1}{2}(u_{p-1} + u_{p+1}).$$

4. La suma de los n primeros términos de la sucesión aritmética: $S_n = \sum_{i=0}^{i=n-1} u_i$

$$\boxed{S_n = u_0 + u_1 + \ldots + u_{n-1} = \frac{n}{2}[2u_0 + (n-1)r]}$$

Ejemplos.

1. Sea la sucesión aritmética de primer término $u_0 = 1$ y de razón r = 3. ¿Cuál es el término número 1996?

El término 1996 es: $u_{1995} = u_0 + 1995 \cdot r = 1 + 3 \cdot 1995 = 5986$

2. Calcular $A = 1 + 2 + 3 + \cdots + n$

A es la suma de los n primeros términos de la sucesión aritmética de primer término $u_0 = 1$ y de razón r = 1:

$$A = \frac{n}{2}[2 + (n-1)] = \frac{n}{2}(n+1), \quad \text{luego:} \quad 1 + 2 + 3 + \cdots + n = \frac{n}{2}(n+1)$$

<u>Definición 2</u>. Sucesiones geométricas.

Sea (u_n) una sucesión de primer término u_0, y tal que, $\forall n \in \mathbf{N}$, $u_{n+1} = q\, u_n$ (q es una constante llamada razón de la sucesión), decimos entonces que (u_n) es una *<u>sucesión geométrica</u>*.

Por ejemplo, si: $u_0 = 5$ y $q = -3$

$$u_0 = 5; \quad u_1 = -3 \cdot u_0 = -15; \quad u_2 = -3 \cdot u_1 = 45; \quad u_3 = -3 \cdot u_2 = -135; \ \cdots$$

si $u_0 = 1$ y $q = ½$; los términos de la sucesión serán:

$$1;\ ½;\ \frac{1}{2^2};\ \frac{1}{2^3};\ \cdots$$

<u>Propiedades.</u>

1. $u_1 = q \cdot u_0$; $u_2 = q \cdot u_1 = q^2 \cdot u_0$; $u_3 = q \cdot u_2 = q^3 \cdot u_0$; $\cdots$;

$$\boxed{u_n = u_0 \cdot q^n \,,\ \forall n \in \mathbf{N}}$$

2. $u_0 \cdot u_n = u_1 \cdot u_{n-1} = u_2 \cdot u_{n-2} = u_p \cdot u_{n-p}$

3. Con excepción de u_0; cada término u_p es igual a la media geométrica de los términos: u_{p-1} y u_{p+1} que se encuadran: $u_p^2 = u_{p-1} \cdot u_{p+1}$

4. la suma S_n de los n primeros términos de la sucesión geométrica:

$$\boxed{S_n = u_0 + u_1 + \ldots + u_{n-1} = \sum_{i=0}^{i=n-1} u_i = u_0 \frac{1-q^n}{1-q} \quad (q \neq 1)}$$

si $q = 1$, $S_n = nu_0$

<u>Ejemplos</u>.

1. Determinar el 10^{mo} término de la sucesión geométrica de primer término $u_0 = 1$ y de razón $q = 2$.

El décimo término será: $u_9 = u_0 \cdot q^9 = 1 \cdot 2^9 = 512$.

2. Calcular: $A = 1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^{n-1}}$

A es la suma de los n primeros términos de la sucesión geométrica de primer término $u_0 = 1$ y de razón $q = ½$:

$$A = 1\cdot\frac{1-(\frac{1}{2})^2}{1-\frac{1}{2}} = 2\cdot[1-(\frac{1}{2})^n]$$

3.- Si la población de una Ciudad de Argentina en 1996 es de 400.000 habitantes; ¿cuál será la población en el año 2010, si se supone un crecimiento anual de 1,5% de la población durante ese periodo?.

-sea P_0 la población en 1996, $P_0 = 400.000$

-la población en 1997 será: $P_1 = P_0 + \frac{1,5}{100}P_0 = P_0 \cdot 1,015$,

-la población en 1998 será: $P_2 = P_1 \cdot 1,015 = P_0 \cdot (1,015)^2$.

Esta población constituye una sucesión geométrica de primer término P_0 y de razón $q = 1,015$; en el año 2010, el término correspondiente a esta población sera el término

$$P_{14} = P_0 \cdot q^{14} = 492.702 .$$

.

3.7.- Grupos

3.7.1. Estructura de grupo.

Definición.

*Se llama **grupo** a todo monoide donde todo elemento es simetrizable.*

En otros términos un conjunto G munido de una ley de composición interna (denotado multiplicativamente en general) es un grupo si

1. la ley es asociativa:

$$(\forall a,b,c \in G) \qquad (ab)c = a(bc);$$

2. admite un elemento neutro e:

$$(\forall a \in G \qquad ae = ea = a;$$

3. todo elemento a de G admite un inverso a^{-1}:

$$aa^{-1} = a^{-1}a = e.$$

Cuando la ley es conmutativa, se dice que G es un ***grupo conmutativo.*** Se denota en general a esta ley aditivamente (y al simétrico de a se le llama el opuesto de a y se denota -a).

En un grupo G, todo elemento es simplificable (P_2), el simétrico de todo elemento es único (P_3) y para todo par ordenado (a,b) de elementos de G (P_4):

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

Ejemplo.

Grupo de las permutaciones de un conjunto E.

Sea E un conjunto cualquiera. Se sabe que una permutación de E es una biyección de E sobre sí mismo. Sea P(E) el conjunto de las permutaciones de E. Este conjunto es una parte del monoide (F(E), $\circ$) de las aplicaciones de E en si mismo.

a) La ley de composición $\circ$ de las aplicaciones es interna en P(E). En efecto, la compuesta de dos biyecciones de E es una biyección de E.

b) La ley de composición de las aplicaciones es asociativa.

c) El elemento neutro, la coincidencia es una biyección.

d) Todo $f \in P(E)$ es una biyección, su recíproca f^{-1} es también una biyección de E sobre E.

Luego (P(E), $\circ$) es un ***grupo.***

En Geometría (E es el conjunto de puntos), toda permutación de E se denomina también **transformación** de E.

3.7.2.- Los enteros relativos.

La adición le confiere a **N** de la estructura de monoide conmutativo donde todo elemento es simplificable. Pero no le confiere de la estructura de grupo. Le falta la siguiente propiedad: todo número tiene un simétrico para la adición. El problema de la simetrización de la adición en **N** conduce a la introducción de nuevos símbolos, denominados ***enteros negativos*** (los enteros naturales se denominan entonces ***enteros positivos***).

A todo número natural $x \in \mathbf{N}$, se asocia un entero negativo, denotado provisoriamente x' (x' es distinto de x salvo para x = 0). Se consideran así dos ejemplares de **N** y para diferenciarlo el uno del otro, se denota al segundo $\mathbf{N}^-$. Se tiene así una

biyección $x \to x'$ de $\mathbf{N}$ sobre $\mathbf{N}^-$ con $0' = 0$. Si se toma $\mathbf{Z} = \mathbf{N} \cup \mathbf{N}^-$, la biyección $x \to x'$ es una extensión de una involución de $\mathbf{Z}$ por la convección $x'' = x$.

Los enteros positivos o negativos son denominados ***enteros relativos.*** Un número relativo se denota por una letra griega : $\alpha \in \mathbf{Z}$. Una letra latina designa un número natural : $a \in \mathbf{N}$.

Se extiende la adición conocida en $\mathbf{N}$ a una adición en $\mathbf{Z}$ de manera que, para todo $a \in \mathbf{N}$, se tenga $a + a' = 0$.

Definición.

A todo par ordenado $(\alpha, \beta) \in \mathbf{Z}^2$, se asocia un entero relativo, denominado **suma** de α y β, denotada $\alpha + \beta$ y definida como sigue:

1. α y β en $\mathbf{N}$: $\alpha + \beta$ es la suma conocida en $\mathbf{N}$.
2. α y β en $\mathbf{N}^-$: $a' + b' = (a + b)'$.
3. $\alpha \in \mathbf{N}^-$ y $\beta \in \mathbf{N}$: $a' + b = b + a' = b - a$, si $b \geq a$;
   $a' + b = b + a' = a - b$, si $b \leq a$.

Es evidente que esta operación es conmutativa y que admite elemento neutro 0. Es evidente también que todo elemento admite un simétrico, denominado aquí el *opuesto*. Para todo $a \in \mathbf{N}$, se puede denotar $a' = -a$.

La asociatividad se puede demostrar como un ejercicio:

$$1) \qquad (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma).$$

a) Cambiar el signo de $\alpha \in \mathbf{Z}$, esto se puede hacer tomando el opuesto. Observar que si se cambia el signo de α y β , la suma $\alpha + \beta$ cambia de signo. Se deduce que es suficiente para demostrar (1) cuando cualquiera de los tres enteros α, β, γ es negativo.

b) Mostrar (con ayuda de la conmutatividad de la adición) que es suficiente demostrar (1) cuando el número negativo ocupa el primer lugar, esto es habrá que demostrar

$$(2) \qquad (a' + b) + c = a' + (b + c).$$

c) para demostrar (2) se contemplan tres casos:

$$a \geq b + c, \quad b < a < b + c, \quad \text{por último } a \leq b.$$

Finalmente, el problema de la simetrización de la adición en $\mathbf{N}$ queda así resuelto. El conjunto $\mathbf{Z}$ de los enteros relativos con la adición así definida es un ***grupo aditivo conmutativo.***

Extensión del orden.

Definición.

Sean dos enteros relativos α y β. Si $-\alpha \in \mathbf{N}$, se dira que "α es al menos igual a β" y se notará $\alpha \leq \beta$.

Se observa primero que si α y β son dos enteros naturales, la relación $\alpha \leq \beta$ coincide con la relación de orden definida en **N**. Ahora, se puede mostrar que la relación así definida en **Z** es un orden total compatible con la adición; para todo entero α, β, γ :

$$\alpha \leq \beta \quad \Rightarrow \quad \alpha + \gamma \leq \beta + \gamma$$

Se dice que **Z** es un ***grupo aditivo ordenado.***

3.7.3.- Sub-grupo

Definición.

Sea G un grupo. Una parte H no vacía de G es denominada ***sub-grupo*** *de G si H es un sub-magma de G y si este sub-magma es así mismo un grupo.*

Como en G todo elemento es simplificable, entonces el elemento neutro de todo sub-grupo H de G coincide con el de G (ver P_5)

P_6 *Sea G un grupo y $\varnothing \neq H \subset G$. Entonces H es sub-grupo de G si, y solamente si,*

$$(1) \quad (a \in H \text{ y } b \in H) \Rightarrow ab \in H,$$
$$(2) \quad a \in H \Rightarrow a^{-1} \in H.$$

Necesidad.

Sea H un sub-grupo de G. entonces A es sub-magma de G y la primer implicación es verdadera. Por otra parte, ya que H y G tienen el mismo elemento neutro, el inverso de todo elemento a de H en G es inverso de a en H y la segunda implicación es verdadera.

Suficiencia.

Sea H una parte no vacía de G que verifique las dos condiciones del enunciado. Entonces H es sub-magma de G de acuerdo a (1). Por consiguiente el elemento neutro e de G pertenece a H pues de acuerdo a (1) y (2)

$$a \in H \quad \Rightarrow \quad a^{-1} \in H \quad \Rightarrow \quad aa^{-1} = e \in H,$$

luego H es sub-monoide de G con el mismo elemento neutro.

Por último, todo elemento de H admite un inverso en H de acuerdo a (2). Luego H es sub-grupo de G.

P_7 *Sea G un grupo y $\varnothing \neq H \subset G$. Entonces H es sub-grupo de G si, y solamente si,*

$$(a \in H \quad y \quad b \in H) \quad \Rightarrow \quad ab^{-1} \in H.$$

La condición es evidentemente necesaria. Se debe probar que es suficiente:

1. El elemento neutro e de G pertenece a H (se toma b = a).
2. La condición (2) de (P_6) se satisface (se toma a = e).
3. La condición (1) de (P_6) es también satisfecha pues

$$(a \in H \quad y \quad c \in H) \quad \Rightarrow \quad ac \in H \qquad \text{(se toma } b = c^{-1}\text{)},$$

luego H es sub-grupo de G.

Ejemplos.

1. Para todo grupo G de elemento neutro e, el singleton {e}es un sub-grupo de G.

2. En Geometría plana euclidiana, el plano es denotado por E, se sabe que el conjunto P(E) de las transformaciones de E es un grupo.

Un sub-grupo importante de P(E) es el sub-grupo $\mathfrak{I}$ de las ***isometrías***.

Este sub-grupo $\mathfrak{I}$ admite así mismo dos sub-grupos observables:
- el sub-grupo $\mathbb{D}$ de los ***desplazamientos;***
- el sub-grupo conmutativo R_o de las ***rotaciones*** de centro ***o*** (para todo punto ***o***);
- el sub-grupo conmutativo T de las ***traslaciones.***
- R_o y T son dos sub-grupos de $\mathbb{D}$

P_8 *La intersección de una familia de sub-grupos de G es un sub-grupo de G.*

Sea $(H_\lambda)_{\lambda \in L}$ una familia de sub-grupos de G. Se debe mostrar que

$$H = \bigcap_{\lambda \in L} H_\lambda$$

es tambien sub-grupo de G. En efecto, $H \neq \varnothing$ pues el elemento neutro pertenece a H. Ademas,

$$x \in H \Rightarrow (\forall \lambda \in L) \quad x \in H_\lambda,$$
$$y \in H \Rightarrow (\forall \lambda \in L) \quad y \in H_\lambda.$$

En consecuencia, para todo $\lambda \in L$, se tiene $xy^{-1} \in H_\lambda$, ya que H_λ es sub-grupo de G. De ello resulta $xy^{-1} \in H$ y es entonces sub-grupo de G (P_7).

3.7.4.- Grupo de los elementos inversibles de un monoide

Sea M un monoide denotado multiplicativamente, de elemento neutro e. Se designa por U al conjunto de los elementos inversibles de M:

$$U = \{x \in M / \exists x' \in M,\ xx' = x'x = e\}.$$

Se a denotado $x' = x^{-1}$. U no es vacío, pues, $e \in U$, y

$$x \in U \Rightarrow x^{-1} \in U.$$

Además, para todo x e y d de U, la propiedad (P_4) muestra que $xy \in U$. U es entonces un grupo.

Teorema 2.

Sea M un monoide y se designa por U al conjunto de los elementos inversibles de M. Luego la restricción a U de la ley de M induce sobre U la estructura de grupo.

U se denomina ***grupo de los elementos inversibles*** del monoide M.

Ejemplo.-

Sea $(\wp(E), \circ)$ el monoide de aplicaciones de un conjunto E en si mismo. El grupo de los elementos inversibles de este monoide es el grupo P(E) de las permutaciones de E.

3.7.5.- Sub-grupo engendrado por una parte.

Sea G un grupo. Para toda parte A y B de G, se denota AB al conjunto de los compuestos ab cuando a recorre A y b recorre B:

$$AB = \{x \in G / \exists\ a \in A, \exists b \in B;\ x = ab\}.$$

Si A ={a} es un singleton, se denota aB (en lugar de {a}B al conjunto de los compuestos ab cuando b recorre B.

Se denota de la misma manera Ab al conjunto de los compuestos ab cuando a recorre A.

Se denota A^{-1} al conjunto de los inversos de los elementos de A:

$$A^{-1} = \{x \in G / \exists\ y \in A;\ x = y^{-1}\}.$$

Sea ahora A una parte no vacía de un grupo G. Se van a considerar los compuestos de un número finito de elementos de A o de A^{-1}, del tipo

$$a_1a_2 \ldots a_n \quad \text{con} \quad a_i \in A \quad \text{o} \quad a_i \in A^{-1}.$$

Se designa por $Gr(A)$ al conjunto de todos estos compuestos:

$$Gr(A) = \{x \in G / \exists n \in N^* \ \text{y} \ \exists a_1, a_2, \ldots, a_n \in A \cup A^{-1} ; x = a_1a_2 \ldots a_n\}.$$

Se muestra que $Gr(A)$ es un Sub-grupo de G. En efecto

$$x \in Gr(A) \Rightarrow \exists n \in N^* \ \text{y} \ \exists a_1, \ldots, a_n \in A \cup A^{-1} ; \ x = a_1 \ldots a_n.$$

$$y \in Gr(A) \Rightarrow \exists p \in N^* \ \text{y} \ \exists b_1, \ldots, b_p \in A \cup A^{-1} ; \ y = b_1 \ldots b_p.$$

Es entonces inmediato que

$$xy^{-1} = a_1 \ldots a_n b_p^{-1} \ldots b_1^{-1},$$

con $a_1, \ldots, a_n, b_p^{-1}, \ldots, b_1^{-1}$ todos en $A \cup A^{-1}$.

En consecuencia, $xy^{-1} \in Gr(A)$, y $Gr(A)$ es sub-grupo de G, que se denomina ***sub-grupo de G engendrado por la parte A.***

Se considera ahora un sub-grupo H cualquiera de G que verifique $H \supset A$. Luego evidentemente $H \supset A^{-1}$, de donde $H \supset (A \cup A^{-1})$. Se muestra que

$$H \supset Gr(A).$$

En efecto, si $x \in Gr(A)$, existe una sucesión finita $a_1, a_2, \ldots, a_n$ de elementos de $A \cup A^{-1}$, entonces de H, tal que $x = a_1a_2 \ldots a_n$. Por consiguiente, $x \in H$.

En consecuencia, todo sub-grupo H de G que contiene A contiene también $Gr(A)$ que es entonces el más pequeño sub-grupo de G que contiene a A.

En resumen, se obtuvo el siguiente resultado:

Teorema 3.

Para toda parte no vacía A de un grupo G, el conjunto $Gr(A)$ de los compuestos de un número finito de elementos de $A \cup A^{-1}$ es un sub-grupo de G que se denomina ***sub-grupo engendrado por la parte A.***

$Gr(A)$ es el más pequeño sub-grupo de G que contiene A.

Si se considera la familia $(H_\lambda)_{\lambda \in L}$ de todos los sub-grupos de G que contienen a A, se tiene en consecuencia

$$Gr(A) = \bigcap_{\lambda \in L} H_\lambda.$$

Casos particulares.

1° Parte generatriz de un grupo G.-

Si Gr(A) coincide con G todo entero, entonces A se denomina *parte generatriz* del grupo G. Se dice también que A es un ***conjunto de generadores*** del grupo G.

2° Grupo monógeno.

Sea G un grupo y $a \in G$. El sub-grupo de G engendrado por {a} se denota Gr(a) y se denomina ***sub-grupo monógeno*** (engendrado por el único elemento a).

Si Gr(a) = G, se dice que G es un ***grupo monógeno***

3° Grupo cíclico.

Sea G un grupo y $a \in G$. Si Gr(a) es ***finito*** se le denomina ***sub-grupo cíclico*** de G. Si además Gr(a) = G, se dice que G es un ***grupo cíclico:***

$$G = \{e, a, a^2, ..., a^{n-1}\}.$$

card G = n se denomina el ***orden*** del grupo.

3.8.- Morfismos de grupos

3.8.1.- Definición

Sean G y G' dos grupos (denotados multiplicativamente). Una aplicación:

f: G $\rightarrow$ G' se dice morfismo de G en G' si

$$(\forall a,b \in G) \qquad f(ab) = f(a)\, f(b).$$

Si f es biyectiva, es un isomorfismo. Los grupos G y G' se dicen entonces ***isomorfos.***

Si G = G', el morfismo f: G $\rightarrow$ G' se denomina *endomorfismo* de G, y si es además biyectivo, se denomina *automorfismo* de G.

Ejemplos.

1. Sean G y G' dos grupos cualesquiera, e' el elemento neutro de G'. La aplicación constante f : G $\rightarrow$ G' : f(x) = e' es un morfismo.

2. Sea G un grupo. A todo $a \in G$ se le asocia la aplicación f_a: G $\rightarrow$ G' siguiente:

$$(\forall x \in G) \qquad f_a(x) = axa^{-1}.$$

f_a es un automorfismo del grupo G, denominado ***automorfismo interior inducido por a.***

3.8.1.- Propiedades

Teorema 4.

Sean G y G' dos grupos y f: G $\rightarrow$ G' un morfismo. Para todo sub-grupo H de G, f(H) es un sub-grupo de G'.

1) Se designan por *e* y *e'* los elementos neutros de G y G' y se muestra primero que ***f(e) = e'***. En efecto, para todo *y* de *f(H)*, existe $x \in H$ tal que $y = f(x)$. Entonces,

$$(\forall y \in f(H) \qquad yf(e) = f(x)\, f(e) = f(xe) = f(x) = y$$

y se tiene así mismo que $f(e)y = y$. Luego *f(e)* es elemento neutro de *f(H)*. Ahora, para $y \in f(H)$, se tiene

$$f(e)\, y = y = e'y$$

y, como *y* es simplificable, se obtiene: $\boxed{f(e) = e'}$.

2) También, para todo x$\in$ G,

$$f(x)f(x^{-1}))\, f(xx^{-1}) = f(e) = e'$$

y así mismo

$$f(x^{-1})f(x) = e'.$$

En consecuencia,

$$\boxed{[f(x)]^{-1} = f(x^{-1})},$$

donde para todo $y \in f(H)$, se tiene $y^{-1} \in f(H)$.

Por último, para todo *y* e *y'* de *f(H)*, existen *x* y *x'* de H tales que

$$y = f(x) \quad \text{y} \quad y' = f(x'),$$

de donde

$$yy' = f(x)\, f(x') = f(xx') \in f(H).$$

En consecuencia (P_6), *f(H)* es sub-grupo de G'.

El teorema queda demostrado. En particular, f(G) es sub-grupo de G'.

Núcleo de un morfismo.

Definición.

Sea $f : G \to G'$ un morfismo de grupos. Se llama ***núcleo*** *de f al conjunto de los elementos de G que tienen por imagen al elemento neutro de G'.*

Se denota

$$\ker (f) = \{x \in G / f(x) = e'\}.$$

Teorema 5.

El núcleo de un morfismo $f : G \to G'$ de grupos es un sub-grupo de G.

En efecto, para todos x e y de ker (f):

$$f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)[f(y)]^{-1} = e'e' = e'$$

entonces $xy^{-1} \in ker\ (f)$.

Teorema 6.

Sea $f : G \to G'$ un morfismo de grupos. Entonces f es inyectiva si, y solamente si, ker (f) = {e}.

En efecto, si f es inyectiva, se tiene

$$x \in ker(f) \Rightarrow f(x) = e' \Rightarrow f(x) = f(e) \Rightarrow x = e.$$

Recíprocamente, se supone que ker (f) = {e}- Entonces, para x e y en G,

$$f(x) = f(y) \Rightarrow f(x)[f(y)]^{-1} = f(xy^{-1)} = e' \Rightarrow xy^{-1} \in ker\ (f) \Rightarrow x = y.$$

3.9.- Grupo - cociente

3.9.1.- Relaciones de equivalencia compatibles con la ley de grupo

Sea G un grupo y se considera una relación de equivalencia $\mathcal{R}$ sobre G compatible con la ley del grupo. Entonces, en el conjunto $G/\mathcal{R}$, la ley-cociente

$$\left(\forall \bar{x}\ \bar{y} \in G / \Re\right) \qquad \bar{x}\,\bar{y} = \overline{xy}$$

define sobre $G/\Re$ una estructura de grupo (se sabe en efecto, que es un monoide donde todo elemento es inversible). $G/\Re$ se denomina ***grupo - cociente*** modulo la relación de equivalencia $\Re$. La aplicación canónica $g : G \to G/\Re$ $[g(x) = \bar{x}]$ es un morfismo subreyectivo de grupos. Para , todos x e y en G:

$$x \equiv y \ (\text{mod } \Re) \Leftrightarrow xy^{-1} \equiv e \ (\text{mod} \Re) \Leftrightarrow xy^{-1} \in \ker (g).$$

Los dos elementos x e y son de la relación $\Re$ si, y solamente si, $xy^{-1} \in \ker(g)$. Se dicen también que son **congruentes módulo el sub-grupo invariante ker (g)**

Bibliografía

-Ayres, F.: Algebra Moderna.
-Doneddu, A.: Algebra y Geometría.
-Gentile, E.: Notas de Álgebra.
-Lentin-Rivaud: Álgebra Moderna
-Pecastaigns, F.: Chemins vers l'Algèbre
-Pinzón, A. Conjuntos y estructuras.
-Queysanne, M.: Algebra Básica.
-Taylor, H- Wade, T.: Matemáticas Básicas.

Ejercicios propuestos.

1.- Demostrar la ley asociativa de la suma de números naturales.

2.- Demostrar que $(\forall n, n \in \mathbf{N})$ $n + 1 = 1 + n$.

3.- Demostrar la ley conmutativa de la suma de números naturales.

4.- Demostrar: $m + n \neq m$ para cualesquiera $m, n \in \mathbf{N}^*$.

5.- Demostrar que $<$ es transitiva, pero no reflexiva ni simétrica.

6.- Demostrar que $0 \leq n$ para todo $n \in \mathbf{N}$.

7.- Demostrar que si : $m, n \in \mathbf{N}$ y $m < n$, entonces para todo $p \in \mathbf{N}^*$, $m + p < n + p$.

8.- Demostrar que: a) $(m + n^{\varphi})^{\varphi} = m^{\varphi} + n^{\varphi}$; b) $(m.n^{\varphi})^{\varphi} = m.n + m^{\varphi}$

9.- Demostrar que si $n, m \in \mathbf{N}$ y $m < n$, $x, y \in \mathbf{R}$ entonces:

a) $x^n.x^m = x^{n+m}$; b) $(x.y)^n = x^n.y^n$; c) $(x^n)^m = x^{n.m}$.

10.- Demostrar que para todo $n \in \mathbf{N}^*$: $\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$.

11.- Demostrar que para todo $n \in \mathbf{N}^*$: $2^n > n$.

12.- Probar que: $8^9 = (16^3)^2.2^3$.

13.- Probar que: $(2^5 - 2^7)^2 = 2^{10}.3^2$.

14.- Probar que: $3^3 < 2^5$.

15.- Calcular:
a) $2^5 + 2^4$; b) $2^5 - 2^4$; c) $2^{n+1} - 2^n$; d) $(3^4.2)^5.(2^4.3)^2$; e) $3^4 - 2^4$; f) $(2^n + 1)^2$.

16.- Analizar la validez de las siguientes afirmaciones:

a) $(2^{2n})^{2k} = 2^{2(n+k)}$; b) $(2^n)^2 = 4^n$; c) $2^{2n}.2^{2n} = 2^{2(n+1)}$.

17.- En cada uno de los casos siguientes, determinar el $t \in \mathbf{N}$ que da lugar a una afirmación verdadera.

a) $3^5.4^5 = 12^t$; b) $9 . 81 = 3^t$; c) $5^t.5^t = 1$; d) $8 . 10^3 = 20^t$.

18.- Demostrar por inducción que para todo $n \in \mathbf{N}$:
a) $1 + 2 + 3 + \ldots + n = \frac{1}{2} n (n + 1)$; b) $1 + 3 + 5 + \ldots + (2n - 1) = n^2$;
c) $1^2 + 2^2 + 3^2 + \ldots + n^2 = 1/6\ n(n + 1)(2n + 1)$; d) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{1}{4} n^2 (n + 1)^2$.

19.- Probar que para todo $n \in \mathbf{N}^*$, $4^n - 1$ es divisible por 3.

20.- Probar que para todo $n \in \mathbf{N}$, $3^{2n+1} + 2^{n+2}$ es múltiplo de 7.

21.- Indique porqué los siguientes conjuntos con la operación definida no son grupos.

a) $a * b = a - b$ en $E = \{0, 1, 2, 3, 4\}$; b) $a + b = a + b$ en $E = \{x / -1 \leq x \leq 1\}, x \in Q$.
c) $a * b = a$ en $E = \{1, 2, 3, 4\}$.

22.- ¿Porqué P(E) no es un grupo con respecto a la $\cup$ y $\cap$?

23.- Verifique que la tabla que sigue no es un grupo.

*	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

24.- Sea G un grupo multiplicativo. Probar :

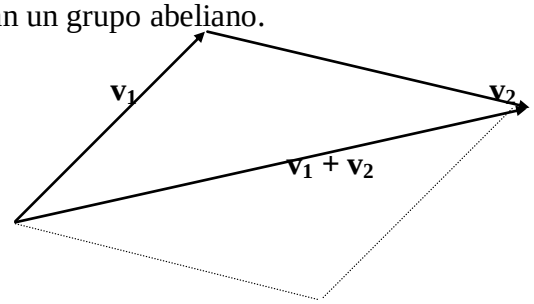
a) $(\forall a, b, c \in G)$ $ab = ac \Leftrightarrow b = c$; b) $(\forall a, b \in G, \exists g, g^{-1} \in G)$, $(a = b.g \wedge a = g^{-1}.b)$
c) $(\forall a, b, c \in G)$, $ab = c \Leftrightarrow b = a^{-1}c$; d) $(\forall a, b, c \in G)$, $aba^{-1} = c \Leftrightarrow ab = ca$

e) $(\forall a, b, c \in G)$, $ab = ba \Leftrightarrow a^{-1}.b^{-1} = b^{-1}.a^{-1}$; f) $(\forall a, b, c \in G)$ $ab = ba \Leftrightarrow aba^{-1}.b^{-1} = 1$ g) $(\forall a, b \in G)$, $(ab)^2 = a^2 b^2$, (G conmutativo); h) $(\forall a, b \in G)$ $aba^{-1} = b$ (G conmutativo).

25.- ¿ Porqué las clases de restos (mod n) no forman con respecto a la multiplicación un grupo?

26.- Establezca las tablas de suma y multiplicación de las clases residuales: mod 4, mod 5 y mod 7, (C_4 , C_5 y C_7). ¿Las tablas de suma conforman la estructura de grupo?. Si se excluye la línea y la columna de ceros, ¿ en qué casos se obtiene una tabla de grupo?.

27.- Si la suma de los vectores $\mathbf{v_1}$ y $\mathbf{v_2}$ se define por la figura, muestre que el conjunto de vectores del plano forman un grupo abeliano.



28.-Muestre que en Z la ecuación $a + x + b = c$ admite la solución única: $x = -a + c - b$.

29.- Resuelva las siguientes ecuaciones en los grupos indicados:

a) En $(Z_5, +)$; $-2 + x + 4 = 1$; b) En $(P(E), \Delta)$; $A \Delta X \Delta A = B$.

30.- Sea $S = R - \{1\}$. Se define una ley sobre S, como $a * b = a + b + ab$. muestre que para esta ley S es un grupo, y halle la solución de la ecuación $2 * x * 3 = 7$ en S.

4.- Anillos y Cuerpos. Números enteros.

4.1.- La estructura de anillo.

4.1.1.- Distributividad.

Consideremos un conjunto E munido de dos leyes de composición, la primera denotada T, la segunda denotada *.

Definiciones.

Se dice que la ley * es *distributiva a izquierda* de la ley T si, cualquiera que sean a, b, c, de E, se tiene

$$a * (b \; T \; c) = (a * b) \; T \; (a * c).$$

Es *distributiva a derecha* si

$$(b \; T \; c) * a = (b * a) \; T \; (c * a).$$

Si es distributiva a izquierda y a derecha, se dice simplemente que la ley * es *distributiva* respecto a la ley T.

OBSERVACIÓN.-

Si la ley * es conmutativa (la ley T no necesariamente) la distributividad de un lado implica evidentemente la distributividad del otro lado.

Ejemplos.

1. En el conjunto P(E) de las partes de E, la unión y la intersección son distributiva la una respecto a la otra:

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

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

2. Sea $(\mathbf{Z},+)$ el grupo aditivo de los enteros y se considera al primer proyector sobre $\mathbf{Z}$: $a * b = a$.

Para todo a, b y c de **Z**, se tiene

$$a * (b + c) = a, \qquad a * b = a, \qquad a * c = a$$

y ya que, $2a \neq a$ (si $a \neq 0$), la ley * no es distributiva a derecha de la adición. Por otra parte,

$$(b + c) * a = b + c, \qquad b * a = b \qquad y \qquad c * a = c,$$

entonces

$$(b + c) * a = (b * a) + (c * a).$$

La ley * es distributiva a derecha de la adición.

4.1.2.- Multiplicación de los enteros naturales.

Los enteros naturales han sido estudiados a partir de los axiomas de Péano. Se debe recordar que el siguiente de un entero natural x es $x^{\varphi} = x + 1$.

Se introduce ahora la multiplicación.

Definición.

A todo par ordenado $(x, y) \in \mathbf{N}^2$, *se le asocia un número natural, denominado producto de x por y, denotado xy, y definido por recurrencia (sobre y) como sigue:*

a) $x.0 = 0.$

b) Se supone definido xy, se define xy^{φ} *por*

$$xy^{\varphi} = xy + x.$$

Para y = 0, se tiene $x.1 = x$ para todo $x \in \mathbf{N}$. Luego 1 es el elemento neutro por derecha. Se puede mostrar que esta multiplicación es conmutativa.

Se muestra ahora que la multiplicación es distributiva a izquierda de la adición (la distributividad a derecha resulta de la conmutatividad), es decir

$$\forall (x, y, z) \in \mathbf{N}^3, \qquad x(y + z) = xy + xz.$$

Se fija arbitrariamente x e y y se razona por recurrencia sobre z. La relación es evidente para z = 0. Se supone que es verdadera para z y se demuestra que lo es para el siguiente z^{φ}. Por definición de la adición y de la multiplicación:

$$x(y + z^{\varphi}) = x(y + z)^{\varphi} = x(y + z) + x.$$

Por hipótesis de recurrencia,

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

La asociatividad de la adición y la definición de la multiplicación dan entonces

$$(xy + xz) + x = xy + (xz + x) = xy + xz^{\varphi}.$$

La distributividad a izquierda queda entonces demostrada.

Se puede también mostrar que la multiplicación es asociativa, luego **N** es un *monoide multiplicativo conmutativo*. Además, todo entero natural salvo el cero, es simplificable y todo entero natural, salvo el 1, no es inversible. Por último se tienen las siguientes relaciones, para todo x, y , z en **N:**

$$x \leq y \quad \Rightarrow \quad xz \leq yz$$

$$(z \neq 0 \quad y \quad x < y) \quad \Rightarrow \quad xz < yz.$$

4.1.3.-Multiplicación de enteros relativos.

Se introdujo a los enteros relativos para resolver el problema de la simetrización en **N**. Se obtuvo el grupo aditivo **Z** de los enteros relativos. Se estudia ahora la multiplicación en **Z**. Pero primero, se introduce la noción de *valor absoluto* (que deberá ser estudiada con mayor detalle en un curso de números reales.

Definición.

Se llama valor absoluto sobre ***Z*** *, a la aplicación de* ***Z*** *en* ***N****, denotada* $\alpha \in N$ *, definida por*

$$\alpha \in N \quad \Rightarrow \quad |\alpha| = \alpha$$

$$\alpha \in N^{-} \quad \Rightarrow \quad |\alpha| = -\alpha$$

Se tiene evidentemente

$$|\alpha| = 0 \Leftrightarrow \alpha = 0.$$

Por definición de adición en **Z**, si α y β *son del mismo signo*, entonces:

$$|\alpha + \beta| = |\alpha| + |\beta|.$$

Se tiene entonces la siguiente definición

Definición.

A todo par ordenado $(\alpha, \beta) \in \mathbf{Z}^2$, *se asocia un entero relativo, denominado producto de* α *por* β, *denotado* $\alpha\beta$ *y definida como sigue:*

1. α *y* β *en* ***N:*** $\alpha\beta$ *es el producto conocido en* ***N;***

2. α *y* β *en* $\mathbf{N}^-$**:** $(-a)(-b) = ab$;

3. $\alpha \in \mathbf{N}^-$ y $\beta \in \mathbf{N}$: $(-a)b = b(-a) = -ab$.

En otros términos:

- El producto de dos números del mismo signo es positivo.
- El producto de dos números de signos diferentes es negativo.
- El valor absoluto del producto es igual al producto de los valores absolutos.

$$|\alpha\beta| = |\alpha||\beta|.$$

La aplicación $\alpha \to |\alpha|$ de $\mathbf{Z}$ en $\mathbf{N}$ es un morfismo para la multiplicación.

Es evidente para esta definición, que la multiplicación en $\mathbf{Z}$ es conmutativa y que admite por elemento neutro al 1.

Asociatividad.

$$\forall(\alpha, \beta, \gamma) \in \mathbf{Z}^3, \qquad (\alpha\beta)\gamma = \alpha(\beta\gamma).$$

En efecto, la igualdad en valor absoluto es válida: esta es la asociatividad en $\mathbf{N}$. Es verdadera también en signo, pues si hay dos números negativos, los productos son positivos de cualquier lado; si hay uno o tres números negativos, los productos son negativos de cualquier lado.

En consecuencia, la multiplicación define en $\mathbf{Z}$ una estructura de *monoide conmutativo.*

Distributividad.

$$\forall(\alpha, \beta, \gamma) \in \mathbf{Z}^3, \qquad \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma .$$

1er caso: β y γ *del mismo signo.* Luego los tres números $\alpha\beta$, $\alpha\gamma$, $\alpha(\beta + \gamma)$ son del mismo signo. La igualdad queda probada en signo. Además, ya que β y γ son del mismo signo, $|\beta + \gamma| = |\beta| + |\gamma|$ y por distributividad en $\mathbf{N}$:

$$|\alpha||\beta + \gamma| = |\alpha||\beta| + |\alpha||\gamma| = |\alpha\beta| + |\alpha\gamma| = |\alpha\beta + \alpha\gamma|$$

(ya que $\alpha\beta$ y $\alpha\gamma$ son del mismo signo). La igualdad en valor absoluto queda probada.

2docaso: β y γ *de signos contrarios.* Entonces $\beta + \gamma$ tiene el signo de uno de los dos, por ejemplo el de β. Observemos que

$$\beta = (\beta + \gamma) + (-\gamma).$$

Los tres números β , $(\beta + \gamma)$ y $(-\gamma)$ son del mismo signo. Por el primer caso,

$$\alpha\beta = \alpha(\beta + \gamma) + \alpha(-\gamma).$$

Para la relación de orden en **Z**, se tienen la siguientes propiedades como resultado inmediato de las definiciones

$$(\gamma \geq 0 \quad \text{y} \quad \alpha \leq \beta) \quad \Rightarrow \quad \alpha\gamma \leq \beta\gamma,$$

$$(\gamma \leq 0 \quad \text{y} \quad \alpha \leq \beta) \quad \Rightarrow \quad \alpha\gamma \geq \beta\gamma$$

Por último, todo entero distinto de cero, es simplificable para la multiplicación.

4.1.4. Estructura de anillo

Definición.

Sea E un conjunto munido de dos leyes de composición internas. Se dice que E es un anillo si

1. la primera ley define sobre E una estructura de *grupo conmutativo*;
2. la segunda ley define sobre E una estructura de *magma asociativo*;
3. la segunda ley es distributiva respecto de la primera.

En un anillo, se denota habitualmente la primera ley aditivamente (grupo conmutativo) y la segunda ley multiplicativamente.

Luego $(E, +, \cdot)$ es un anillo si

a) $(E, +)$ es un grupo conmutativo (de elemento neutro denotado 0);
b) la multiplicación en E es asociativa y distributiva respecto de la adición.

En el caso donde la multiplicación es conmutativa, se dice que el anillo es *conmutativo*.

En el caso donde la multiplicación tiene un elemento neutro (denotado en general por 1) se dice que el anillo es *con unidad*. (La multiplicación define entonces en E una estructura de monoide.)

Ejemplos.

1. De acuerdo a las propiedades que hemos obtenido antes para la adición y la multiplicación de enteros relativos, se puede afirmar que el conjunto **Z** de los enteros relativos, con esa adición y esa multiplicación, es un *anillo conmutativo con unidad***.**

2. El conjunto P de los *enteros pares***,** con la adición y la multiplicación de enteros, es un *anillo conmutativo sin unidad***.**

3. *Anillo nulo.*- Sea (A, +) un grupo conmutativo. Se define sobre A una segunda ley por

$$(\forall a, b \in A) \qquad ab = 0.$$

Con esta nueva ley, A es un anillo conmutativo, denominado *anillo nulo* construido sobre el grupo conmutativo (A, +).

4. {0} es un *anillo unario* (un solo elemento). El elemento neutro 0 de la adición coincide aquí con el elemento neutro de la multiplicación. Es además el único anillo con unidad donde los dos elementos neutros coinciden como lo prueba la siguiente propiedad:

P_1 *Para todo elemento a de un anillo A:*

$$a0 = 0a = 0.$$

En efecto, para todo $b \in A$, $b + 0 = b$ implica

$$a(b + 0) = ab \quad \Rightarrow \quad ab + a0 = ab + 0$$

y como en un grupo todo elemento es simplificable, se obtiene $a0 = 0$. Se muestra de la misma forma, que $0a = 0$.

De lo que resulta si A es con unidad, de elemento neutro multiplicativo 1, con $A \neq \{0\}$, que existe $a \neq 0$ en A tal que

$$a1 = 1a = a,$$

y no se puede tomar $1 = 0$, pues $a \neq 0$; luego $1 \neq 0$.

P_2 *Para cualesquiera elementos a, b de un anillo A:*

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

Para todo b de A, se tiene $b + (-b) = 0$ y, por consiguiente,

$$a(b + (-b)) = ab + a(-b) = a0 = 0.$$

donde $a(-b)$ es el opuesto de ab.

Se puede mostrar de la misma manera que $(-a)b$ es el opuesto de ab.

4.1.5. Sub-anillo

Definición.

Sea A un anillo y H una parte no vacía de A. Se dice que H es sub-anillo de A si las restricciones a H de las dos leyes de A confieren a H la estructura de anillo.

La propiedad siguiente caracteriza a un sub-anillo:

P_3 *Sea A un anillo y* $H \subset A$. *Entonces H es sub-anillo de A si, y solamente si,*

$$1° \quad (a \in H \quad y \quad b \in H) \quad \Rightarrow \quad a - b \in H,$$
$$2° \quad (a \in H \quad y \quad b \in H) \quad \Rightarrow \quad ab \in H.$$

La primera propiedad equivale a decir que (H,+) es sub-grupo conmutativo de A. La segunda equivale a decir que (H, ·) es sub-magma de (A, ·).

Como la asociatividad de la multiplicación y la distributividad en H resultan de las de A la propiedad queda establecida.

Ejemplos.

1. El conjunto P de números pares es un sub-anillo de el anillo **Z** de os enteros relativos.
2. Sea A el anillo nulo construido sobre un grupo conmutativo cualquiera. Todo sub-grupo de este grupo es un sub-anillo de A.

4.1.6. Elementos inversibles.

Sea $A \neq \{0\}$ un anillo con unidad. Entonces la multiplicación confiere a A de la estructura de monoide. Todo elemento inversible de este monoide se denomina *elemento inversible del anillo A.*

Se dijo antes, que el conjunto U de los elementos inversibles de este monoide constituye un grupo multiplicativo. De acuerdo a P_1, el elemento neutro 0 de la adición de A no es inversible. Luego si se toma

$$A^* = A - \{0\}, \text{ se tiene } \quad U \subset A^*-$$

U se denomina *grupo de los elementos inversibles de el anillo A***.**

Ejemplos.

1. En el anillo **Z** de los enteros, U = {-1.+1}.

2. En $\mathbf{Z}^2$, se define ahora una adición y una multiplicación por

$$\forall\ (a, b) \in \mathbf{Z}^2 \qquad (a, b) + (a', b') = (a + a', b + b'),$$
$$\forall\ (a', b') \in \mathbf{Z}^2 \qquad (a, b)(a', b') = (aa', bb').$$

Queda como ejercicio demostrar que $\mathbf{Z}^2$ munido de estas dos leyes es un *anillo conmutativo con elemento unidad* que se denomina *anillo - producto* del anillo $\mathbf{Z}$. El elemento neutro de la adición es (0, 0) y el de la multiplicación es el (1, 1).

El grupo U de los elementos inversibles del anillo-producto $\mathbf{Z}^2$ es

$$U = \{(-1, -1); (-1, 1); (1, -1); (1, 1)\}.$$

OBSERVACIÓN.- Un sub-anillo H de un anillo con unidad A puede se unífero con elemento unidad distinto al del anillo A. Por ejemplo, en $\mathbf{Z}^2$, el conjunto H de los (a, 0) cuando a recorre $\mathbf{Z}$ es un sub-anillo de $\mathbf{Z}^2$ que tiene por elemento unidad al par (1, 0) distinto al elemento unidad (1, 1) de $\mathbf{Z}^2$.

4.1.7. Divisores de cero.

Definiciones.

Sea $A \neq \{0\}$ un anillo. Si existen dos elementos a, b de A tales que

$$a \neq 0, \quad b \neq 0, \quad ab = 0,$$

se dice entonces que a es un divisor de cero por izquierda y que b es un divisor de cero por derecha de el anillo A. Se dice también que a y b son dos divisores de cero.

En el caso donde el anillo A es conmutativo, todo divisor de cero de un lado es divisor de cero de el otro lado.

Ejemplos.

1. $\mathbf{Z}$ no tiene divisores de cero.

2. Se caracteriza en el anillo producto $\mathbf{Z}^2$, al conjunto D de los divisores de cero. Un elemento (a, b) es divisor de cero si $(a, b) \neq (0, 0)$ y si existe $(a', b') \in \mathbf{Z}^2$ tal que $(a', b') \neq (0, 0)$ y

$$(a, b)(a', b') = (0, 0) \quad \Rightarrow \quad (aa' = 0 \ \text{ y } \ bb' = 0).$$

Entonces es necesario que $a = 0$ o $b = 0$.

Recíprocamente, todo (a, 0), con $a \neq 0$, es divisor de cero pues, para todo entero $b' \neq 0$, se tiene

$$(a, 0)(0, b') = (0, 0).$$

Asimismo, todo $(0, b)$ con $b \neq 0$ es divisor de cero. En consecuencia,

$$D = \{(a, b) \in \mathbf{Z}^{2*} / \ a = 0 \quad o \quad b = 0\}.$$

Se tiene la siguiente propiedad:

P_4

Sea un anillo $A \neq \{0\}$ y $a \in A^*$. Luego a es simplificable a izquierda (resp. a derecha) si, y solamente si, a no es divisor de cero por izquierda (resp. por derecha).

Necesidad.

Sea $a \in A$ y a simplificable a izquierda. Entonces,

$$ax = 0 \qquad \Rightarrow \qquad x = 0.$$

Luego a no es divisor de cero a izquierda.

Suficiencia.

Para cualesquiera a, b, c de A*, se tiene

$$ab = ac \qquad \Rightarrow \qquad a\,(b - c) = 0.$$

Entonces, si a no es divisor de cero por izquierda, se deduce que $b - c = 0$, entonces a es simplificable por izquierda. De la misma manera se demuestra para la derecha.

Consecuencia.

Sea un anillo con unidad cualquiera $A \neq \{0\}$. Se a designado por U al grupo de los elementos inversibles y se dijo que todo elemento de U es simplificable. Además $U \subset A^*$ y $U \neq \varnothing$.

Se designa D al conjunto de los divisores de cero de A. Se tiene también que $D \subset A^*$ y $D \cap U = \varnothing$.

Se designa S al conjunto de los elementos *simplificables a derecha y a izquierda* de A que *no son inversibles.* (S puede contener a aquellos elementos inversibles de *un solo lado).* Se tiene $S \subset A^*$ y además $U \cap S = \varnothing$ y $D \cap S = \varnothing$. La propiedad (P_4) lleva a que $A^* = U \cup S \cup D$.

Teorema 1.

Sea un anillo con unidad $A \neq \{0\}$. Si U es el grupo de los elementos inversibles, S el conjunto de los elementos simplificables a derecha y a izquierda que no son inversibles, D el conjunto de los divisores de cero, se tiene

$$A^* = U \cup S \cup D, \quad con \quad U \cap S = S \cap D = D \cap U = \varnothing.$$

OBSERVACIÓN.- Pueden existir en un anillo A divisores de un solo lado que son simplificables y asimismo inversibles por el otro lado. Estos elementos pertenecen a D en el teorema precedente.

4.1.8. Anillo íntegro.

Definición.

Se dice que un anillo A es íntegro si el es distinto de {0} y no posee divisores de cero.

En otros términos, $A \neq \{0\}$ es íntegro si $D = \varnothing$.

Ejemplos.

1. El anillo $\mathbf{Z}$ de los enteros es íntegro.
2. Su anillo producto $\mathbf{Z}^2$ no lo es.

OBSERVACIÓN.-

Si $A \neq \{0\}$ no tiene ningún divisor de cero a derecha (resp. a izquierda), el es íntegro.

P_5 *Sea A un anillo unidad íntegro. Entonces todo elemento inversible de un lado es inversible.*

Sea, por ejemplo, a un elemento de A inversible a derecha. Existe entonces $b \in A$ tal que $ab = 1$ y

$$ab - 1 = 0 \Rightarrow b(ab - 1) = bab - b = (ba - 1)b = 0.$$

Dado que A es integro y $b \neq 0$, entonces b es simplificable y se obtiene $ba - 1 = 0$, luego b es también inverso a izquierda.

Ejemplos.

1.- Probar que $\frac{1}{2} \notin \mathbf{Z}$.

Solución: Dado que $1 < 2 \Rightarrow \frac{1}{2} < 1$. Como $0 < \frac{1}{2}$, se tiene que $0 < \frac{1}{2} < 1$. y esto significa que $\frac{1}{2} \notin \mathbf{Z}$.

2.- Mostrar que $-\frac{1}{2} \notin \mathbf{Z}$.

Solución: Si suponemos que $-\frac{1}{2} \in \mathbf{Z}$, entonces tendría que ser $\frac{1}{2} = -(-\frac{1}{2}) \in \mathbf{Z}$ que, de acuerdo al ejemplo 1, no es cierto.

3.- $\mathbf{Z}$ no es un conjunto bien ordenado.

Para que un conjunto sea bien ordenado, toda parte del mismo debe tener primer elemento. En $\mathbf{Z}$ el subconjunto $\mathbf{N}^-$, no tiene primer elemento, ya que: si $n \in \mathbf{N}^-$, entonces $n = -a$, $a \in \mathbf{N}$. Como $a < a + 1$, sera $-(a + 1) < -a = n$. Como $-(a + 1) \in \mathbf{N}^-$, n no es primer elemento de $\mathbf{N}^-$. Por consiguiente no tiene primer elemento.

4.1.9. Cuerpo. Sub-cuerpo.

Definición.

Se llama cuerpo a un anillo unidad donde todo elemento no nulo es inversible.

En otros términos, un anillo unidad A es un cuerpo si, y solamente si,

$$A^* = U.$$

(Los conjuntos S y D del teorema 1 son vacíos.)

Si A es conmutativo, se dice que el cuerpo es conmutativo.

Ejemplos.

1. El cuerpo **Q** de los números racionales
2. El cuerpo **R** de los números reales
3. El cuerpo **C** de los números complejos.

Definición.

Sea K un cuerpo y $H \subset K$ $(H \neq \varnothing)$. Se dice que H es sub-cuerpo de K si las restricciones a H de las dos leyes de K confieren a H de la estructura de cuerpo.

Los sub-cuerpos se caracterizan inmediatamente por la propiedad siguiente:

P_6 *Sea K un cuerpo y $H \subset K$ $(H \neq \varnothing)$. Entonces H es sub-cuerpo de K si, y solamente si, para cualesquiera a y b,*

$$(a \in H \quad y \quad b \in H) \quad \Rightarrow \quad a - b \in H,$$
$$(a \in H \quad y \quad b \in H - \{0\}) \quad \Rightarrow \quad ab^{-1} \in H.$$

Ejemplo.- El conjunto **R** es sub-cuerpo de **C** y **Q** es sub-cuerpo de **R** entonces de **C**.

P_7 *Sea A un anillo con unidad donde todo elemento no nulo es inversible por derecha (resp. por izquierda). Entonces A es un cuerpo.*

Se supone que, para todo $a \in A^*$, existe $b \in A$ tal que $ab = 1$. Sea $ca = 0$ con $a \neq 0$. Luego

$$0 = (ca)b = c(ab) = c.$$

Luego *todo* elemento a de A^* no es divisor de cero a derecha. Se puede decir que A^* es íntegro. Es suficiente aplicar la propiedad (P_5) para ampliar la demostración.

4.2. Ideal de un anillo.

4.2.1. Ideal por derecha (resp. por izquierda).

Definición.

Sea A un anillo. Un ideal por derecha (resp. por izquierda) de A es una parte J de A tal que

$$1.\ (a \in J \quad y \quad b \in J) \quad \Rightarrow \quad a - b \in J,$$
$$2.\ (a \in J \quad y \quad x \in A) \quad \Rightarrow \quad ax \in J \quad (resp.\ xa \in J).$$

En otros términos, J es un ideal por derecha (resp. por izquierda) de A si

1. J es sub-grupo aditivo de A
2. $JA \subset J$ (resp. $AJ \subset J$).

Ejemplo.- Sea A un anillo cualquiera y $a \in$ A. Entonces aA es ideal a derecha. En efecto, si x e y pertenecen a aA, existen x' e y' en A tales que $x = ax'$ e $y = ay$, de donde

$$x - y = a(x' - y') \in aA ,$$

y la condición (1) se verifica. Ahora, para todo $z \in A$,

$$xz = a(x'z) \in aA$$

y la condición (2) se verifica.

Asimismo Aa es ideal por izquierda de A.

OBSERVACIÓN.- Todo ideal a derecha (resp. a izquierda) de A es un sub-anillo de A. Pero la recíproca es falsa. Por ejemplo, si $A = \mathbf{Q_{10}}$ es el anillo de los números decimales, entonces $\mathbf{Z}$ es un sub-anillo de $\mathbf{Q_{10}}$ pero no es un ideal de $\mathbf{Q_{10}}$ (por ejemplo, $3 \in \mathbf{Z}$ y $1/10 \in \mathbf{Q_{10}}$, con $3 \times 1/10 \notin \mathbf{Z}$).

P8 *La intersección de una familia de ideales a derecha (resp. a izquierda) de un anillo A es un ideal a derecha (resp. a izquierda) de A.*

Sea $(J_\lambda)_{\lambda \in L}$ una familia de ideales, por ejemplo por derecha, de un anillo A. Se toma

$$H = \bigcap_{\lambda \in L} J_\lambda .$$

Se dijo antes que H es un sub-grupo aditivo de A. Ahora, para todo $a \in H$, se tiene

$$(\forall \lambda \in L) \qquad a \in J_\lambda$$

Como J_λ es un ideal a derecha, entonces para todo $x \in A$, tiene que ser $ax \in J_\lambda$ (para todo $\lambda \in L$), de donde $ax \in H$, que es entonces un ideal por derecha de A.

P9 *Sea J y $\mathcal{G}$ dos ideales a derecha (resp. a izquierda) de un anillo A. Entonces $J + \mathcal{G}$ es un ideal a derecha (resp. a izquierda) de A.*

En efecto, si x e y pertenecen a $J + \mathcal{G}$, existen a y b en J y existen a' y b' en $\mathcal{G}$ tales que

$$x = a + a' \qquad e \qquad y = b + b',$$

luego

$$x - y = (a - b) + (a' - b') \in J + \mathcal{G}$$

Por otra parte, si por ejemplo J y $\mathcal{G}$ son dos ideales por derecha, para todo $z \in A$, se tiene

$$az \in J \qquad y \qquad a'z \in \mathcal{G}$$

y, por consiguiente,

$$xz = (a + a')z = az + a'z \in J + \mathcal{G}$$

que demuestra la propiedad.

Consecuencia.

Si J_1, J_2, ..., J_n es una familia finita de ideales a derecha (resp. a izquierda) de un anillo A, entonces $J_1 + J_2 + ... + J_n$ es un ideal a derecha (resp. a izquierda) de A.

4.2.2. Ideal engendrado por una parte

Sea P una parte no vacía de un anillo A se estudia ahora el conjunto , denotado J(P), definido como sigue:

J(P) es el conjunto de los elementos x de el anillo A que tienen la siguiente propiedad: existe $n \in N^*$, una sucesión $a_1, a_2, ..., a_n$ de n elementos de P y una sucesión $x_1, x_2, ..., x_n$ de n elementos de A tales que $x = a_1 x_1 + a_2 x_2 + ... + a_n x_n$.

Se muestra que J(P) es un ideal a derecha de A.

1° $(x \in J(P)$ y $y \in J(P)) \Rightarrow x - y \in J(P)$.

En efecto , por hipótesis,

$$x = a_1 x_1 + ... + a_n x_n. \quad \text{e} \quad y = b_1 y_1 + ... + b_p y_p,$$

con los n + p elementos $a_1, ..., a_n, b_1, ..., b_p$ en P y los n + p elementos $x_1,..., x_n, y_1, ..., y_n$ en A. De ello resulta

$$x - y = a_1 x_1 + ... + a_n x_n. + b_1 (-y_1) + ... + b_p(-y_p) \in J(P).$$

2° $(x \in J(P)$ y $z \in A) \Rightarrow xz \in J(P)$,

pues

$$xz = a_1(x_1 z) + ... + a_n(x_n z) \in J(P).$$

J(P) es entonces un ideal a derecha de A.

Teorema 2.

Sea A un anillo y P una parte no vacía de A. El conjunto J(P) de elementos x de el anillo A definido como sigue:

"Existe un entero $n > 0$, una sucesión $a_1 ,..., a_n$ de n elementos de P y una sucesión $x_1, ..., x_n$, de n elementos de A tales que $x = a_1 x_1 + ... * a_n x_n$ " es un ideal a derecha de A.

Definición.

J(P) se denomina ideal a derecha de A engendrado por la parte P.

Se define asimismo el ideal por izquierda de A engendrado por la parte P. En el caso donde P se reduce a un singleton $\{a\}$, el ideal a derecha engendrado por a es evidentemente aA. Asimismo el ideal a izquierda engendrado por a es Aa.

4.2.3. Ideal de un anillo con unidad.

Si A es *con unidad*, entonces, para toda parte P de A, se tiene

$$P \subset J(P).$$

En efecto,

$$(a \in P \quad y \quad 1 \in A) \quad \Rightarrow \quad a = a1 \in J(P).$$

En este caso, J(P) es el *ideal más pequeño a derecha* que contiene a P. En efecto, sea H un ideal a derecha de A que verifique que $H \supset P$. Entonces para todas las sucesiones $a_1, \ldots a_n$ de elementos de P (entonces de H) y $x_1, \ldots, x_n$ de elementos de A, el elemento $a_1x_1 + \ldots + a_nx_n \in H$. Luego $H \supset J(P)$.

Por consiguiente, J(P) es la intersección de la familia de todos los ideales a derecha de A que contienen P.

P10 *Sea A un anillo unífero (con unidad). Para toda parte no vacía P de A, se tiene $P \subset J(P)$ y J(P) es el ideal más pequeño a derecha de A conteniendo a P. En particular, el ideal más pequeño a derecha (resp. a izquierda) conteniendo a es aA (resp. Aa)*

4.2.4. Ideal bilateral.

Definición.

Se llama ideal bilateral de un anillo A a un ideal a derecha y a izquierda de A.

En otros términos, J es un ideal bilateral de A si

1. J es sub-grupo aditivo de A.
2. $JA \subset J$ y $AJ \subset J$.

Si el anillo A es conmutativo, una de las inclusiones dadas en (2) implica la otra. En este caso, todo ideal de A es bilateral.

Ejemplos.

1. {0} es ideal bilateral de todo anillo A.
2. A es ideal bilateral de todo anillo A.
3. Para todo elemento a de un anillo A que verifique que $aA = Aa$, el ideal aA es bilateral. (La hipótesis $Aa = aA$ significa que, para todo $x \in A$ existe $y \in A$ tal que $ax = ya$, y para todo $y \in A$, existe $x \in A$ tal que $ya = ax$.)

4.2.5. Ideal principal. Anillo principal.

Definición.

Sea A un anillo. Un ideal J de A se dice principal si existe un $a \in A$ tal que $J = aA = Aa$

.

Un ideal principal es entonces *bilateral.*

Ejemplo.- El conjunto {0} es un ideal principal de todo anillo A.

En el caso donde A no es conmutativo, un ideal principal es un ideal del tipo aA. En el caso donde A no es conmutativo pero es con unidad, entonces si aA y Aa son bilaterales se tiene $aA = Aa$ (y aA es entonces principal). En efecto, $a \in (Aa)$ y como aA es bilateral, se deduce $aA \subset Aa$. Asimismo, $a \in Aa$ implica $aA \subset Aa$. (Existen casos donde aA es bilateral con $aA \subset Aa$.)

Definición.

Un anillo A se dice principal si todo ideal de A es principal.

A título de ejercicio, se demuestra la siguiente propiedad:

P_{11} *Todo anillo principal es con unidad.*

En efecto, A es ideal bilateral de A. Como A es principal, existe $a \in A$ tal que $aA = Aa = A$. Se puede decir que las aplicaciones f y g de A en A,

$$f(x) = ax \qquad y \qquad g(x) = xa,$$

son *sobreyectivas.* Existen en consecuencia $e \in A$ y $\omega \in A$ tales que

$$ae = a \qquad y \qquad \omega a = a.$$

Ahora, para todo $y \in A$, existe $x \in A$ tal que

$$y = ax \quad \Rightarrow \quad \omega y = (\omega a)x = ax = y$$

existe $x' \in A$ tal que

$$y = x'a \quad \Rightarrow \quad ye = x'(ae) = x'a = y.$$

En resumen, para todo $y \in A$,

$$\omega\, y = y \qquad \text{y} \qquad ye = y.$$

Tomando $y = e$ en la primera relación y $y = \omega$ en la segunda, se obtiene

$$\omega\, e = e \qquad \text{y} \qquad \omega\, e = \omega$$

y, en consecuencia, $\omega = e$, que es elemento neutro de la multiplicación. La propiedad queda demostrada

4.3.- El anillo principal de los enteros.

4.3.1.- División euclidiana en **Z**.

En lo que sigue "a" es un número entero ($a \in \mathbf{Z}$) y "b" es un número natural, $b \neq 0$, $b \in \mathbf{N}$).

Teorema.

Para todo par $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$, existe un y sólo un entero $q \in \mathbf{Z}$ tal que:

$$bq \leq a < b(q + 1)$$

- -Unicidad.

Si existieran dos enteros q y q' tales que:

$$bq \leq a < b(q + 1) \quad \text{y} \quad bq' \leq a < b(q' + 1)$$

por transitividad;

$$bq < b(q' + 1) \Rightarrow q < q' + 1 \Rightarrow q - q' < 1 \Rightarrow q' - q > -1$$

$$bq' < b(q + 1) \Rightarrow q' < q + 1 \Rightarrow q' - q < 1 \Rightarrow q' - q < 1$$

o sea,

$$-1 < q' - q < 1 \Rightarrow q' - q = 0 \Rightarrow q = q'$$

- - Existencia.

Si a = 0, se tiene q = 0, sin dudas.

1.- Si $a > 0$, consideremos $A = \{n \in \mathbf{N} / bn > a\}$. A no es vacío (por ejemplo $a + 1 \in A$. Entonces A admite un elemento mínimo (al menos igual a 1) que se puede denotar $q + 1$ con $q \in \mathbf{N}$. Se tiene evidentemente $q + 1 \in A$, luego $b(q + 1) > a$. Se tiene también que $bq \leq a$, o si no $bq > a$ implicaría que $q \in A$ y contradice que $q + 1 = \text{mín } A$.

2.- Por último suponemos $q < 0$. Luego $(- a) > 0$ y, de acuerdo a lo anterior, existe un $q' \in \mathbf{N}$ tal que,

$$bq' \leq -a < b(q' + 1) \Rightarrow b(- q' - 1) < a \leq b(-q').$$

Si $- a = bq'$, se toma $q = - q'$ y queda demostrada la existencia. O si no, $q = - q' - 1$ y la existencia está demostrada.

Corolario

Para todo par $(a, b) \in \mathbf{Z} \times \mathbf{N^*}$, existe un y sólo un par $(q, r) \in \mathbf{Z}^2$ tal que:

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

Definiciones

Determinar el par (q, r) es efectuar la división euclidiana de a por b. Al número a se le llama dividendo, al b divisor, al q el cociente euclidiano, y a r el resto.

El teorema anterior caracteriza al cociente euclidiano y

$$bq \leq a < b(q + 1) \Rightarrow 0 \leq a - bq < b$$

Recíprocamente, si se tiene $a = bq + r$ y $0 \leq r < b$, entonces

$$0 \leq a - bq < b \Rightarrow bq \leq a < b(q + 1).$$

4.3.2.- Sub-grupos aditivos de **Z**. Ideales de **Z**.

Sea $a \in \mathbf{Z}$. La parta $a\mathbf{Z}$ es un sub-grupo aditivo de $\mathbf{Z}$ pues,

$$(\forall x, y \in \mathbf{Z}) \qquad ax - ay = a(x - y) \in a\mathbf{Z}$$

Recíprocamente, para todo sub-grupo aditivo H de $\mathbf{Z}$, se mostrará que existe un $a \in \mathbf{Z}$ tal que $H = a\mathbf{Z}$.

Si $H = \{0\}$, entonces $a = 0$. Si $H \neq \{0\}$, designaremos por A la parte de H definida como sigue:

$$A = \{x \in H / x > 0\}$$

A es una parte no vacía de **N**. Entonces admite un elemento mínimo a = mínA. Se tiene $a \in A$, luego $a > 0$. Además, se tiene $a\mathbf{Z} \subset H$, ya que $a \in H$ y que $a\mathbf{Z}$ es un grupo monógeno engendrado por a.

Sea $x \in H$. Efectuamos la división euclidiana de x por a:

$$x = aq + r; \qquad 0 \leq r < a.$$

Se tiene $x \in H$ y $aq \in a\mathbf{Z} \subset H$, entonces $x - aq = r \in H$.

Si se supone $r > 0$, luego $r \in A$ y $r <$ mín A (contradicción).

En consecuencia $r = 0$ y $H = a\mathbf{Z}$.

Teorema.

Todo sub-grupo del grupo aditivo **Z** *de los enteros es del tipo* $a\mathbf{Z}$, *con* $a \in \mathbf{Z}$.

Corolario.

El anillo **Z** *de los enteros es principal. (Todo ideal de* **Z** *es principal).*

En efecto, todo sub-grupo aditivo de **Z** es del tipo $a\mathbf{Z}$, y en consecuencia todo ideal de **Z** es de este tipo, luego es principal. Entonces **Z** es un anillo principal.

OBSERVACIÓN.- Para todo $a \in \mathbf{Z}$, $a\mathbf{Z}$ es un ideal de **Z**, entonces subanillo de **Z**. Pero para $a \neq \pm 1$, el anillo $a\mathbf{Z}$ no es principal pues no será unífero.

4.3.3.- Divisibilidad. Múltiplos. m.c.m..

Definición.

Sean dos enteros a y b. Si existe $q \in \mathbf{Z}$ tal que $a = bq$, se dice que b divide a, o que a es múltiplo de b. Se denota $b|a$.

El conjunto de los múltiplos de b es evidentemente $b\mathbf{Z}$. Por definición:

$$b|a \Leftrightarrow a \in b\mathbf{Z}.$$

P_{12}

$$b|a \Leftrightarrow a\mathbf{Z} \subset b\mathbf{Z}$$

En efecto, si b|a, entonces todo múltiplo de a es múltiplo de b de donde

$$a\mathbf{Z} \subset b\mathbf{Z}.$$

Recíprocamente, si se verifica esta inclusión entonces, $a \in a\mathbf{Z}$, luego $a \in b\mathbf{Z}$. y b|a.

- -Para todo $a \in \mathbf{Z}$, se tiene 1|a, a|a, a|0.
- $b \neq 0$ divide a, si, y solamente si, la división euclidiana de a por | b | da un resultado nulo.

Además se tiene

$$(a|b \text{ y } b|a) \Rightarrow a = \pm b$$
$$(a|b \text{ y } b|c) \Rightarrow a|c$$

- ***<u>Mínimo común múltiplo de dos enteros</u>***.

*Sean a y b dos enteros. Se llama común múltiplo de a y de b a todo elemento de la intersección de $a\mathbf{Z} \cap b\mathbf{Z}$. Esta intersección es un ideal de **Z**. Ya que **Z** es principal, existe un entero natural $m \in \mathbf{N}$ y uno solo tal que:*

$$a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$$

<u>Definición</u>.

Al entero natural m se le llama **<u>mínimo común múltiplo</u>** de a y b y se denota

$$m = \text{m.c.m.}(a, b) \quad \text{o} \quad m = a \left) \overline{m}\, b$$

Se define así una ley de composición de $\mathbf{Z}^2 \to \mathbf{N}$, con $(a, b) \to a \left) \overline{m}\, b$ que es conmutativa. Se se cambia el signo de a o de b, el resultado no cambia. Para todo $a \in \mathbf{Z}$, se tiene

$$a \left) \overline{m}\, 1 = |\, a \,| \quad \text{y} \quad a \left) \overline{m}\, 0 = 0.$$

<u>Ejemplo</u>: Hallar el mínimo común múltiplo de 8 y 14.

Solución: Escribimos los múltiplos de 8 y 14 y buscamos el menor común a ambos.

8: 8, 16, 24, 32, 40, 48, 56, ...

14: 14, 28, 42, 56, 72, ...

Se tiene entonces que: $56 = \text{m.c.m.}(8, 14) = 8 \left) \overline{56}\, 14$

- ***mínimo común múltiplo de varios enteros***.

En forma mas general, sea una familia finita de enteros $\{a_1; a_2; \cdots, a_n\}$. Se llama común múltiplo de estos n enteros a todo elemento de la intersección

$$a_1\mathbf{Z} \cap a_2\mathbf{Z} \cap \cdots \cap a_n\mathbf{Z}.$$

Como esta intersección es un ideal de el anillo principal **Z**, existe entonces un entero natural $m \in \mathbf{N}$ (y uno solo) tal que

$$a_1\mathbf{Z} \cap a_2\mathbf{Z} \cap \cdots \cap a_n\mathbf{Z} = m\mathbf{Z}$$

Definición

Al entero natural m se le llama mínimo común múltiplo de los enteros a_1**;** a_2; $\cdots$ a_n. y se denota $m = m.c.m.(a_1; a_2; \cdots a_n)$.

Se puede ver que el conjunto de los múltiplos de dos o varios números coincide con el conjunto de los múltiplos de sus m.c.m.

4.3.4.- Divisores comunes. M.C.D..

Sea $a \in \mathbf{Z}$. Se designara por D(a) al conjunto de los divisores de a

$$D(a) = \{x \in \mathbf{Z} / x \mid a\}.$$

Si a = 0, se tiene D(0) = **Z**. Si $a \neq 0$, D(a) es finito y no contiene al 0. Por ejemplo

$$D(12) = \{ \pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 12\}.$$

Sean a y b dos enteros. Se llama ***divisor común de a y b*** a todo elemento de la intersección: $D(a) \cap D(b)$.

P_{13}

$$\delta \in D(a) \cap D(b) \Leftrightarrow a\mathbf{Z} + b\mathbf{Z} \subset \delta\mathbf{Z}$$

En efecto, si δ es un divisor común de a y de b entonces $a\mathbf{Z} \subset \delta\mathbf{Z}$ y $b\mathbf{Z} \subset \delta\mathbf{Z}$ (ver propiedad anterior, P_{12}), de donde $a\mathbf{Z} + b\mathbf{Z} \subset \delta\mathbf{Z}$.

Recíprocamente, si se dá la inclusión, entonces $a\mathbf{Z} \subset a\mathbf{Z} + b\mathbf{Z} \subset \delta\mathbf{Z}$ y δ divide a. Asimismo δ divide b.

Ahora, ya que todo ideal de **Z** es principal, existe un entero natural $d \in \mathbf{N}$ (y uno solo) tal que:

$$a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z} \qquad (1)$$

De acuerdo a la propiedad anterior, de es un común divisor de a y de b. Además δ es un divisor común de a y de b, si y solamente si, $d\mathbf{Z} \subset \delta\mathbf{Z}$, de donde δ divide a d. El conjunto de los comunes divisores de a y de b, coinciden con el conjunto de los divisores de d.

Definición.

Al entero natural definido por (1) se le denomina ***máximo común divisor*** *de a y de b y se denota* $d = M.C.D.(a, b)$ *o también* $d = a \overline{\wedge M} b$.

Teorema.

El conjunto de los divisores comunes de dos enteros coincide con el conjunto de los divisores de su M.C.M..

$$D(a) \cap D(b) = D(a \overline{\wedge M} b)$$

Se tiene así una ley de composición de $\mathbf{Z}$ en $\mathbf{N}$, con $(a, b) \rightarrow a \overline{\wedge M} b$, que es conmutativa, y si se cambia el signo de a o de b, el resultado $a \overline{\wedge M} b$ no cambia. Para todo $a \in \mathbf{Z}$, se tiene

$$a \overline{\wedge M} 0 = |a| \qquad y \qquad a \overline{\wedge M} 1 = 1$$

Algoritmo de Euclide.

Consiste en un procedimiento para el cálculo práctico del M.C.D.(a, b)

Lema 1.

Sean a y b dos enteros. Para todo entero q, tomamos $r = a - bq$.
Entonces:

$$a \overline{\wedge M} b = b \overline{\wedge M} a$$

En efecto, $r = a - bq$ pertenece al ideal $a\mathbf{Z} + b\mathbf{Z}$, entonces $a \overline{\wedge M} b$ divide a r y como divide también a b, entonces $a \overline{\wedge M} b$ divide a $b \overline{\wedge M} r$. Como r y a juegan el mismo rol, se tiene también $b \overline{\wedge M} r$ divide a $a \overline{\wedge M} b$.

Para el cálculo del M.C.D.(a, b), se puede acotar al caso donde a y b sean dos enteros naturales no nulos. El Algoritmo de Euclide consiste en efectuar las divisiones euclidianas sucesivas.

Suponemos $a \geq b$ y efectuamos la división euclidiana de a por b:

$$a = bq_1 + r_1;\ 0 \leq r_1 < b.$$

Por le lema 1, se tiene $a\overline{\bigwedge M}\ b = b\overline{\bigwedge M}\ r_1$. Se reemplaza el par (a, b) por el par (b, r_1) constituida por enteros naturales más pequeños. Se reitera el procedimiento sobre (b, r_1). Se efectúa así las divisiones euclidianas sucesivas:

$$\begin{aligned} b &= r_1q_2 + r_2 \qquad 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 \qquad 0 \leq r_3 < r_2 \end{aligned}$$

Con

$$a\overline{\bigwedge M}\ b = b\overline{\bigwedge M}\ r_1 = r_1\overline{\bigwedge M}\ r_2 = r_2\overline{\bigwedge M}\ r_3 = \cdots$$

La sucesión $r_1, r_2, r_3, \cdots$, es estrictamente decreciente en **N**, entonces finita. Existe en consecuencia un número natural n (el cardinal de esta sucesión) tal que $r_n = 0$

Entonces:

$$r_{n-2} = r_{n-1}q_n + 0$$

prueba que $a\overline{\bigwedge M}\ b = r_{n-2}\overline{\bigwedge M}\ r_{n-1} = r_{n-1}$.

El M.C.D. de a y de b es el último resto no nulo del algoritmo.

Ejemplo. Halllemos el máximo común divisor de 234 y 129, haciendo las divisiones sucesivas y usando el algoritmo de la división, podemos escribir:

$$\begin{aligned} 234 &= 129 \cdot 1 + 105 \\ 129 &= 105 \cdot 1 + 24 \\ 105 &= 24 \cdot 1 + 9 \\ 24 &= 9 \cdot 2 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 \end{aligned}$$

Es decir el máximo común divisor de 234 y 129 es el número 3.

4.3.5.- Enteros primos entre sí.

Definición.

Dos enteros a y b se dicen ***primos entre sí****, si* $a\overline{\bigwedge M}\ b = 1$, *(M.C.D.(a, b) = 1).*

Que es equivalente a decir que el ideal engendrado por a y b es **Z**:

$$a\overline{\bigwedge M}\ b = 1 \quad \Leftrightarrow \quad a\mathbf{Z} + b\mathbf{Z} = \mathbf{Z}.$$

***Teorema de Bezout*.**

Dos enteros a y b son primos entre sí, y solo sí, existen dos enteros x e y tales que

$$ax + by = 1.$$

En efecto, si $a\mathbf{Z} + b\mathbf{Z} = \mathbf{Z}$, luego $1 \in \mathbf{Z}$ muestra que existen dos enteros x e y tales que $ax + by = 1$.

Recíprocamente, si tales enteros x e y existen, será $1 \in a\mathbf{Z} + b\mathbf{Z}$ y éste ideal que contiene al 1, coincide con **Z**.

Lema 2.

Para cualesquiera a, b, c:

$$ca \left(\overline{M}\right. cb = |c| \cdot (a \left(\overline{M}\right. b).$$

En efecto, si $I = a\mathbf{Z} + b\mathbf{Z}$ es el ideal engendrado por a y b, entonces cualquiera que sea el entero c, el ideal engendrado por ca y cb es el conjunto de los $cax + cby = c(ax + by)$, cuando x e y recorren **Z**, luego coincide con cI:

$$ca\mathbf{Z} + cb\mathbf{Z} = c(a\mathbf{Z} + b\mathbf{Z}) = c\cdot(a \left(\overline{M}\right. b)\mathbf{Z}.$$

Teorema de la divisibilidad.

Si "a" *divide a* "bc" *y si* "a" *es primo con* "b", *entonces* "a" *divide a* "c". Será:

$$a \left(\overline{M}\right. b = 1 \;\Rightarrow\; ca \left(\overline{M}\right. cb = |c|$$

Dado que "a" divide "bc", y como divide a "ac", divide entonces $ca \left(\overline{M}\right. cb = |c|$.

Ahora, consideremos dos enteros a y b no nulos; sea $d = a \left(\overline{M}\right. b$ e introducimos los cocientes exactos α y β de a y de b por d:

$$a = d\alpha \quad y \quad b = d\beta.$$

Calculamos $\delta = \alpha \left(\overline{M}\right. \beta$.

Será:

$$d\alpha \left(\overline{M}\right. d\beta = d\delta \;\Rightarrow\; d = d\delta \;\Rightarrow\; \delta = 1.$$

Se enuncia entonces la siguiente propiedad:

P_{14}

Los cocientes (exactos) de dos enteros no nulos a y b por a $\wr$ b son primos entre sí.

Sea $m = a \wr b = m.c.m.(a, b)$. Se introducen los cocientes exactos α y β de m por a y b.

$$m = a\alpha = b\beta.$$

Calculamos $\delta = \alpha \wr \beta$. Se introducen los enteros α', β', m' tales que:

$$\alpha = \delta\alpha', \beta = \delta\beta' \text{ y } m = \delta m'.$$

Se tiene $m' \mid m$. Además

$$m' = a\alpha' = b\beta' \Rightarrow m' \in a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z} \Rightarrow m \mid m'.$$

En consecuencia $m = m'$ y $\delta = 1$ y se tiene:

P_{15} Sean a y b dos enteros no nulos. Los cocientes (exactos) de $a \wr b$, por a y b son primos entre sí.

Consecuencia.

De acuerdo a las notaciones precedentes, para todo entero k, se tiene

$$km = (k\alpha)a = (k\beta)b$$
$$\alpha \wr \beta = 1 \Rightarrow k\alpha \wr k\beta = |k|.$$

Dado que el producto ab es múltiplo común de a y de b, existe $k \in \mathbf{Z}$ tal que

$$ab = mk.$$

Para ese k, se tiene $k\alpha = b$ y $k\beta = a$, de donde $k\alpha \wr k\beta = b \wr a = |k|$. Se puede entonces enunciar lo siguiente:

P_{16} El valor absoluto del producto de dos enteros es igual al producto de sus M.C.D. por sus m.c.m.

$$(a \wr b)(a \wr b) = |ab|.$$

Esta relación es verdadera asimismo, si a o b son nulos.

4.3.6.- Divisores comunes de varios enteros.

Sea una familia finita de enteros $\{a_1, a_2, \cdots, a_n\}$. Se llama divisor común de estos n enteros a todo elemento de la intersección:

$$D = D(a_1) \cap D(a_2) \cap \cdots \cap D(a_n).$$

Se introduce el ideal engendrado por $a_1, \cdots, a_n$

$$I = a_1\mathbf{Z} + a_2\mathbf{Z} + \cdots + a_n\mathbf{Z},$$

y generalizando la propiedad 13:

$$\delta \in D \Leftrightarrow I \subset \delta\mathbf{Z} \qquad (2)$$

En efecto, si δ es un divisor común de $a_1, \cdots, a_n$, entonces (P_{12}) $a_i\mathbf{Z} \subset \delta\mathbf{Z}$, $(1 \le i \le n)$ y por consiguiente la suma de los ideales $a_i\mathbf{Z}$ está incluido en $\delta\mathbf{Z}$**:**

$$I = a_1\mathbf{Z} + a_2\mathbf{Z} + \cdots + a_n\mathbf{Z} \subset \delta\mathbf{Z}$$

Recíprocamente, si esta inclusión tiene lugar, como

$$(1 \le i \le n) \qquad a_i \in a_i\mathbf{Z} \subset I \subset \delta\mathbf{Z}$$

se tiene $\delta \mid a_i$ $(1 \le i \le n)$ y δ es un divisor común de $a_1, \cdots, a_n$.

Ahora, ya que todo ideal de $\mathbf{Z}$ es principal, entonces I es principal y existe un entero natural $d \in \mathbf{N}$ (y uno solo) tal que

$$a_1\mathbf{Z} + a_2\mathbf{Z} + \cdots + a_n\mathbf{Z} = d\mathbf{Z}. \qquad (3)$$

Por (2) , de es un divisor común de $a_1, \cdots, a_n$. Además, para que δ sea una un divisor común de $a_1, \cdots, a_n$, es necesario y es suficiente por (2), que $d\mathbf{Z} \subset \delta\mathbf{Z}$, de donde $\delta \mid d$.

Definición.

Al entero natural d definido por (3) se le denomina *máximo común divisor* de los n enteros $a_1, a_2, \cdots, a_n$ y se denota $MCD(a_1, a_2, \cdots, a_n)$.

Se a obtenido el siguiente teorema:

Teorema 6.

El conjunto de los divisores comunes de varios números coincide con el conjunto de los divisores de su MCD.

Dado que la adición de ideales es asociativa, se puede afirmar que la ley de composición en **Z**, $(a, b) \to a \overline{)M}\, b$ es asociativa y se denota:

$$MCD\,(a_1, a_2, \cdots, a_n) = a_1 \overline{)M}\, a_2 \overline{)M} \cdots \overline{)M}\, a_n.$$

Para el cálculo práctico del MCD, se calculan sucesivamente:

$$d_2 = a_1 \overline{)M}\, a_2; \qquad d_3 = d_2 \overline{)M}\, a_2, \cdots,$$

hasta que

$$d_n = d_{n-1} \overline{)M}\, a_n = MCD(a_1, a_2, \cdots, a_n).$$

Enteros primos entre si.

Se dice que los enteros $a_1, a_2, \cdots, a_n$ son primos entre sí; si $MCD(a_1, a_2, \cdots, a_n) = 1$.

Por ejemplo los tres enteros 6, 10, 15 son primos entre sí.

Si entre los n enteros $a_1, a_2, \cdots, a_n$ dos enteros son primos entre sí, entonces, cualesquiera que sean los $n - 2$ restantes, los n enteros son primos entre si.

Teorema de Bezout.

Los n enteros $a_1, a_2, \cdots, a_n$ son primos entre ellos, si, y solamente si, existen n enteros $x_1, x_2, \cdots, x_n$ tales que

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 1$$

En efecto, si $a_1\mathbf{Z} + a_2\mathbf{Z} + \cdots + a_n\mathbf{Z} = \mathbf{Z}$, entonces 1 pertenece a **Z** muestra que existen n enteros $x_1, x_2, \cdots, x_n$ tales que $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 1$.

Recíprocamente, si existen n enteros, entonces se tiene $1 \in a_1\mathbf{Z} + a_2\mathbf{Z} + \cdots + a_n\mathbf{Z}$ y este ideal que contiene al 1, coincide con **Z**.

NOTA:

Se dice que n enteros $a_1, a_2, \cdots, a_n$ son primos entre sí dos a dos si

$$(1 \le i < j < n) \quad a_i \overline{)M}\, a_j = 1.$$

Por ejemplo, los tres enteros 8, 9, 35 son primos entre si dos a dos.

Se puede ver que los n enteros primos entre si dos a dos son a posteriori primos entre sí, pero la recíproca es falsa.

4.3.6.- Números primos.

En lo que sigue, se considera al **conjunto N* de los enteros naturales no nulos.**

Definición.

Un entero $p \in \mathbf{N}^*$ se dice primo si $p > 1$ y si no divisible más que por si mismo y por 1

$$p \text{ es primo} \quad \Leftrightarrow \quad D(p) = \{1, p\}$$

Los números primos menores a 20 son:

$$2, 3, 5, 7, 11, 13, 17, 19.$$

NOTA: En el caso de que el conjunto de referencia sea el de los enteros relativos **Z**, en lugar de **N*,** como hemos considerado nosotros, se puede definir a un número primo, como todo número entero relativo que posea exactamente 4 (cuatro) divisores. En ese caso entonces serán primos también los números opuestos a los dados más arriba, esto es: (-2), (-3), (-5), (-7), (-13), (-17), (-19) .

Un resultado inmediato de la definición, es que si un numero primo p no divide a un entero a, entonces p y a son primos entre si.

P_{17} *Todo entero superior a 1 no primo admite al menos un divisor primo.*

Sea un entero no primo a superior a 1. Entonces D(a) contiene un número distinto de a y de 1. Tomamos

$$d = \text{mín}(D(a)) - \{1\}$$

y mostraremos que d es primo. En efecto, si no lo fuera, existiría un entero d' tal que sería a la vez $1 < d < d'$ y $d' \mid d$, de donde $d' \mid a$ y por consiguiente $d' \in D(a) - \{1\}$ con d' estrictamente inferior al mínimo d. Contradicción.

P_{18} *Si un número primo divide un producto de enteros, divide a uno de ellos.*

En efecto, si p divide ab sin dividir a, entonces a será primo con p, divide a b de acuerdo al teorema de la divisivilidad.

Corolario

Si un número primo divide un producto de factores primos, el es uno de ellos.

Teorema 6.

El conjunto de los números primos es infinito.

Supongamos que el conjunto P de los números primos sea finito de cardinal n

$$P = \{p_1, p_2, \cdots, p_n\}$$

debemos mostrar que es una contradicción.

Consideremos el entero $a = p_1\, p_2 \cdots p_n + 1$.

Se tiene que $a > \max P$. Consideramos dos casos:

1. Si a es primo, se tiene que $a \in P$ y $a >$ máx P. Contradicción.
2. Si a no es primo, admite al menos un divisor primo d (P_{17}). Luego se tiene $d \in P$ y por consiguiente d divide $p_1\, p_2 \cdots p_n$ ya que d es igual a uno de los factores del producto. Entonces

$$(d \mid a \;\; y \;\; d \mid p_1 p_2 \cdots p_n) \;\; \Rightarrow \;\; d \mid 1 \quad \text{(contradicción)}$$

Entonces P no puede ser finito.

Descomposición de un entero en factores primos.

Teorema.

Todo entero no primo superior a 1 es el producto de factores primos
La descomposición es única.

Existencia.

Sea a un entero natural superior a 1, no primo. De acuerdo a P_{17}, admite un divisor primo p_1:

$$a = p_1 a_1; \qquad p_1 \in P, \qquad a_1 < a.$$

Si $a_1 \in P$, la existencia queda establecida. Si $a_1 \notin P$, entonces a_1 admite un divisor primo p_2:

$$a_1 = p_2 a_2; \qquad p_2 \in P, \qquad a_2 < a_1.$$

Es decir

$$a = p_1 p_2 a_2; \qquad p_1, p_2 \in P, \qquad a_2 < a_1 < a.$$

Si $a_2 \in P$, la existencia queda establecida. O si no, se continúa haciendo intervenir un divisor primo p_3 de a_2. En la etapa de rango k, se llegará a:

$$a = p_1 p_2 \cdots p_k a_k; \qquad (p_1, p_2, \cdots, p_k \text{ primos}) \in P$$
$$\text{con} \qquad a > a_1 > a_2 > \cdots > a_k$$

La sucesión de enteros naturales a_k es estrictamente decreciente, luego finita. Si se designa por n el cardinal de esta sucesión, se tiene $a_n = p_n \in P$ y

$$a = p_1 p_2 \cdots p_n$$

La existencia de una descomposición de a en factores primos queda entonces establecida.

Unicidad:

Supongamos que existen dos descomposiciones para el mismo entero a:

$$a = p_1 p_2 \cdots p_n = p'_1 p'_2 \cdots p'_m$$

Como p_1 divide al primer producto, divide también al segundo. Por el corolario de P_{18}, p_1 es igual a uno de los p'_i por ejemplo p'_1 . Simplificando, se obtiene:

$$p_2 \cdots p_n = p'_2 \cdots p'_m$$

Haciendo el mismo razonamiento se llega a identificar los n números primos del primer producto con los del segundo y por consiguiente $n \leq m$. Pero como las dos descomposiciones juegan el mismo rol, se tiene también que $m \leq n$, de donde $m = n$, con lo que se completa la demostración.

OBSERVACIÓN:

Si, en la descomposición de a, existen α_1 factores primos iguales a p_1, agrupando todos estos factores iguales, se obtiene $p_1^{\alpha_1}$.

Sea p_2 un factor primo distinto de p_1. Si existen α_2 factores primos iguales a p_2, agrupando todos estos factores se obtiene $p_2^{\alpha_2}$. De manera que la descomposición de el entero a en factores primos se presenta finalmente bajo el siguiente aspecto:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$p_1, p_2, \cdots, p_r$ serán primos distintos dos a dos y $\alpha_1, \alpha_2, \cdots \alpha_r$ serán enteros de **N***.

Por ejemplo: $360 = 2^3 \cdot 3^2 \cdot 5$.

Bibliografía

-Ayres, F.: Algebra Moderna.
-Doneddu, A.: Algebra y Geometría.
-Gentile, E.: Notas de Álgebra.
-Lentin-Rivaud: Álgebra Moderna
-Pecastaigns, F.: Chemins vers l'Algèbre
-Pinzón, A. Conjuntos y estructuras.
-Queysanne, M.: Algebra Básica.
-Taylor, H- Wade, T.: Matemáticas Básicas.

Ejercicios propuestos.

1 .- Sea F el conjunto de las funciones cuyos dominios y codominios son los enteros. Muestre que , si al conjunto F se dota se las operaciones:

$(f + g)(x) = f(x) + g(x)$ y $(f . g)(x) = f(x) . g(x)$, $\forall$ f , g $\in$ F, es un anillo.

2 .- Considere el conjunto 2 ZxZ. Defina la suma y producto en 2ZxZ de la siguiente manera:

$$(x, a) + (y, b) = (x + y; a + b)$$
$$(x, a) . (y. b) = (xy + bx + ay; ab),$$

con (x, a); (y, b) $\in$ 2ZxZ. Muestre que (2ZxZ, + , .) es un anillo conmutativo con unidad.

3 .- Demuestre que $(Z_3, +. .)$; $(Z_6, +, .)$ y $(Z_{15}, +, .)$, tienen estructura de anillo.

4 .- Sea f una función de $\{(a + ib/ a, b \in Z, i^2 = -1)\}$ sobre sí mismo definida por:
f(a + bi) = a - bi. Muestre que f es un homomorfismo.

5 .- Demostrar que ½ $\notin$Z.

6 .- ¿ Cuáles de los siguientes números reales son enteros?

½ ; 7/3 ; 27/3 ; 1 + ½ ; -2/2 ; 0/2 ; 2/-2 .

7 .- ¿Que enteros z, $-10 \leq z \leq 10$ se escriben en la forma 4m + 1, para algún m$\in$Z?. Ídem para 4m + 3.

8.- Calcular en Z

1 - (2 - (3 - (4 - (5 - (6 - (7 - (8 - (9 -(10 - 11))))))))).

9 .- Dado x $\in$ R, encontrar m $\in$ Z tal que $m \leq x \leq m + 1$, en los casos siguientes:

a) x = -1/2 ; b) x = - 7/3 ; c) x = 18/5 ; d) x = - 23/3 ; e) x = -17.

10.- ¿ Cuáles de los siguientes números enteros son pares , n $\in$ N ?

a) $3n^2 + 1$; b) n(n + 1) ; c) (n - 1)(n + 1) ; d) $n^3 - n$.

Recordar: Un número entero m se dice par sii 2 | m.

Algoritmo de la división en Z.

Sean a y b números enteros, b > 0, entonces, existen y son únicos enteros q y r tales que: a = b.q + r, con $0 \leq r < b$. q y r se denominan respectivamente cociente y resto.

11.- Determinar q y r si:

a) a = 4231 , b = 7; b) a= -4231 y b = 7; c) a= 957 y b = 12; d) a = 132 y b = -89.

12.- Se sabe que el resto de la división de 748 por un número n positivo es 20 y el resto de la división de 1229 por n es 33. Hallar n.

Máximo común divisor.

Sean a y b enteros, (a, b) ≠ (0, 0) (o sea no simultáneamente nulos). Existe d ∈ **N** con las siguientes propiedades:

i) d | b y d | b
ii) Existen enteros u y v tales que d = u.a + v.b

Entonces d se denomina el máximo común divisor (m.c.d.) de a y b y se denota d = (a, b)

13.- Determinar el m.c.d. si : a) (a, b) = (84, 45) ; b) (84, -45).

Mínimo común múltiplo

Sean a y b enteros, no nulos. Entonces a.b y -(a.b) son múltiplos de a y de b. Se sigue de esto que a y b poseen un múltiplo común mayor que cero. O sea, el conjunto H de múltiplos comunes positivos de a y b es no vacío.

Si m es el elemento mínimo de H, tenemos las siguientes propiedades:

i) m es múltiplo de a y de b.
ii) m > 0
iii) Si k ∈ **Z**, k > 0, k múltiplo de a y b, entonces m ≤ k.

Al m asociado a a y b lo denominamos el mínimo común múltiplo.

14.- Hallar el mínimo común múltiplo de: a) 1 y 12; b) 1 y -1; c) 8 y 14; d) 12 y 15; e) 11 y -13.

Teorema fundamental de la aritmética..

Sea n ∈ **Z**; n ≠ 0; n ≠ 1; n ≠ -1. Entonces existe una sucesión finita de primos

p_i , i = 1, ..., k tal que $0 < p_1 < ,,, < p_k$.

$$n = \varepsilon . \prod_{i=1}^{k} p_i = \varepsilon . p_1 ... p_k$$ donde ε es 1 o es -1

15.- Representar los siguientes enteros como productos de primos.

a) 1472; b) $(210)^4$; c) 18.365.-

16.- Escribir 141 y 152 en base 4. Hacer su suma y comprobar los resultados.

Congruencias.

Sea m un número positivo. La relación congruente módulo m (≡ mod m), se define para todos los pares a, b ∈ **Z** por a ≡ b (mod m) ⇔ m | (a - b).

17.- Hallar los menores enteros positivos módulo 5 con los cuales son congruentes 19 ; 288.

18.- Analizar la validez de las siguientes afirmaciones:

a) $11 \equiv -1\ (6)$; b) $13 \equiv 0\ (2)$; c) $10^2 \equiv 10\ (3)$; d) $31 \equiv -18\ (7)$.

19.- Qué valores de m hacen verdadera las congruencias siguientes:

a) $5 \equiv 4\ (m)$; b) $1197 \equiv 186\ (m)$.

5.- Enumeramientos

5.1.- Arreglos

Comentario:

El análisis combinatorio es la ciencia, y en alguna medida, el arte de contar o enumerar los elementos de un conjunto *finito.* Por otra parte, un buen conocimiento de combinatoria, siempre útil, permite resolver muchos problemas de situaciones reales, como asimismo de probabilidad, de forma especialmente rápida y elegante.

6.1.1.- Factorial.

Definición.

Sea n un número natural, se llama factorial de n, y se denota n!, al número natural definido como sigue:

a) 0! = 1;
b) Se supone definido n! , y se define (n + 1)! por

$$(n + 1)! = (n + 1)\cdot n!$$

Se obtiene así por ejemplo:

$$1! = (0 + 1)! = (0 + 1)\cdot 0! = 1\cdot 1 = 1, \qquad 2! = (1 + 1)! = (1 + 1)\cdot 1! = 2 \cdot 1 = 2$$

etc., y para todo $n \in \mathbf{N^*}$,

$$n! = 1 \cdot 2 \cdot 3 \cdot \ ... \cdot n$$

El factorial de n es el producto de todos los enteros de 1 a n.

La aplicación $n \rightarrow n!$, queda además, de acuerdo al axioma de recurrencia, definido para todo **N.**

Es decir la función factorial, tiene dominio el conjunto **N** y por codominio al conjunto **N***. Es una función no inyectiva, dado que 0! = 1! = 1, y no sobreyectiva dado que no existe ningún número natural n cuyo factorial sea el número 3, (por ejemplo).

La gráfica de esta función, es decir el dibujo en el plano de $\{(n, p) / n! = p\}$, es un conjunto de puntos aislados.

Simplificación.- Muchas veces en el cálculo aparecen cocientes de factoriales, que en la práctica convienen simplificar, (usando la definición) para un mejor manejo de los mismos. Por ejemplo:

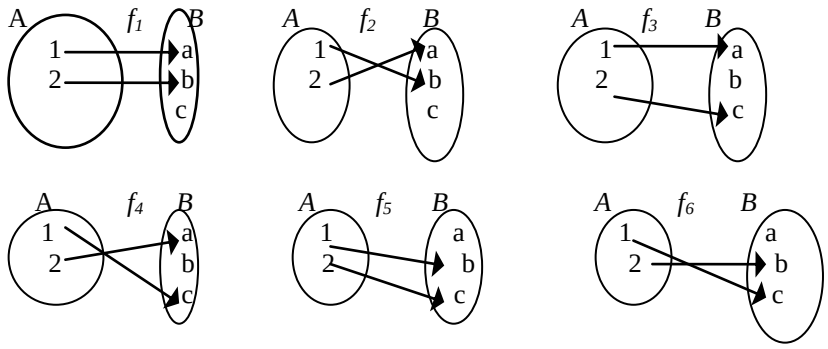
$$1.- \quad \frac{(n+2)!}{(n-1)!} = \frac{(n+2)\cdot(n+1)\cdot n\cdot(n-1)!}{(n-1)!} = (n+2)\cdot(n+1).n$$

$$2.- \quad \frac{(n-1)!}{(n-3)!} = \frac{(n-1)\cdot(n-2)\cdot(n-3)!}{(n-3)!} = (n-1)\cdot(n-2)$$

Antes de definir arreglos o variaciones, vamos a considerar el siguiente problema:

-Dados los conjuntos $A = \{1, 2\} \subset \mathbf{N}$ y $B = \{a, b, c\}$. ¿Cuántas funciones inyectivas distintas, de A en B , se pueden definir?.

Se puede resolver el problema haciendo los diagramas de Venn de todas las funciones inyectivas distintas:



Los seis diagramas representan a seis funciones inyectivas distintas, y no hay ninguna más

Se debe notar, que, al ser el dominio A es un subconjunto de números naturales esta totalmente ordenado por la relación usual de orden de números naturales, como además la función es inyectiva, se induce el mismo orden en el conjunto imagen de la función. Por consiguiente las seis funciones quedan caracterizadas, si se identifican a las seis imágenes distintas (respetando el orden establecido).

Por ejemplo:

a, b (imagen de A por f_1)
b, a (imagen de A por f_2)
a, c (imagen de A por f_3)
c, a (imagen de A por f_4)
b, c (imagen de A por f_5)
c, b (imagen de A por f_6).

A cada una de las seis imágenes, se les llama una variación o arreglo de 2 en 3 (o también de 2 elementos tomados de 3 elementos).

El problema a resolver, es entonces, hacer una definición de este concepto que nos permita, identificar a las variaciones con problemas reales y una formulación que nos permita calcular el número de arreglos posibles.

5.1.2.- Definición.

Se considera un conjunto B finito cualquiera, no vacío, de n elementos y sea:

$$I_p = [1, p] \subset \mathbf{N} \text{ un intervalo inicial de } \mathbf{N} \text{ tal que } p \leq n.$$

Definición.

Se llama arreglo de los n objetos de B, p a p, a la imagen de una inyección cualquiera de $I_p = [1, p]$ en B.

Sea *f* una de esas inyecciones, el orden estricto y total en el intervalo I_p define un orden estricto y total en el arreglo $f(I_p) \subset B$, de la siguiente manera: cualesquiera que sean los números distintos *i* y *j* de el intervalo I_p, si $i < j$, se dirá que *f(i)* es anterior a *f(j)* y se denotará $f(i) < f(j)$:

$$i < j \Rightarrow f(i) < f(j).$$

Se obtiene así, por grafo del arreglo,

$$f(I_p) = \{ a_1, a_2, ..., a_p \},$$

con

$$(\forall i \in I_p) \quad a_i \in B.$$

En otros términos: *Se llaman variaciones o arreglos de n elementos tomados de p en p, a las colecciones distintas que pueden formarse con p elementos distintos entre los n, siendo dos colecciones distintas si tienen algún elemento distinto, o teniendo los mismos elementos, están en distinto orden.*

5.1.3.- Número de arreglos.

El problema que se propone ahora es el siguiente:
¿Cuál es el número total de arreglos de *n* objetos de B, *p* a *p* ?

La respuesta se da por el siguiente teorema:

Teorema 1.

Dado el conjunto B de n elementos y un número natural p tal que $1 \leq p \leq n$, *el número total de las funciones inyectivas de [1, p] en B viene dado por:*

$$n(n - 1)(n - 2) \ldots (n - p + 1).$$

Demostración.

Se toma $I_p = [1, p]$ y se razona por recurrencia sobre p, limitada a [1, n].

1° El teorema es verdadero para p = 1. En efecto, el intervalo $I_1 = \{1\}$ no tiene más que un elemento. Una inyección de I_1 en B queda entonces determinada toda vez que se fije la imagen de 1 que es única. Como hay n elementos en B hay en consecuencia, n funciones inyectivas.

2° Sea $1 \leq p \leq n$. Se supone que el número de las inyecciones de I_p en B sea igual a

$$n(n - 1)(n - 2) \ldots (n - p + 1).$$

Se debe demostrar que el número de funciones inyectivas de I_{p+1} en B es igual a

$$n(n - 1)(n - 2) \ldots (n - p + 1)(n - p)$$

(número deducido del precedente y multiplicado por $n - p$, es decir, $[(n - p + 1) - 1]$.

Sea f un inyección de I_p en B. Entonces, $f(I_p)$ contiene p elementos. Se puede extender f en una inyección de I_{p+1} en B definiendo $f(p + 1)$. Ahora, B - $f(I_p)$ contiene n - p elementos; hay entonces n - p elecciones posibles para la imagen $f(p + 1)$. Toda inyección de I_p en B se extiende en consecuencia en n - p inyecciones de I_{p+1} en B. Como toda inyección de I_{p+1} en B es la extensión de una inyección de I_p en B, el teorema queda demostrado.

Notación.

Se denota $A_{n,p} = V_{n,p} = n(n . 1)(n - 2) \ldots (n - p + 1)$; se tiene evidentemente

$$A_{n,p} = V_{n,p} = \frac{n!}{(n-p)!}$$

Caso particular.

Si $p = n$, se obtiene

$$A_{n,n} = V_{n,n} = n!$$

Corolario:

Sea B un conjunto de n elementos, el número total de biyecciones de [1, n] sobre B es n!

Ejemplos:

1- ¿ En cuántas formas pueden fotografiarse 5 personas en grupo alineados de 3 personas?

Respuesta: $V_{5,3}$.

2- En una sala de diversiones hay 8 juegos individuales distintos. ¿En cuántas formas pueden ocuparlos 5 personas?

Respuesta: $V_{8,5}$.

5.2.- Permutaciones de un conjunto finito.

Se llaman permutaciones ordinarias en el conjunto $B = \{a_1, a_2, a_3, ..., a_p\}$ de *p* elementos, a las diferentes agrupaciones que pueden formarse con dichos elementos, tomados de *p* en *p* (distintos todos ellos) las cuales sólo diferirán en el orden de colocación de los mismos.

Se puede observar que hay tantas aplicaciones biyectivas posibles como permutaciones de los elementos $a_1, a_2, a_3, ... a_p$, y que cada permutación está formada por las imágenes de los elementos 1, 2, .. . p del intervalo inicial [1, p], con lo que se puede afirmar que: "las permutaciones ordinarias en el conjunto $B = \{a_1, a_2, a_3, ... a_p\}$ de p elementos son tantas como aplicaciones biyectivas pueden establecerse de un conjunto arbitrario A también de p elementos , y en cada aplicación biyectiva las imágenes , constituyen una permutación diferente en B.

En el teorema 1, se puede tomar, en lugar del intervalo [1, p], un conjunto cualquiera I_p que tenga p elementos. Se obtiene así el enunciado más general:

Sea I_p un conjunto cualquiera de p elementos y B un conjunto cualquiera de n elementos $(1 \leq p \leq n)$, el número total de las inyecciones de I_p en B es

$$n(n - 1) ... (n - p + 1).$$

En particular, I_p puede ser una parte de B.

Si $I_p = B$, entonces se sabe que una inyección de B sobre sí mismo es biyectiva y se denomina *permutación de* B.

Es decir:

5.2.1- Definición.

Sea $B = [1, p] = \{1,2, ..., p\}$ el intervalo inicial de orden p. Se llama permutación de B a toda aplicación $f : B \to B$ biyectiva.

Es costumbre denotarlas con las matrices:

$$f := \begin{pmatrix} 1 & 2 & 3 & & i & & p \\ f(1) & f(2) & f(3) & \dots & f(i) & \dots & f(p) \end{pmatrix}$$

escribiendo debajo de cada *i,* el valor *f(i)* asignado por la función. De esta forma una permutación está dada por la sucesión:

$$f(1) \quad f(2) \quad f(3) \quad \ldots \quad f(p)$$

de números en [1, p]. Por ejemplo si $p = 2$ hay sólo dos permutaciones: 12 y 21 , que corresponden respectivamente a las aplicaciones:

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

si $p = 3$ hay 6 permutaciones

$$123 \quad 132 \quad 213 \quad 231 \quad 312 \quad 321$$

correspondiente a las aplicaciones:

$$\begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix} \quad \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix} \quad \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} \quad \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} \quad \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix} \quad \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}$$

Se tiene así el teorema:

Teorema 2.

El número de las permutaciones de un conjunto B de n elementos es n!.

OBSERVACIÓN.- Es usual, en lugar de decir arreglos de *n* objetos de B, *n* a *n* , se diga "permutación de los *n* objetos", confundiendo la aplicación "permutación de B" con la imagen que ella da de B. Se trata aquí de no cometer esta confusión y se usará el nombre de arreglo para designar a la imagen.

Ejemplo 1: ¿De cuántas formas pueden fotografiarse una familia de 5 personas puestas en hilera?

Respuesta: $5! = 120$.

El mismo problema pero ahora se pide que la madre y el padre estén siempre juntos.

Respuesta: $2 \cdot 4! = 48$. En efecto, es este caso padre y madre forman un sólo objeto de manera que se trata de permutaciones de 4 objetos. Pero además hay dos formas en que pueden ubicarse, uno respecto del otro.

Ejemplo 2: ¿De cuántas formas pueden fotografiarse 6 chicas y 7 chicos puestos en hilera pero de manera tal que nunca aparezcan juntos dos personas del mismo sexo. Respuesta: $6! \cdot 7!$

Ejemplo 3: 3 parejas van al teatro y sacan 6 entradas consecutivas de una misma fila que reparten al azar. El espacio muestral tiene de cardinal el número de permutaciones de 6 elementos Respuesta: 6! = 720. Tienen 720 formas diferentes de sentarse los 6.

5.2.2.- Inversiones en una permutación

Se llama inversión a todo par de subíndices de una permutación, que esté en orden inverso al natural.

(a_1 a_2 a_3 a_4) no tiene inversiones.
(a_2 a_1 a_3 a_4) tiene la inversión (2-1),
la (a_3 a_1 a_4 a_2) tiene tres inversiones (3-1) ; (3-2) ; y (4-2).

La permutación se llama de "clase par" o de "clase impar" según que el número de inversiones de los subíndices sea par o impar.
Si el número de inversiones es cero, se considera de clase par.

5.3.- Combinaciones.

Comentario:
En lo precedente, además de establecer nociones generales sobre algunas formas de contar, hemos estudiado algunas situaciones que aparecen con frecuencia en Combinatoria. Por ejemplo, hemos desarrollado fórmulas para el cálculo de *permutaciones y variaciones*, esto es, elecciones ordenadas de una cierta cantidad de elementos, sin repetición. Cuando no nos importa el orden en que los objetos son elegidos, nos referimos a *combinaciones* de los mismos. Por lo tanto, las combinaciones de n objetos tomados de a p, pueden describirse como todas las formas posibles de elegir un subconjunto de p elementos, en un conjunto de n elementos. Debe quedar claro aquí que la expresión "conjunto de p elementos" designa, por supuesto, a p elementos **distintos.**

Antes de hacer una definición formal de este concepto, se considera el siguiente problema:

Dados los conjuntos $I_3 = [1, 3]$ y el conjunto $B = \{1, 2, 3, 4\}$, ¿Cuántas funciones inyectivas existen de I_3 en B?. La respuesta es $A_{4,3} = 4 \cdot 3 \cdot 2 = 24$ funciones inyectivas y se pueden representar por:

123, 132, 213, 231, 312, 321

124, 142, 214, 241, 412, 421

134, 143, 314, 341, 413, 431

234, 243, 324, 342, 423, 432

Ahora bien, de acuerdo a lo que se dijo en el comentario inicial, se puede decir en general, que dado un conjunto finito, se llama combinación de orden p a todo subconjunto de p elementos. Es claro que cada variación de p en n determina una combinación (la combinación se forma con los elementos de la variación). Pero distintas variaciones pueden dar lugar a la misma combinación. En el ejemplo anterior, las variaciones de 3 en 4 que hemos enumerado más arriba dan lugar a sendas combinaciones cuando ignoramos el orden de los elementos. Estas son: 123, 124, 134 y 234.

5.3.1. Definición

Sea B un conjunto no vacío de n elementos y p un número natural tal que $1 \leq p \leq n$.

Definición.

Se llama combinación de los n elementos de B, p a p, a toda parte de B de p elementos.

En una combinación, ningún orden interviene en estos p objetos.

Por lo dicho anteriormente, siendo las combinaciones de n objetos aquellos arreglos que se diferencian en por lo menos un elemento, bajo el supuesto de conocer el número de combinaciones de n elementos tomados de p en p , fácilmente obtenemos el total de variaciones de esos mismos objetos, también de p en p, si en cada combinación procedemos a alterar el orden de disposición de sus elementos en todas las formas posibles. Pero, como cada combinación, tiene p objetos distintos, alterar su orden en todas las formas posibles y computar su número es hallar las permutaciones de p elementos. Por lo tanto, a partir de las combinaciones, es posible calcular el número de variaciones de igual orden si, a cada una de ellas, le efectuamos las permutaciones indicadas.

El número de las combinaciones de n objetos p a p está dado por el teorema siguiente:

Teorema 3.

Dado un conjunto B de n elementos, el número de partes de B que tienen p elementos ($1 \leq p \leq n$) es:

$$\frac{n(n-1)\ldots(n-p+1)}{p!}.$$

Demostración.

Se considera al conjunto $\mathcal{F}$ de todas las inyecciones de $I_p = [1, p]$ en B. Se sabe que $\mathcal{F}$ contiene:

$n(n - 1)(n - 2) \ldots (n - p + 1)$ funciones inyectivas (teorema 1).

Si $f \in \mathcal{F}$, entonces $f(I_p)$ es una parte de B que tiene p elementos. Se van a contar, en $\mathcal{F}$, las inyecciones que dan de I_p la misma imagen $A \subset B$. Para ello, se estudia la relación binaria siguiente en $\mathcal{F}$:

$$f \equiv g \quad \Leftrightarrow \quad f(I_p) = g(I_p)$$

La relación $\equiv$ es reflexiva, simétrica y transitiva (queda como ejercicio probarlo). Es decir es una relación de equivalencia. Por consiguiente parte a $\mathcal{F}$ en clases. Todas las inyecciones de una clase dan la misma imagen en B y toda parte A de B que tenga p elementos define una y sólo una clase. El número de clases es en consecuencia igual al número buscado de partes de B que tienen p elementos.

Se busca ahora el número de funciones en cada clase. A todo par f, g tal que $f \equiv g$, se le asocia una aplicación h de I_p en I_p de la manera siguiente:

$$(f, g) \rightarrow h \ ;$$

$$h : I_p \rightarrow I_p$$
$$x \xrightarrow{h} y = h(x) \quad \text{tal que } f(x) = g(y).$$

La aplicación h ha sido bien definida pues, a todo x de I_p le corresponde uno , y sólo un y, de I_p tal que $f(x) = g(y)$, dado que g es inyectiva y que

$$f(I_p) = g(I_p).$$

Además, h es biyectiva, pues todo y de I_p es la imagen de uno y sólo un elemento x de I_p, ya que f es inyectiva.

En consecuencia, h es una *permutación* de I_p. Además,

$$(\forall\, x \in I_p) \qquad f(x) = g(y) = g[h(x)],$$

de lo que surge que $f = g \circ h$.

Por último, para f y g dadas en una misma clase, la permutación h es única.

Si se designa por $\mathcal{P}$, al conjunto de las permutaciones de I_p, se acaba de demostrar:

$$f \equiv g \quad \Rightarrow \quad (\exists!\ h \in \mathcal{P} \quad \text{tal que} \quad f = g \circ h\ ).$$

La recíproca es inmediata: si existe una permutación h de I_p tal que $f = g \circ h$, se tiene evidentemente $f(I_p) = g(I_p)$, entonces $f \equiv g$.

En consecuencia, el número de los elementos f de una clase de equivalencia representada por g es igual al número de las permutaciones de $\mathcal{P}$. Se sabe que este número es $p!$ (teorema 2).

Como el número total de las funciones de $\mathcal{F}$ es $A_{n,p}$, el número total de las clases es entonces:

$$\frac{A_{n,p}}{p!} = \frac{n(n-1)...(n-p+1)}{p!} = \frac{n!}{p!(n-p)!}$$

El teorema 3 queda demostrado.

Notaciones.

El número de las combinaciones de n objetos p a p se denota $C_{n,p}$.
Se tiene

$$C_{n,p} = \frac{A_{n,p}}{p!} = \frac{n(n-1)(n-2)...(n-p+1)}{p!} = \frac{n!}{p!(n-p)!}$$

Es costumbre denotar a este último número como:

$$C_{n,p} = \binom{n}{p} = \frac{n!}{(n-p)!\,p!} \quad .$$

Se puede extender esta fórmula a $p = 0$, si se recuerda que $0! = 1$, con lo que $C_{n,0} = 1$. Dado que:

$$C_{n,0} = \binom{n}{0} = \frac{n!}{(n-0)!.0!} = \frac{n!}{n!.1} = 1. \qquad \text{Tambien se define:}$$

$$C_{n,p} = \binom{n}{p} = 0 \qquad \text{si} \qquad n < p.$$

Ejemplos

1.- En una carrera compiten 10 corredores y se clasifican los tres primeros para la siguiente fase. ¿De cuántas maneras puede producirse la clasificación?

$$C_{10,3} = \frac{V_{10,3}}{P_3} = \frac{10\ .\ 9\ .\ 8}{3\ .\ 2} = 120$$

2.- Se reparten tres globos entre seis amigos. El número de posibles repartos es

$$C_{6,3} = 20.$$

3.- ¿Cuántos equipos de fútbol se pueden formar con 15 personas, si un equipo tiene once integrantes?

4.- ¿Cuántas líneas quedan determinadas en el plano por 10 puntos no alineados de a 3?

5.3.2.- Propiedades

P$_1$ $\quad C_{n,p} = C_{n,n-p}$; o tambien $\quad \binom{n}{p} = \binom{n}{n-p}$

En efecto,

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

el cociente no cambia cuando se reemplaza p por $n - p$.

P$_2$ $\quad n > p \geq 1 \quad$ *implica*

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

En efecto,

$$\binom{n-1}{p} + \binom{n-1}{p-1} = \frac{(n-1)!}{p!(n-p-1)!} + \frac{(n-1)!}{(p-1)!(n-p)!}$$

$$= \frac{(n-1)!}{p!(n-p)!}[(n-p)+p] = \frac{n!}{p!(n-p)!} = \binom{n}{p}.$$

Esta propiedad nos enseña cuándo la suma de dos números combinatorios es cerrada:

Dos números combinatorios se pueden sumar, cuando tienen el mismo numerador (n - 1) y sus denominadores son consecutivos (p y p - 1) , el resultado es otro número combinatorio que tiene por numerador al anterior incrementado en 1, esto es p; y cómo denominador al mayor de los dos denominadores dados p.

Esta suma de números combinatorios, permite definir por recurrencia, los coeficientes del desarrollo del binomio de Newton para cada número natural n.

Escribiendo la relación anterior para variados valores de n y p se obtiene el triángulo de Pascal

5.3.3.- Triángulo de Pascal.

n = 0						1					
n = 1					1		1				
n = 2				1		2		1			
n = 3			1		3		3		1		
n = 4		1		4		6		4		1	
n = 5	1		5		10		10		5		1
n = 6		1		6		15		20		15	
n = 7			1		7		21		35		
n = 8				1		8		28		56	
n = 9					1		9		36		
n = 10						1		10		45	

Ahora bien , la P_1 : $C_{n.p} = C_{n,n-p}$, se interpreta de la siguiente manera : *cada subconjunto de p elementos en [1, n] determina unívocamente un subconjunto de n - p elementos.*

En cambio, la P_2 : $C_{n,p} = C_{n-1,\ p} + C_{n-1,\ p-1}$; dice que: *las combinaciones de p elementos de n, se clasifican en dos subconjuntos disjuntos:*

A: los que contienen a n,
B: los que no contienen a n.

Entonces A tiene $C_{n-1,\ p-1}$ elementos y B tiene $C_{n-1,\ p}$ elementos.

Los subconjuntos no vacíos de [1, n] se pueden clasificar en subconjuntos de 1 elemento, subconjuntos de 2 elementos , etc., esto no lleva a la fórmula

$$2^n = C_{n\ ,0} + C_{n\ ,1} + \ldots + C_{n\ ,n} = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}.$$

En términos del triángulo de Pascal significa que los elementos de la fila *n* suman 2^n .

5.4.- Binomio de Newton

5.4.1.- Definición y ejemplos.

Consideremos un anillo conmutativo A. Sea *n* un número natural y *x* e *y* dos elementos de A.

Se denomina *binomio de Newton* al elemento $(x + y)^n$ de el anillo A.

Por ejemplo, de acuerdo a las propiedades de las leyes de composición en un anillo A conmutativo:

$$(x + y)^2 = x^2 + 2xy + y^2$$
$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

el problema que se quiere resolver es encontrar un desarrollo para $(x + y)^n$, cualquiera se el número natural n.

5.4.2.- Notación

Sean $a_1 , a_2 , a_3 , \cdots a_n,$ elementos en número finito de un semigrupo aditivo E. La suma siguiente :

$$s = a_1 + a_2 + a_3 + \cdots + a_n$$

Se denota :

$$s = \sum_{k=1}^{n} a_k$$

Ejemplo en N:

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

5.4.3.- Teorema.

Sea A un anillo conmutativo, x e y dos elementos de A y n un número natural no nulo. Entonces:

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

Demostración.

Razonamos por recurrencia sobre el número n.

1º La relación es verdadera para $n = 1$.

La sumatoria se efectúa sobre dos términos:

$$x + y = \binom{1}{0} x + \binom{1}{1} y \,; \qquad \textit{donde} \quad \binom{1}{0} = \binom{1}{1} = 1 .$$

2º Suponemos la ley válida para n y demostrémosla para n + 1. Por hipótesis de recurrencia,

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

Multiplicando los dos miembros por $(x + y)$, se obtiene

$$(x+y)^{n+1} = \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n+1-k}$$

Sea p un número natural tal que $0 < p < n + 1$, buscamos los terminos en $x^p y^{n+1-p}$.

Hay dos:

a) Uno proviene de la primer suma con $k + 1 = p$.

Escribimos entonces ésta primer suma con el índice p de suma y sacando el último término x^{n+1} fuera de esta sumatoria;

$$\sum_{p=1}^{n+1} \binom{n}{p-1} x^p y^{n+1-p} = x^{n+1} + \sum_{p=1}^{n} \binom{n}{p-1} x^p y^{n+1-p}$$

b) El otro proviene de la Primer sumatoria con $k = p$,

Escribimos esta sumatoria con el índice p y sacamo de la misma el primer término y^{n+1};

$$\sum_{p=0}^{n} \binom{n}{p} x^p y^{n+1-p} = y^{n+1} + \sum_{p=1}^{n} \binom{n}{p} x^p y^{n+1-p}$$

De manera que en definitiva,

$$(x+y)^{n+1} = x^{n+1} + \sum_{p=1}^{n} \left[\binom{n}{p-1} + \binom{n}{p} \right] x^p y^{n+1-p} + y^{n+1}$$

Aplicando la propiedad de la suma de números combinatorios, se tiene:

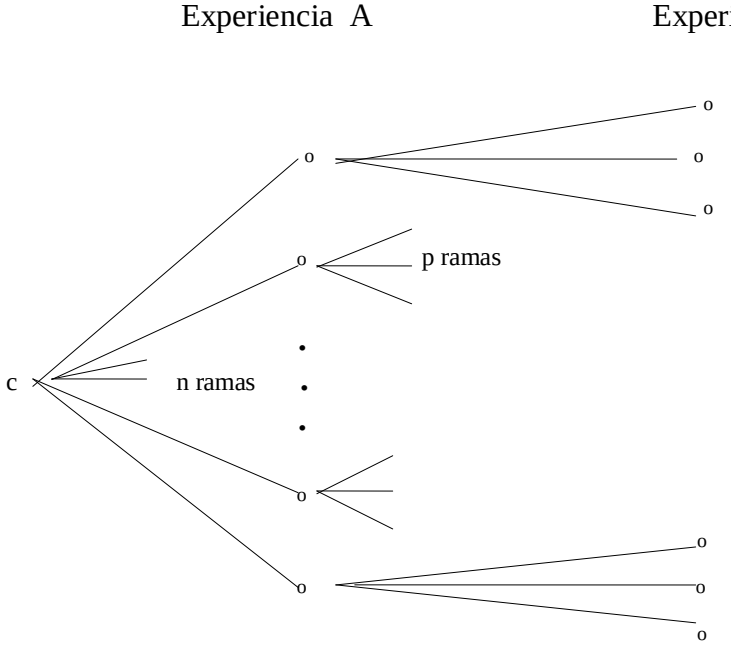
$$(x+y)^{n+1} = x^{n+1} + \sum_{p=1}^{n} \binom{n+1}{p} x^p y^{n+1-p} + y^{n+1} = \sum_{p=0}^{n+1} \binom{n+1}{p} x^p y^{n+1-p}$$

El teorema queda demostrado.

5.5.- Principio general de enumeración.

Si una experiencia A arroja n resultados posibles y por cada resultado de A se realiza una experiencia B que puede arrojar p resultados posibles, entonces la realización en sucesión de A y B arroja un número total de $n \cdot p$ resultados posibles.

Es útil graficar esta situación utilizando un "*diagrama de árbol*" .-

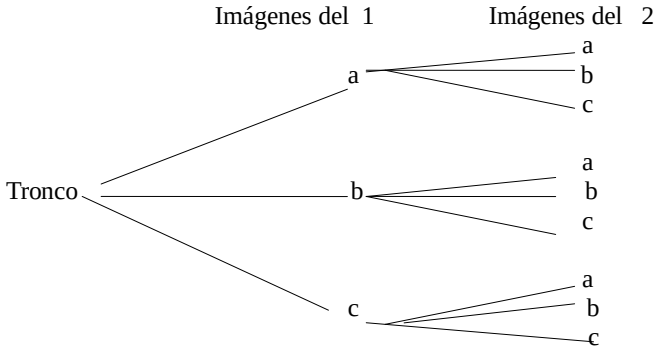


A partir del tronco dibujamos las n ramas correspondientes a la primer experiencia y luego por cada rama dibujamos las p ramas correspondientes a la segunda experiencia. Es claro que el número total de ramas es $n \cdot p$. Podemos extender estas consideraciones a k experiencias, $A_1, ..., A_k$ $k \in \mathbf{N}$.

Si para cada i, $1 \leq i \leq k$, A_i es una experiencia que tiene n_i resultados posibles y si por cada resultado que tiene A_i experiencias se realiza una experiencia A_{i+1} que tiene n_{i+1} resultados posibles, entonces el número total de resultados posibles que tiene la realización en sucesión de $A_1, A_2, ..., A_k$ es el producto $n_1 \cdot n_2 \cdot ... \cdot n_k$.

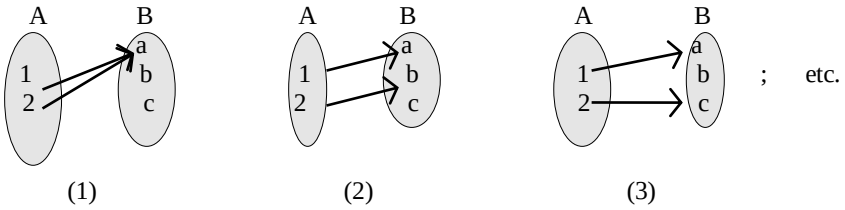
Un diagrama de árbol, también nos permite enumerar el número de funciones que se pueden obtener, dados dos conjuntos finitos, como se ilustra en el siguiente ejemplo:

Ejemplo.- Dados el conjunto $A = \{1, 2\}$ y el conjunto $B = \{a, b, c\}$, se trata de "contar " haciendo un diagrama de árbol , el número de funciones de A en B.



La primer rama me determina la imagen {a, a} = {a} de la primer función (función constante), la segunda {a, b} etc., en total 9 (nueve). O sea, por cada elemento del codominio a, b, y c tenemos 3 (tres) opciones para elegir la segunda imagen, toda vez que se toma por segunda imagen la misma letra se trata de una función constante.

Para "ver" como van apareciendo estas funciones, se pueden hacer algunos diagramas del tipo sagital:



La (1) corresponde a la primer rama y es entonces la función constante, la (2) a la segunda y así sucesivamente. Como por cada elemento del codominio tenemos tres opciones, como se ve en el diagrama de árbol hecho antes, el número de funciones será igual a $3 \cdot 3 = 3^2 = 9$.

Al conjunto imagen de una de tales funciones se denomina ***variación con repetición*** de tres elementos tomados de dos en dos.

Es decir dado un conjunto finito E de n elementos se llama variaciones con repetición p-arias, de los elementos de E, a las diferentes agrupaciones que pueden formarse con dichos elementos tomados de p en p, iguales o diferentes, tales que se distingan en algún elemento o en el orden de colocación. Como por otra parte se ilustró en el ejemplo anterior.

5.6.- Variaciones con repetición.

Se tienen n elementos distintos: $a_1, a_2, a_3, ..., a_n$

Pretendemos ocupar p lugares con ellos de modo que cada elemento pueda ocupar más de un lugar. Las distintas disposiciones se llaman ***variaciones con repetición de n elementos tomados p a p.***

O también, sean A y B dos conjuntos finitos de cardinales respectivos p y n. A las funciones de A en B se les llaman variaciones con repetición.

Vamos a considerar el caso más general, calculando el número total de funciones o aplicaciones de [1, p] en [1, n], donde p y n son números naturales arbitrarios. Este problema da lugar al siguiente teorema:

5.6.1.- Teorema 4:

El número total de aplicaciones de [1, p] en [1, n], se denomina número de variaciones de n elementos tomados de a p con repetición, y se denota y calcula como:

$$\boldsymbol{Vr_{n,p} = n^p}.$$

Demostración.

Para hallar la cantidad de variaciones con repetición que pueden formarse con *n* elementos tomados de *p* en *p,* se emplea el método de inducción matemática. Su cantidad, en órdenes equivalentes, es evidentemente superior al de las variaciones simples pues, además de éstas, son considerados también los que se obtienen repitiendo ilimitadamente cada uno de los elementos dados.

La demostración se hace entonces por recurrencia, es decir se toma [1, p] y se razona por inducción sobre p limitada a [1, n].

1° El teorema es verdadero para p = 1. Dado que el número de funciones de [1, 1] en [1, n]; se calcula como $n^1 = n$. Es decir se tiene tantas imágenes como elementos tenga el codominio de la función. En otros términos, la función queda determinada toda vez que se fije la imagen de 1, como en el codominio de la función hay n elementos habrá en consecuencia n funciones.

2° Se supone ahora, que hay n^p funciones de [1, p] en [1, n], es decir $Vr_{n,p} = n^p$. Se tiene que demostrar que el número de funciones de [1, p +1] en [1, n] es: $Vr_{n,\,p+1} = n^{p+1}$.

Para calcular el número de aplicaciones de [1, p +1] en [1, n] , se debe observar que por cada función de [1, p] en [1,n] se obtiene n aplicaciones de [1, p +1] en [1, n], simplemente dando los n valores posibles a p +1.

Es decir, cada aplicación de las dadas, es *extiende* a una aplicación de [1, p +1] en [1, n]. Y recíprocamente, lo mismo. Por lo tanto, hay n veces el número de aplicaciones de [1, p] en [1, n]. Este número es entonces:

$$n^p \cdot n = n^{p+1}$$

Es decir, el teorema queda demostrado.

Ejemplos.

1.- En un hipódromo hay que acertar el vencedor de cada una de las seis carreras en las que corren 12 caballos. El número de jugadas posibles que se tienen que realizar para acertar con seguridad es

$$Vr_{12,6} = 12^6 = 2.985.984$$

2.- Si el número de partidos de una fecha de fútbol es 14, y como los resultados posibles son 3, empate, local o visitante, el número de jugadas que hay que hacer para acertar con seguridad en una de ellas todos los resultados es:

$$Vr_{3,14} = 3^{14} = 4.782.969$$

3.- Tres amigos van a un carrito de lomito a comprar uno para cada uno. Hay lomitos de 6 variedades. El número de posibles elecciones es

$$Vr_{6,3} = 6^3 = 216$$

4.- Con los dígitos 1,2,3,4,5, ¿cuántos números de dos dígitos pueden formarse?

$$Vr_{5,2} = 5^2 = 25.$$

No debe olvidarse que, debido a la propiedad de repetición ilimitada de los elementos dados, el número p puede adoptar valores arbitrariamente grandes y lógicamente, cuando se desee, mayores que n. Con esta indicación se comprende que es posible representar la sucesión indefinida de los números naturales, con sólo diez símbolos arábigos: 1, 2, 3, 4, 5, 6, 7, 8, 9 y 0.

Ejemplo: ¿Cuántos números distintos de cuatro cifras se pueden expresar con los números 1, 2 y 3?

$$Vr_{3,4} = 3^4 = 81$$

algunos de estos 81 números de cuatro cifras son los siguientes: 1321; 1223; 3333; 1232; 2211; 2123; etc.

5.7.- Permutaciones con repetición.

Consideremos ahora la palabra UMPUMU. El problema es ¿Cuántas palabras se pueden formar permutando las letras al azar. El número posibles de palabras son las permutaciones de 6 elementos donde uno se repite 3 veces, otro 2, y el tercero sólo aparece una vez:

$$P_6^{3,2,1} = 6! / 3!\, 2!\, 1! = 720 / 6 \,.\, 2 = 60.$$

Se puede formar 60 "palabras" distintas.

Sea, ahora el conjunto $C = \{a_1, a_2, a_3, \ldots a_n\}$ de n elementos del que se pueden obtenerse $n!$ permutaciones ordinarias; en este supuesto, si en una de ellas tomamos los α elementos $a_1, a_2, a_3, \ldots a_\alpha$ $(\alpha < n)$ y los permutamos a su vez sin alterar el orden de los demás, obtendremos $\alpha!$ permutaciones diferentes, es decir, las $n!$ permutaciones de n quedarán clasificadas en $\alpha!$ grupos distintos, pero si estos α elementos fuesen uno mismo repetido α veces en lugares diferentes, las $\alpha!$ permutaciones obtenidas serían todas iguales, puesto que no se diferenciarían en el orden de sus elementos. En consecuencia, "el número de permutaciones distintas que puedan obtenerse con n elementos, entre los cuales hay α iguales, es $n!/\alpha!$. Si ahora se supone que en estas

permutaciones tiene que haber β elementos iguales el grupo de las anteriores quedará reducido a

$$\frac{n!}{\alpha!\beta!}$$

Si se continúa razonando de este modo llegaremos a la conclusión de que "El número de permutaciones diferentes que pueden obtenerse con n elementos entre los cuales un elemento se repite α veces, otro β veces, .. , otro τ veces, será

$$\frac{n!}{\alpha!\beta!\tau!}$$

con la condición de que

$$\alpha + \beta + ... + \tau = n.$$

5.7.1.- Definiciones.

1.- Si se tienen n elementos, de los que α son iguales, β son iguales, ..., y otros τ son iguales, es decir, que uno se repite α veces, otro β veces, ..., y otro τ veces, por tanto $\alpha + \beta + ... + \tau = n$; entonces el número ***de permutaciones con repetición*** *que se pueden formar con esos n elementos y se escribe $P_n^{\alpha,\beta,...,\tau}$, viene dado por la fórmula:*

$$P_n^{\alpha,\beta,...,\tau} = \frac{n!}{\alpha!\beta!\tau!}$$

(Si un elemento no se repite, es decir, aparece una sola vez, $\alpha = 1$, no se suele poner, ya que $1! = 1$, pero hay que tener en cuenta que la suma de los que se repiten y de los que no, tiene que ser n.)

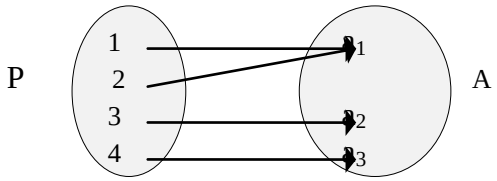
5.7.2.- Permutaciones con repetición y aplicaciones sobreyectivas.

Sea el conjunto $A = \{a_1, a_2, a_3\}$ y se va a formar todas las permutaciones posibles de cuatro elementos, en las que el a_1 entra dos veces, el a_2 y el a_3 una sola vez.

En total serán $P_4^{2,1,1} = \frac{4!}{2!1!1!} = 12$, que son las siguientes:

$\{a_1, a_1, a_2, a_3\}$	$\{a_1, a_1, a_3, a_2\}$
$\{a_1, a_2, a_1, a_3\}$	$\{a_1, a_2, a_3, a_1\}$
$\{a_1, a_3, a_1, a_2\}$	$\{a_1, a_3, a_2, a_1\}$
$\{a_2, a_1, a_1, a_3\}$	$\{a_2, a_1, a_3, a_1\}$
$\{a_2, a_3, a_2, a_1\}$	$\{a_3, a_1, a_1, a_2\}$
$\{a_3, a_1, a_2, a_1\}$	$\{a_3, a_2, a_1, a_1\}$

Si ahora se forman todas las aplicaciones sobreyectivas posibles del conjunto de cuatro elementos $P = \{1, 2, 3, 4\}$, tales que el elemento a_1 sea imagen de dos elementos de P y que y tanto a_2 como el a_3 sean imagen de un solo elemento de P, se verá que el número de aplicaciones es el mismo que de permutaciones con repetición expuestas y que los conjuntos imagen serán precisamente estas permutaciones Se puede poner por ejemplo



Corresponde a la permutación $\{a_1, a_1, a_2, a_3\}$. De una manera ordenada podrían formarse todas las demás aplicaciones sobreyectivas con las condiciones impuestas. En resumen, se puede afirmar que "Las permutaciones con repetición de n elementos en el conjunto $A = \{a_1, a_2, a_3, ..., a_n\}$, en las que el elemento a_1 se repite α veces, el a_2 β veces, el a_n τ veces (con la condición de que $\alpha + \beta + \tau = n$) son tantas como las aplicaciones sobreyectivas de un conjunto de n elementos $P = \{1, 2, 3, .. n\}$ en A, en las cuales el elemento a_1 será imagen de α elementos de P, el a_2, de β elementos de P ..., el a_n de τ elementos de P. Los conjuntos imagen constituirán las diferentes permutaciones de este tipo que son posibles.

Problema.

¿Cuántas números diferentes de 6 cifras se pueden formar de modo que tanto el 1 como el 2, como el 3 figuren dos veces en el mismo número?

Solución:

$$P_6^{2,2,2} = \frac{6!}{2!2!2!} = 90$$

5.7.3.- Permutaciones circulares.

Se llaman ***permutaciones circulares*** de *n* elementos al número de las distintas formas de colocar a *n* elementos en círculo, teniendo en cuenta que no hay primero ni último.

Dos colecciones se distinguen, por tanto en las posiciones relativas de los elementos exclusivamente, a este número se lo designa por P_c^n, y viene dado por la fórmula:

$$P_c^n = P_{n-1} = (n - 1)!$$

ya que basta fijar a uno de los elementos y permutar el resto con relación a él.

Ejemplo:

1.- Cinco fuerzas políticas se sientan a negociar en una mesa redonda y son colocados al azar.

El espacio muestral tiene como cardinal las permutaciones circulares de 5 elementos:

$$P_5^c = P_4 = 4! = 24.$$

2.- Ocho amigos se reúnen periódicamente a cenar. Lo hacen siempre en el mismo restaurante, en la misma mesa redonda. En una oportunidad, uno de ellos, gran memorioso, advierte sorprendido que esa noche cada comensal tiene a su derecha la misma persona que la vez anterior. Comenta que es una gran casualidad, pues siempre se sientan al azar y son muchas las formas que tienen de ubicarse. ¿Cuántas son?.

Solución:

Se supone primero que se han numerado las sillas y que los comensales se han sentado aleatoriamente en ellas. Se les pide ahora que todos se corran hacia la derecha tres lugares. ¿Se piensa que esta nueva disposición es distinta de la anterior?. No, si sólo nos interesa qué personas tiene a su derecha y a su izquierda cada comensal.

Sin embargo, como permutaciones son distintas, si se piensa a éstas como todas las formas posibles de hacer corresponder a cada persona un número entre 1 y 8. Ahora bien, si en vez de hacerlos correr tres lugares, se hubiera desplazado cualquier número de lugares entre uno y ocho, la conclusión hubiera sido exactamente la misma. Esto significa que, si se cuentan las permutaciones de 8 elementos, estamos contando 8 veces cada una de las disposiciones que nos interesan. Se debe dividir por 8, y , por lo tanto, el número de formas de sentarse será igual a :

$$P_8^c = P_7 = 7! = 5.040.$$

5.8.- Combinaciones con repetición.

Se llaman combinaciones con repetición n-arias , de m elementos las diversas agrupaciones que se pueden formar con dichos elementos tomados de n en n, distintos o repetidos, considerando como iguales los constituidos por los mismos elementos repetidos igual número de veces. Es decir:

Se llaman ***combinaciones con repetición*** de m elementos tomados n a n, al número de colecciones distintas que se pueden formar con n elementos de entre los m, pudiéndose repetir, donde dos colecciones son distintas exclusivamente si tienen algún elemento distinto, a este número se le designa $C^r_{m,n}$ y viene dado por la fórmula:

$$C^r_{m,n} = C_{m+n-1,\,n} = \binom{m+n-1}{n}$$

Se considera el siguiente ejemplo: Tres fuerzas políticas pretenden formar una comisión de 5 personas. El espacio muestral de todas las comisiones posibles (referidos a las fuerzas políticas que integran la comisión) es el número de combinaciones con repetición de tres elementos tomados de 5 en 5; y se calcula como:

$$C^{r}_{3,5} = C_{7,5} = \binom{5+3-1}{5} = \binom{7}{5} = 21$$

5.8.1.- Cálculo del número de combinaciones con repetición.-

Para formar las combinaciones con repetición de orden *n*, a partir de las de orden *n-1*, se va agregando a cada combinación el último de los elementos que figuran en ella y cada uno de los siguientes.

Ejemplo:

En el conjunto $A = \{ a_1, a_2, a_3 \}$ se pueden formar las siguientes combinaciones con repetición:

Binarias:

$(a_1, a_1); (a_1, a_2); (a_1, a_3); (a_2, a_2); (a_2, a_3); (a_3, a_3);$

agregando a cada combinación binaria el último de los elementos que figuran en ella y cada uno de los siguientes , se obtienen las :

Ternarias:

$(a_1, a_1, a_1); (a_1, a_1, a_2); (a_1, a_1, a_3); (a_1, a_2, a_2); (a_1, a_2, a_3); (a_1, a_3, a_3); (a_2, a_2, a_2); (a_2, a_2, a_3); (a_2, a_3, a_3); (a_3, a_3, a_3);$

y a partir de estas las

Cuaternarias:

$(a_1, a_1, a_1, a_1); (a_1, a_1, a_2, a_2); (a_1, a_1, a_3, a_3); (a_1, a_2, a_2, a_2);$
$(a_1, a_1, a_1, a_2); (a_1, a_1, a_2, a_3); (a_1, a_2, a_2, a_3); (a_1, a_1, a_1, a_3); (a_1, a_2, a_3, a_3);$
$(a_1, a_3, a_3, a_3); (a_2, a_2, a_2, a_2); (a_2, a_2, a_3, a_3); (a_2, a_3, a_3, a_3); (a_2, a_2, a_2, a_3);$
$(a_3, a_3, a_3, a_3);$

Para establecer la diferencia entre las diversas posiciones de un mismo elemento que se repite, se incrementa el subíndice de cada uno de ellos en tantas unidades como elementos le preceden en cada combinación. Así , por ejemplo la (a_1, a_2, a_2, a_4) se escribe (p_1, p_3, p_4, p_7). De este modo se logra que los índices resulten diferentes y colocados en orden creciente. Cada combinación *n*-aria de los *m* elementos de $A = \{a_1, a_2, a_3, \ldots a_m\}$ repetidos o no, quedan representados por un símbolo, que es en definitiva una combinación ordinaria de orden *n* formada en el conjunto : $P = \{p_1, p_2. \ldots p_{m+n-1}\}$.

Como resultado se obtiene que " El número de combinaciones *n*-arias con repetición de los *m* elementos de A es igual al de combinaciones ordinarias también de orden *n* , que se pueden obtener con los *m+n-1* elementos del conjunto P, o sea:

$$C^{r}_{m,n} = C_{m+n-1} = \frac{V_{(m+n-1),n}}{P_n}$$

Problema

Dados k elementos indistinguibles entre sí y n cajas, determinar el número total de formas de ubicar los k objetos en las n cajas. Por ejemplo k canarios y n jaulas.

Se puede esquematizar una distribución cualquiera de la siguiente manera:

*** * -- -- **** * 9 objetos (*) en 6 cajas __

Se puede representar esta situación en la forma siguiente

*** | * | | | **** | *

denotando las cajas con barras e indicando con el número de asterisco a izquierda el número de objetos en esa caja, salvo en la caja de la extrema derecha que no es necesario escribirla. Por ejemplo

| | | ** | | ***

describe la distribución de 5 objetos en 6 cajas de esta forma: las tres primeras vacías, la cuarta tiene 2 elementos, la quinta esta vacía y la sexta contiene 3 elementos.

Por lo tanto es esta representación aparecen n-1 barras y k puntos. En definitiva se trata de hallar todas las permutaciones de k+n-1 objetos k iguales entre si y n-1 iguales entre si.

Este número es :

$$\frac{(k+n-1)!}{k!.(n-1)!} = \binom{k+n-1}{n-1} = \binom{k+n-1}{k} \qquad (1)$$

A manera de repaso digamos que hay n^k formas posibles de distribuir k objetos distintos entre si, en n cajas (totalidad de aplicaciones de $[1, n]$ en $[1, k]$). Si ahora los objetos son *indistinguibles* el número total de posibles distribuciones es el dado por (1).

Ejemplo

1.- Un ascensor lleva 10 pasajeros y puede detenerse en cualquiera de los 12 pisos.

i) ¿ En cuántas formas pueden descender los 10 pasajeros si nos se hacen distinción de personas?

Respuesta. $\binom{10+11}{10} = \binom{21}{10} = 352.716$

ii). ¿En cuántas formas pueden descender si en cada piso desciende a lo sumo un pasajero?

Respuesta. $\binom{12}{10} = 66$

Se calculan ahora todas las aplicaciones crecientes de [1, k] en [1, n].

(Una aplicación f: [1, k] $\rightarrow$ [1, n] se dice creciente si :

$$1 \le i \le j \le k \quad \Rightarrow \quad f(i) \le f(j)).$$

Solución.

Se ve que dar una tal aplicación es dar exactamente una distribución de k objetos indistinguibles en n celdas.

Por ejemplo, sea k = 5, n = 4. A la distribución

** | * | | ** o sea $\underline{**}$ $\underline{*}$ _ $\underline{**}$

le hacemos corresponder la función creciente

1 1 2 4 4 o sea f(1) = 1; f(2) = 1; f(3) = 2; f(4) = 4 ; f(5) = 4

Por lo tanto hay:

$\binom{n}{k}$ aplicaciones estrictamente crecientes de [1, k] en [1, n]

$\binom{k+n-1}{k}$ aplicaciones crecientes de [1, k] en [1, n].

Bibliografía

-Ayres, F.: Algebra Moderna.
-Doneddu, A.: Algebra y Geometría.
-Gentile, E.: Notas de Álgebra.
-Lentin-Rivaud: Álgebra Moderna
-Pecastaigns, F.: Chemins vers l'Algèbre
-Pinzón, A. Conjuntos y estructuras.
-Queysanne, M.: Algebra Básica.
-Taylor, H- Wade, T.: Matemáticas Básicas.

Ejercicios propuestos.

Ej.1: Simplificar las expresiones siguientes ($n \in N$)

a) $\frac{n!}{(n-2)!}$ si $2 \le n$; b) $\frac{(n+2)!}{n!}$; c) $\frac{(n+2)!}{(n-2)!}$ si $2 \le n$; d) $\frac{n!}{(n-2)! \cdot 2!}$ si $2 \le n$

Ej. 2: Calcular: a) $V_{0,0}$; b) $V_{n,0}$; c) $V_{n,n-1}$; d) $V_{8,1}$; e) $A_{7,3}$; –

Ej. 3: Si en un colectivo hay 10 asientos vacíos. ¿En cuántas formas pueden sentarse 7 personas?

Ej. 4: Calcular: a) P_0 ; b) P_5 ; c) P_3 ; d) P_{n-1} ; e) P_n .

Ej. 5: ¿Cuántas permutaciones pueden formarse con las letras de silva?

Ej. 6: Calcular: a) $C_{0,0}$; b) $C_{1,0}$; c) $C_{3,0}$; d) $C_{n,0}$; e) $C_{n,1}$; f) $C_{24,20}$; g) $C_{8,5}$;

Ej. 7: Dado un conjunto X = {1, 2, 3, 4, 5}, ¿Cuántos subconjuntos de tres elementos podemos obtener en X?

Ej. 8: Calcule: a) $\binom{3}{0}$; b) $\binom{3}{2}$; c) $\binom{5}{1}$; d) $\binom{5}{4}$; e) $\binom{2}{0}$; f) $\binom{n}{0}$; g) $\binom{n}{1}$.

Ej. 9: Probar que: $2^4 = \binom{4}{0}+\binom{4}{1}+\binom{4}{2}+\binom{4}{3}+\binom{4}{4}$.

Ej.10: Determinar n tal que $3\binom{n}{4} = 5\binom{n-1}{5}$.

Ej.11: Resolver: a) $\binom{11}{2x-5} = \binom{11}{3x+1}$; b) $\binom{n}{4}+\binom{n}{k} = \binom{7}{5}$

Ej.12:Desarrollar: a) $(a + b)^4$; b) $(1 + x)^6$; c) $(2a + 3b)^4$; d) $(2x – 3y^2)^6$; e) $(1 – 2y)^5$;

f) $(x + 1/x)^6$; g) $(\frac{x}{y} + \frac{y}{x})^3$; h) $(e^x - e^{-x})^4$; i) $\left(\frac{1}{2}x + \frac{2}{x}\right)^5$; k) $(2x-y)^4 - (2y-x)^4$

Ej.13:Determinar el séptimo término de la expresión: $(3x – 2y)^{10}$.

Ej.14: Simplificar: $(a + b)^3 – 3b(a + b)^2 + 3b^2 (a + b) – b^3$.

Ej.15: Dado el conjunto X = {1, 2, 3}, determinar el número de aplicaciones de f: $X \to X$. Haga un diagrama de árbol.

Ej.16: ¿Cuántos números de cuatro dígitos pueden formarse con los dígitos 1, 2, 3, 4, 5, 6?

Ej.17: Desarrollar 2^n. (sugerencia: desarrolle usando el binomio de Newton $(1 + 1)^n$.

Ej.18: Probar que $\left(1+\frac{1}{n}\right)^n > 2$. (usar la fórmula del binomio)

6.- Cuerpo de las fracciones de un anillo conmutativo.

6.1.- Introducción.-

Sabemos que **Z** es un anillo conmutativo. Que la multiplicación no define en **Z** una estructura de grupo (los únicos elementos inversibles de **Z** son +1 y -1). El problema que se plantea para **Z** es el de hacer una extensión de **Z** a un *conjunto más vasto que sea un grupo conmutativo*. La solución de este problema conducirá a la construcción del cuerpo **Q** de los números racionales.

Estudiaremos éste problema para un anillo A cualquiera, que nos permitirá, por ejemplo aplicarlo al anillo de los polinomios en una indeterminada sobre un cuerpo y obtener el cuerpo de las fracciones racionales.

6.1.1.- Problema.

Sea A un anillo conmutativo, no necesariamente con elemento unidad. ¿Existe un cuerpo conmutativo K tal que $A \subset K$ y que A sea sub-anillo de K?.

Si la respuesta es afirmativa, entonces existirá de entre todas las soluciones para K una que sea el cuerpo más pequeño respondiendo a la pregunta, y será la intersección de todas las soluciones.

El objeto de este estudio es el de mostrar que, éste cuerpo más pequeño existe y también como se construye.

6.1.2.- Condiciones necesarias.

Supongamos que tal cuerpo existe. Entonces $A \subset K$ exige evidentemente que A sea íntegro, ya que en un cuerpo todo elemento no nulo es simplificable (no posee divisores de cero). Supongamos esta condición realizada.

Todo elemento $b \in A^*$ tiene un inverso b^{-1} en el cuerpo K. Designemos por Q la parte de K constituida de los elementos ab^{-1} cuando a recorre A y b recorre A*.

$$Q = \{ x \in K / \exists a \in A, \exists b \in A^*; x = ab^{-1} \}.$$

ab^{-1} se denomina fracción de numerador a y denominador b.

Debemos probar que Q es un cuerpo, sub-cuerpo de K.

1° *Q* es un sub-grupo multiplicativo de K*.*

Demostramos.

$$a)\ (ab^{-1} \in Q^* \text{ y } cd^{-1} \in Q^*) \Rightarrow (ab^{-1})(cd^{-1}) \in Q^*$$

En efecto, como K es un cuerpo conmutativo.

$$(1) \qquad (ab^{-1})(cd^{-1}) = (ac)(b^{-1}d^{-1}) = (ac)(bd)^{-1} \in Q^*.$$

$$(2) \qquad ab^{-1} \in Q^* \Rightarrow (ab^{-1})^{-1} \in Q^*.$$

En efecto,

$$(ab^{-1})^{-1} = ba^{-1} \in Q^*$$

2° *Q es un sub-cuerpo aditivo de K.*

Demostramos.

$$(ab^{-1} \in Q \wedge cd^{-1} \in Q) \Rightarrow (ab^{-1} - cd^{-1}) \in Q$$

En efecto,

$$ab^{-1} = adb^{-1}d^{-1} = ad(bd)^{-1}$$

$$cd^{-1} = bcb^{-1}d^{-1} = bc(bd)^{-1}$$

Que no es otra cosa que la reducción al mismo denominador.

En consecuencia,

$$ab^{-1} - cd^{-1} = (ad - bc)(bd)^{-1} \in Q$$

Q es entonces un sub-cuerpo de K; Q contiene A pues todo a de A se escribe $a = (ab)b^{-1} \in Q$.

Q es el cuerpo más pequeño que contiene a A, ya que todo cuerpo conteniendo a A debe contener ab^{-1}, cualquiera que sea $(a, b) \in AxA^*$.

Dos pares distintos (a, b) y (c, d) de AxA^* pueden dar el mismo resultado en Q, es decir, se verifica:

$$ab^{-1} = cd^{-1}$$

Observamos que:

$$ab^{-1} = cd^{-1} \Leftrightarrow ad = bc.$$

Abordaremos el estudio de la relación binaria así definida en (AxA^*) y probaremos que es una relación de equivalencia. Designaremos por Q al conjunto cociente obtenido.

Después definiremos una multiplicación y una adición en Q apoyándonos en las condiciones necesarias dadas en 1 y 2.

6.2.- Resolución del problema.

Sea A un anillo conmutativo íntegro.

Definición 1.

Se llama fracción todo par $(a, b) \in AxA^*$. El primer elemento a, se llama numerador, el segundo b denominador de la fracción.

Definición 2.

Dos fracciones (a, b) y (c, d) se dicen equivalentes si ad = bc. Se denota

$$(a, b) \equiv (c, d) \quad \Leftrightarrow \quad ad = bc.$$

El calificativo de equivalentes dadas a estas fracciones está justificada por el hecho de que la relación $\equiv$ es una equivalencia en AxA^*. En efecto

a) Es manifiestamente reflexiva;
b) es simétrica, pues: $ad = bc \Leftrightarrow cb=da$, pues el anillo A es conmutativo;
c) es transitiva. Debemos probar que:

$$[(a,b) \equiv (c,d) \quad \wedge \quad (c,d) \equiv (e,f)] \qquad \Rightarrow \qquad (a,b) \equiv (e,f)$$

Por hipótesis se tiene

$$ad = bc \quad \wedge \quad cf = de$$

entonces

$$adf = bcf \quad \wedge \quad bcf = bde$$

por consiguiente

$$adf = bde$$

Como A es íntegro y $d \neq 0$, se deduce simplificando por d,

$$af = be, \quad \text{o sea} \quad (a, b) \equiv (e, f).$$

El conjunto cociente AxA^* por esta relación de equivalencia será denotado Q. Una clase de equivalencia será denotada por la letra griega $\alpha \in Q$ o por [a, b] si se desea poner en evidencia a un representante (a, b) de la clase $\alpha = [a, b]$

6.3. - Adición.

La definición de adición en Q nos está sugerida por la condición necesaria (2), consideremos ahora la ley de composición interna en AxA* (denotada aditivamente), definida por:

$$(a, b) + (c, d) = (ad + bc, bd).$$

Esta ley es compatible con la relación de equivalencia $\equiv$:

$$[(a, b) \equiv (a', b') \wedge (c, d) \equiv (c', d')] \quad \Rightarrow \quad (ad + bc; bd) \equiv (a'd' + b'c'; b'd').$$

En efecto, por hipótesis se tiene $ab' = ba' \wedge cd' = dc'$.

Multiplicando los dos miembros de la primera igualdad por dd' y la segunda por bb' se obtiene:

$$adb'd' = bda'd' \quad \wedge \quad bcb'd' = bdb'c'.$$

Sumando miembro a miembro y por distributividad en A se obtiene:

$$(ad + bc)\, b'd = bd(a'd' + b'c').$$

La compatibilidad queda entonces demostrada.

Definición.

La suma de dos clases [a, b] y [c, d] de Q es

$$[a, b] + [c, d] = [ad + bc; bd]$$

Reducción a un mismo denominador.

Para todo anillo conmutativo A, y para toda fracción (a, b) y (c, d) de AxA*, existen dos fracciones respectivamente equivalentes que tienen el mismo denominador. Por ejemplo, si

m = bd, se tiene

$$(a, b) \equiv (ad, m) \quad \text{y} \quad (c, d) \equiv (cb, m)$$

Se dice que se han reducido las dos fracciones a un mismo denominador.

Simplificación de la adición.

Para todo $m \in A^*$ y toda fracción (a, b), se tiene :

$$(am, bm) \equiv (a, b),$$

Dado que, siendo A conmutativo am.b = bm.a

La adición toma entonces una forma más simple, si se han reducido a un mismo denominador a los representantes de las dos clases.

$$[a, m] + [b, m] = [(a + b)m, m^2] = [a + b, m]$$

Con este aspecto, es entonces inmediato que la adición en Q es conmutativo, asociativa, que admite elemento neutro, [0, m] (que, es evidentemente una clase cuando m recorre A* y que se la denota 0) y todo [a, b] tiene un opuesto -[a, b] = [-a, b].

Esta adición confiere a Q la estructura de **grupo conmutativo**.

6.4. Multiplicación.

La multiplicación en Q está sugerida por la condición necesaria (1). Consideremos la ley de composición interna en AxA* denotada multiplicativamente y definida por:

$$(a, b)\,(c, d) = (ac, bd).$$

Esta ley es compatible con la relación de equivalencia ≡:

$$[(a, b) \equiv (a', b') \wedge (c, d) \equiv (c', d')] \Rightarrow (ac, bd) \equiv (a'c', b'd').$$

En efecto, por hipótesis, se tiene ab' = ba' y cd' = dc'.

Multiplicando miembro a miembro se obtiene acb'd' = bda'c'.

La ley cociente es por definición la multiplicación en Q.

Definición.

El producto de dos clases [a, b] y [c, d] de Q es

$$[a, b] \cdot [c, d] = [ac, bd].$$

Esta multiplicación es a toda luz asociativa y conmutativa.

Dado que se ha partido de un anillo A no necesariamente con elemento unidad, ésta multiplicación en Q admite elemento neutro [m, m] (que es evidentemente una clase de Q cuando m recorre A* y que se denotará 1). En efecto para toda clase [a, b] de Q,

$$[a, b]\cdot[m, m] = [am, bm] = [a, b]$$

Por último, toda clase [a, b] de Q distinta de 0, admite un inverso. En efecto, $[a, b] \neq 0$ equivale a que $a \neq 0$ y la clase [b, a] existe en Q; además:

$$[a, b]\cdot[b, a] = [ab, ab] = 1.$$

Se concluye en que la multiplicación confiere a Q^* de la estructura de grupo conmutativo. Por último, ella es distributiva respecto de la adición:

$$([a, m] + [b, m])\cdot[c, d] = [a + b, m]\cdot[c, d] = [(a + b)c, md] = [ac + bc, md]$$

$$= [ac, md] + [bc, md] = [a, m]\cdot[c, d] + [b, m]\cdot[c, d].$$

En consecuencia, Q es un cuerpo conmutativo.

6.5.- Inmersión de A en Q.

Mostraremos primero que, para todo $a \in A$, el conjunto Ma de las fracciones (am, m) cuando m recorre A^* es una clase de Q. De manera más precisa, para todo p fijo en A^*, mostraremos que Ma = [ap, p].

1° Mostraremos que $Ma \subset [ap, p]$. En efecto, para todo $m \in A^*$:

$$amp = map \Rightarrow (am, m) \equiv (ap, p) \Rightarrow (am, m) \in [ap, p].$$

2° Por último que $[ap, p] \subset Ma$. Sea $(b, c) \in [ap, p]$. Entonces,

$$bp = cap \Rightarrow b = ca \Rightarrow (b, c) \equiv (ac, c) \in Ma.$$

Entonces Ma es la clase [ap, p] de Q. Luego la correspondencia

$$a \to [am, m] \quad (m \in A^*) \qquad \text{es una aplicación f de A en Q.}$$

f es inyectiva , pues

$$[am, m] = [bm, m] \Rightarrow am^2 = bm^2 \Rightarrow a = b.$$

f es un morfismo para la adición pues, para todo a y b de A,

$$[(a+ b)m, m] = [am, m] + [bm, m] \Rightarrow f(a+b) = f(a) + f(b) .$$

f es un morfismo para la multiplicación, pues:

$$[abm, m] = [am,m]\cdot[bm, m] \Rightarrow f(ab) = f(a)\cdot f(b)$$

En consecuencia, f(A) es un sub-anillo de Q isomorfo al anillo A.

La inmersión de A en Q consiste en identificar A y $f(A)$. Más precisamente, para todo $a \in A$ y todo $m \in A^*$, se escribe:

$$a = [am, m].$$

Se puede ver entonces que todo elemento de Q es del tipo ab^{-1} con $a \in A$ y $b \in A^*$, b^{-1} designa al inverso de b en Q. En efecto, para toda $[a, b] \in Q$ y todo $m \in A^*$,

$$[a, b] = [am, m][m, bm] = ab^{-1}.$$

En consecuencia, Q es el más pequeño cuerpo anteriormente enunciado.

Teorema 1.

Sea A un anillo conmutativo. Existe un cuerpo donde A es sub-anillo si, y solamente sí, A es integro.

Si A es íntegro, el cuerpo más chico Q donde A es sub-anillo, es único.

Definición.

Q se denomina cuerpo de las fracciones del anillo A.

Se denota más comúnmente por $a \in Q \ \wedge \ b \in Q^*$:

$$ab^{-1} = \frac{a}{b}$$

6.6.- El Cuerpo de los Números Racionales.

Si se toma el anillo íntegro $A = Z$ de los enteros, su cuerpo de fracciones es el cuerpo **Q** de los números racionales.

Una fracción es un par, denotado como $\frac{a}{b}$, de enteros $a \in Z$ y $b \in Z^*$. Se puede caracterizar a la clase de todas las fracciones equivalentes a una fracción dada $\frac{a}{b}$, es decir la familia de fracciones $\frac{x}{y}$, tales que

$$ay = bx.$$

Si $a = 0$, es la familia $\left\{\frac{0}{y}\right\}$ cuando y recorre Z^*.

Supongamos $a \neq 0$ y sea d el máximo común divisor de (a, b).

Tomamos:

$$a = da' \quad y \quad b = db'.$$

Entonces, a' y b' son primos entre sí y

$$ay = bx \Leftrightarrow a'y = b'x.$$

Como b' "divide a" b'x, "divide a" a'y. O sea, a' y b' son primos entre sí. (Por teoremas de divisibilidad, b' "divide a" y).

Existe entonces $k \in Z^*$ tal que $y = kb'$, de donde

$$b'x = a'y = kb'a' \Rightarrow x = ka'$$

La familia de las fracciones equivalentes a $\frac{a}{b}$ es entonces $\left(\frac{ka'}{kb'}\right)_{k \in Z^*}$. Es evidente que se obtiene la misma familia si k recorre solamente N*.

Ejemplo

Si $\frac{a}{b} = \frac{21}{27}$ entonces MCD = d = 3.

Tomamos $a = da'$ y $b = db'$

o sea, $21 = 3.7$ y $27 = 3.9$

7 y 9 tienen por divisor común a 1, y en N es único (son primos entre sí).

es decir, que

$$ay = bx \Leftrightarrow a'y = b'x$$

o sea

$$21y = 27x \Leftrightarrow 7.y = 9x.$$

como b' = 9 divide a 9x, también divide a 7y, entonces b' = 9 divide a y.

Tenemos que:

$$9x = 7y = k.9.7 \Rightarrow x = k.7.$$

La familia de fracciones equivalentes es $\left(\frac{k \cdot 7}{k \cdot 9}\right)_{k \in Z^*}$.

Simplificar una fracción, es encontrar una fracción equivalente donde los términos sean en valor absoluto, más pequeños. Para simplificar $\frac{a}{b}$ es suficiente reemplazar a y b por sus cocientes exactos, obtenidos al dividir por uno de sus divisores comunes. Se obtendrá la fracción equivalente más simple cuando se toman los cocientes

a'' y b'' de a y de b obtenidos al dividirlos por el m.c.d. de (a, b). La fracción $\frac{a'}{b'}$ ya no puede ser más simplificada, se dice que la fracción es irreducible.

Ejemplo:

Fracciones equivalentes a $\frac{54}{126}$

Se tiene $54 \wedge 126 = 18$, con $54 = 18 \cdot 3$ y $126 = 18 \cdot 7$.

La fracción irreducible equivalente es entonces $\frac{3}{7}$.

La familia de fracciones equivalentes es: $\left\{\frac{3}{7}, \frac{3\cdot 2}{7\cdot 2}, \frac{3\cdot 3}{7\cdot 3}, \cdots, \frac{3k}{7k}, \cdots\right\}, k \in N^*$

6.7.- Grupos conmutativos ordenados.

Sea G un grupo conmutativo, denotado aditivamente; de elemento neutro 0. Supongamos, que el conjunto G sea ordenado por una relación de orden denotada $\leq$.

Recordemos que el orden se dice trivial, si coincide con la relación de igualdad. Si el conjunto G está ordenado no trivialmente, entonces evidentemente $G \neq \{0\}$.

Definición.

Sea G un grupo conmutativo con una relación de orden $\leq$, se dice que el orden $\leq$ confiere a G de la estructura de grupo ordenado si la ley de G es compatible con la relación de orden.

Si, además, el orden es total se dice que G es un grupo totalmente ordenado.

En otros términos, $(G, \leq)$ es un grupo ordenado si $\leq$ es un orden en G y si para todo a, b y c de G;

$$a \leq b \quad \Rightarrow \quad a + c \leq b + c.$$

Es un grupo totalmente ordenado, sí, además, para todo a y b de G,

$$\text{o bien } a \leq b \text{ o bien } b \leq a.$$

Ejemplo.

El grupo aditivo de Z es totalmente ordenado por la relación de orden habitual.

2.Grupos estrictamente ordenados.

Sea $(G, \leq)$, un grupo no ordenado trivialmente. Denotamos $<$, al orden estricto inducido por $\leq$.

$$a < b \Leftrightarrow (a \leq b \wedge a \neq b).$$

Mostramos ahora que, para todos a, b, c de G,

$$a < b \Rightarrow a + c < b + c.$$

En efecto, si de tuviera $a + c = b + c$, como en G todo elemento c es simplificable, conduciría $a = b$ contrariando la hipótesis.

Se dice entonces que $(G, <)$ es un grupo estrictamente ordenado.

Recíprocamente, si $(G, <)$ es un grupo estrictamente ordenado, disignamos por $\leq$ al orden (no trivial) inducido por $<$:

$$a \leq b \Leftrightarrow (a < b \vee a = b)$$

Teorema 2.

Sea $(G, \leq)$ un grupo ordenado (orden no trivial). Si $<$ es el orden estricto deducido de $\leq$, entonces $(G, <)$ es un grupo estrictamente ordenado.

Recíprocamente, sea $(G, <)$ un grupo estrictamente ordenado. Si $\leq$ es el orden deducido de $<$, entonces $(G, \leq)$ es un grupo ordenado (orden no trivial).

6.7.1.-Caracterización de un grupo ordenado.

Sea $(G, \leq)$ un grupo conmutativo ordenado. Tomamos:

$$N = \{a \in G / a \geq 0\}.$$

A N le llamaremos cono positivo del grupo ordenado G. Observemos que:

$$a \geq 0 \Leftrightarrow a + (-a) \geq 0 + (-a) \Leftrightarrow 0 \geq -a.$$

Recordemos que, para toda parte N de un grupo G denotado aditivamente, $(-N)$ es el conjunto de los elementos opuestos a los de N. Por consiguiente:

$$(-N) = \{a \in G / a \leq 0\}.$$

La antisimetría de la relación de orden dada muestra que:

$$(a \leq 0 \wedge 0 \leq a) \Rightarrow a = 0.$$

En consecuencia:

$$N \cap (-N) = \{0\}. \qquad (1)$$

PROPIEDAD.

En todo grupo ordenado, se pueden sumar dos desigualdades miembro a miembro.

$$(a \leq b \wedge c \leq d) \Rightarrow a + c \leq b + d$$

En efecto

$$a \leq b \Rightarrow a + c \leq b + c$$
$$c \leq d \Rightarrow b + c \leq b + d$$

Es suficiente aplicar la transitividad para obtener la propiedad. En particular:

$$(a \geq 0 \wedge b \geq 0) \Rightarrow a + b \geq 0.$$

En consecuencia $N + N \subset N$. (2).

Supongamos, además, G totalmente ordenado. Entonces todo a de G es comparable a 0: o bien es $a \geq 0$ o bien es $a < 0$. Entonces,

$$N \cup (-N) = G \qquad (3)$$

Recíprocamente, sea G un grupo conmutativo y supongamos que existe una parte N de G que verifica (1) y (2). Notamos que $N \neq \Phi$, ya que (1) implica $0 \in P$.

Definimos una relación binaria en G, denotada $\leq$, como sigue:

$$a \leq b \Leftrightarrow b - a \in N.$$

Mostramos primero que esta relación es un orden en G:

1° es reflexiva pues, para todo $a \in G$, $a - a = 0 \in N$;

2° es antisimétrica. En efecto, sea $b - a \in N$ y $a - b \in N$. Entonces $-(b - a) = a - b \in (-N)$. Luego $a - b \in N \cap (-N) = \{0\}$, de donde $a = b$;

3° es transitiva. En efecto, sea $b - a \in N$ y $c - b \in N$. Entonces la relación (2) implica $(c - b) + (b - a) = c - a \in N$.

Luego $\leq$ es un orden en G. Este orden es trivial si, y solamente si, $N = \{0\}$.

Por último, este orden es compatible con la ley de G pues,

$$(\forall c \in G) \qquad a \leq b \;\Rightarrow\; b - a \in N \;\Rightarrow\; (b + c) - (a + c) \in N$$
$$\Rightarrow\; a + c \leq b + c.$$

Entonces $(G, \leq)$ es un grupo ordenado.

Ahora, supongamos, además, que la relación (3) sea verdadera y mostremos que el orden es total. En efecto, para todos a y b de G, $b - a$ pertenece a $G = N \cup (-N)$, de donde $b - a \in N \vee b - a \in (-N)$ es, decir, $a \leq b$ o $b \leq a$. Entonces el orden es total.

Teorema 3.

Sea G un grupo conmutativo.

1° Si G es un grupo ordenado por $\leq$, entonces la parte $N = \{x \in G / x \geq 0\}$ verifica:

$$N \cap (-N) = \{0\} \qquad \text{y} \qquad N + N \subset N$$

2° Recíprocamente, sea N una parte de G que verifica las dos relaciones precedentes. Entonces la relación binaria en G

$$a \leq b \quad \Leftrightarrow \quad b - a \in N$$

es un orden que confiere a G la estructura de grupo ordenado.

3° El orden es además total si, y solamente sí, $N \cup (-N) = G$.

Definición.

N se denomina cono positivo del grupo ordenado G.

El orden es trivial sí, y solamente sí, $N = \{0\}$.

Ejemplos

1.- En el grupo aditivo $\mathbf{Z}$ tomamos $N = \mathbf{N}$. Se tiene

$$\mathbf{N} \cap (-\mathbf{N}) = \{0\}, \qquad \mathbf{N} + \mathbf{N} \subset \mathbf{N}; \qquad \mathbf{N} \cup (-\mathbf{N}) = \mathbf{Z}.$$

$\mathbf{Z}$ es entonces un grupo aditivo totalmente ordenado por el cono positivo $\mathbf{N}$. Este es el orden habitual del grupo de los enteros.

2.- También en $\mathbf{Z}$ tomamos P como el conjunto de los enteros naturales pares. Se tiene.

$$P \cap (-P) = \{0\} \qquad \text{y} \qquad P + P \subset P.$$

El grupo aditivo de Z queda así ordenado por el cono positivo P de los números naturales pares. Este orden no es total pues $P \cup (-P) \neq Z$.

OBSERVACIÓN.-

Si G es un grupo ordenado no trivialmente ($N \neq \{0\}$), tomamos $N^* = N - \{0\}$. Se tiene

$$N^* \cap (-N^*) = \varnothing \qquad y \qquad N^* + N^* \subset N^*.$$

Recíprocamente, si N^* es una parte no vacía de un grupo $G \neq \{0\}$ que verifique estas dos relaciones, entonces la relación binaria en G, denotada $<$ y definida por:

$$a < b \iff b - a \in N^*$$

define sobre G la estructura de grupo estrictamente ordenado.

Corolario.

Sea $G \neq \{0\}$ un grupo conmutativo.

1.- Si G es un grupo estrictamente ordenado por $<$, entonces la parte :

$$N^* = \{x \in G / x > 0\}$$

Verifica

$$N^* \cap (-N^*) = \phi \qquad y \qquad N^* + N^* \subset N^*$$

2.-Recíprocamente, sea N^* una parte vacía de G que verifica las dos relaciones precedentes. Entonces la relación binaria en G:

$$a < b \iff b - a \in N^*,$$

es un orden que confiere a G la estructura de grupo estrictamente ordenado.

3.-El orden es además, total sí, y solamente sí:

$$N^* \cup (-N) = G - \{0\}.$$

6.8.- Anillos ordenados.

Definición.-

Sea A un anillo (no necesariamente conmutativo) y supongamos que existe sobre A una relación de orden $\leq$ tal que, el grupo aditivo (conmutativo) de A sea ordenado por esta relación. Entonces se dirá que este orden confiere a A la estructura de

anillo ordenado si además, el orden es total, se dice que A es un anillo totalmente ordenado

En otros términos, una relación de orden $\leq$ en un anillo A confiere a A la estructura de anillo ordenado si, para todos a, b, c de A:

$$a \leq b \Rightarrow a + c \leq b + c,$$
$$(c \geq 0 \wedge a \leq b) \Rightarrow (ac \leq bc \wedge ca \leq cb).$$

Ejemplo.

El anillo Z de los enteros está ordenado totalmente por la relación de orden habitual.

Sea $(A, \leq)$ un anillo ordenado. De acuerdo al estudio precedente si N es el cono positivo del grupo aditivo de A, se tiene

$$N \cap (-N) = \{0\} \quad y \quad N + N \subset N.$$

Ahora, la condición suplementaria sobre la multiplicación exige que para todos a y b de A,

$$(a \geq 0 \wedge b \geq 0 \Rightarrow ab \geq 0.$$

entonces

$$NN \subset N. \qquad (4)$$

Recíprocamente, sea A un anillo y supongamos que existe una parte N de A que verifique (1), (2), y (4).

Entonces por el teorema 3, el grupo aditivo de A está ordenado por el cono positivo N. Además, para todos a, b, c de A.

$$(c \geq 0 \wedge a \leq b) \Rightarrow (c \in N \wedge b - a \in N)$$

$$\Rightarrow c(b - a) \in NN \subset N \Rightarrow (cb - ca) \in N \Rightarrow ca \leq cb$$

Asimismo $(b - a) \in N$, de donde $ac \leq bc$

En consecuencia, A es un anillo ordenado.

Teorema 4

Sea A un anillo.

1.-Si A es un anillo ordenado por $\leq$, la parte $N = \{x \in A / x \geq 0\}$, verifica

$$N \cap (-N) = \{0\}; \qquad N + N \subset N; \qquad NN \subset N$$

2.Recíprocamente, sea N una parte de A que verifica estas tres relaciones. Luego la relación binaria en A:

$$a \leq b \quad \Leftrightarrow \quad b - a \in N,$$

es un orden que confiere a A la estructura de anillo ordenado.

Definiciones.

N se llama cono positivo del anillo ordenado A. Todo elemento de N es calificado de positivo. Todo elemento de $(-N)$ de negativo.

El orden es trivial si, y solamente si, $N = \{0\}$.

Ejemplos.

a.- En el anillo Z de los enteros se dijo ya que $N = \mathbf{N}$ es el cono positivo del grupo aditivo totalmente ordenado. Se tiene además $\mathbf{NN} \subset \mathbf{N}$. Luego Z es un anillo totalmente ordenado por el cono positivo $\mathbf{N}$.

b.- En el anillo Z, si P es el conjunto de los números naturales pares, se ha visto ya que el grupo aditivo de Z está parcialmente ordenado por el cono positivo P. Se tiene además: $PP \subset P$. entonces Z es un anillo ordenado (parcialmente) por el cono positivo P.

PROPIEDAD 2. Para todos a, b y c de un anillo ordenado A:

$$(c \leq 0 \ \wedge \ a \leq b) \quad \Rightarrow \quad (ca \geq cb \ \wedge \ ac \geq bc).$$

(La multiplicación para todo $c \leq 0$ "cambia las desigualdades".)

En efecto,

$$c \leq 0 \quad \Rightarrow \quad (-c) \geq 0 \text{ . Sea } \quad a \leq b.$$

Entonces

$$[(-c) \in N \ \wedge \ (b - a) \in N] \quad \Rightarrow \quad -c(b - a) = ac - bc \ \in NN \subset N$$

En consecuencia, $ac \geq bc$. Se demuestra asimismo que $ca \geq cb$.

PROPIEDAD 3. Si b y c son dos elementos positivos de un anillo A:

$$(a \leq b \ \wedge \ c \leq d) \quad \Rightarrow \quad (ac \leq bd \ \wedge \ ca \leq db).$$

En efecto,

$$\left.\begin{array}{l}(c \geq 0 \ \wedge \ a \leq b) \Rightarrow ac \leq bc \\ (b \geq 0 \ \wedge \ c \leq d) \Rightarrow bc \leq bd\end{array}\right\} \ \Rightarrow \ ac \leq bd.$$

En particular es legítimo multiplicar miembro a miembro dos desigualdades entre elementos todos positivos de un anillo ordenado A.

6.9.- Representación n-ádica.

Observemos algunos ejemplos, para introducir el concepto.

$$\frac{1}{2}=\frac{5}{10};\qquad \frac{1}{4}=\frac{25}{100}=\frac{20}{100}+\frac{5}{100}=\frac{2}{10}+\frac{5}{10^2};\qquad \frac{1}{20}=\frac{5}{10^2}$$

En estos tres ejemplos los denominadores quedan expresados como potencias del número 10. Es más, tienen la forma:

$$\frac{n_i}{10^i};\ \text{con}\quad 0\le n_i<10$$

Es decir es un desarrollo en las potencias $\frac{1}{10^i}$

En general, lo que se plantea es el problema de escribir un número racional $\frac{a}{b}$ en la forma:

$$\frac{a}{b}=a_0+\frac{a_1}{10}+\frac{a_2}{10^2}+\cdots+\frac{a_t}{10^t}$$

con, por supuesto, a_0 , a_1, a_2, $\cdots$, a_t elementos de **Z** y además como antes $0\le a_i<10$. Se debe observar sin embargo, que estos desarrollos son finitos, cosa que no ocurre siempre. Esto se debe a los ejemplos que hemos tomado:

$\frac{1}{2}=\frac{5}{10}=0{,}5;$ $\frac{1}{4}=\frac{25}{100}=\frac{20}{100}+\frac{5}{100}=\frac{2}{10}+\frac{5}{10^2}=0{,}25$ y finalmente $\frac{1}{20}=\frac{5}{10^2}=0{,}05.$

Decimos que estos desarrollos son finitos.

En cambio, si consideramos el número $\frac{1}{3}$, podemos observar que el desarrollo será infinito, dado que:

$$\frac{1}{3}=\frac{10}{3\cdot 10}=\frac{3\cdot 3+1}{3\cdot 10}=\frac{3}{10}+\frac{1}{3\cdot 10}=\frac{3}{10}+\frac{10}{3\cdot 10^2}=\frac{3}{10}+\frac{3\cdot 3+1}{3\cdot 10^2}=$$

$$=\frac{3}{10}+\frac{3}{10^2}+\frac{1}{3\cdot 10^2}=$$

y multiplicando y dividiendo la última fracción para obtener 10^3 en el denominador y, realizando las mismas operaciones de antes obtendríamos una expresión infinita del tipo:

$$= \frac{3}{10} + \frac{3}{10^2} + \frac{3}{10^3} + \cdots + \frac{3}{10^n} + \cdots$$

$$= 0{,}33333\cdots$$

Desarrollo n-ádico.

Planteado el problema, consideremos ahora un $\frac{p}{q} \in \mathbf{Q}$, con m > 0, sabemos que:

$p = q \cdot c_0 + r_0$ con $c_0, r_0 \in \mathbf{Z}$ y $0 < r_0 < q$, de acuerdo al algoritmo de la división de enteros.

Entonces tendremos que:

$$\frac{p}{q} = \frac{q\cdot c_0 + r_0}{q} = c_0 + \frac{r_0}{q} = c_0 + \frac{10\cdot r_0}{10\cdot q} =$$
$$= c_0 + \frac{q\cdot c_1 + r_1}{10\cdot q} = c_0 + \frac{c_1}{10} + \frac{r_1}{10\cdot q}$$

Repitiendo el mismo mecanismo se obtiene una expresión general del tipo:

$$\frac{p}{q} = c_0 + \frac{c_1}{10} + \frac{c_2}{10^2} + \frac{c_3}{10^3} + \cdots + \frac{c_n}{10^n} + \frac{r_n}{q\cdot 10^n}$$

Ejemplo.

$$\frac{212}{999} = 0 + \frac{212}{999} = \frac{2120}{10\cdot 999} = \frac{2\cdot 999 + 122}{10\cdot 999} = \quad \text{(dado que } 2120 = 2\cdot 999 + 122\text{)}$$

$$\frac{212}{999} = \frac{2}{10} + \frac{122}{10\cdot 999} = \frac{2}{10} + \frac{1220}{10^2\cdot 999} = \frac{2}{10} + \frac{1\cdot 999 + 221}{10^2\cdot 999} =$$

$$= \frac{2}{10} + \frac{1}{10^2} + \frac{221}{10^2\cdot 999} = \frac{2}{10} + \frac{1}{10^2} + \frac{2210}{10^3\cdot 999} =$$

$$= \frac{2}{10} + \frac{1}{10^2} + \frac{2\cdot 999 + 212}{10^3\cdot 999} = \frac{2}{10} + \frac{1}{10^2} + \frac{2}{10^3} + \frac{212}{10^3\cdot 999} =$$

$$= \frac{2}{10} + \frac{1}{10^2} + \frac{2}{10^3} + \frac{212}{10^3\cdot 999} = \frac{2}{10} + \frac{1}{10^2} + \frac{2}{10^3} + \frac{2120}{10^4\cdot 999} =$$

$$= \frac{2}{10} + \frac{1}{10^2} + \frac{2}{10^3} + \frac{2\cdot 999 + 122}{10^4\cdot 999} = \frac{2}{10} + \frac{1}{10^2} + \frac{2}{10^3} + \frac{2}{10^4} + \frac{122}{999}$$

y los restos se repiten. Si continuamos el desarrollo los numeradores de las fracciones serían

$$\overline{212}\ \overline{212}\ \overline{212}\cdots$$

Lema.

Todo número racional $\frac{p}{q}$ admite una representación decimal.

Esta afirmación la hemos resuelto fundamentalmente en forma intuitiva, para fundamentar mejor el lema el alumno puede recurrir a la bibliografía que se indica más abajo.

Bibliografía.

Doneddu, A. Curso de Matemáticas. Aguilar.
Gentile, E.R. Notas de Álgebra 1. EUDEBA.
Queysanne, M. Algebra Básica. Vicens-Vives.
Rivaud, J. Algebra Moderna . Reverté
Taylor, H.E.; Wade, Thomas, L. Matemáticas Básicas. Limusa S.A.

Ejercicios propuestos

Ej. 1.- Dado un número racional $\alpha \in]0, 1[$; encontrar un número $q \in \mathbf{N^*}$ tal que

$$\frac{1}{q+1} \le \alpha < \frac{1}{q}.$$

Ej. 2.- Resolver en **Q**:

a) x + ½ = ¾ ; b) $\frac{-3}{4} - 7 + 2x = 0$; c) $\frac{2}{3} - \frac{3}{5} - \frac{5}{7}x = 0$; d) $-\frac{8}{5} + \frac{3}{5} - \frac{5}{7}x = 0$.

Ej. 3.- Resolver en **Q**: a) $\frac{\frac{5}{3}+2}{\frac{3}{2}-\frac{7}{3}}x = \frac{4}{5}$; b) $\frac{\frac{5}{3}+2}{\frac{3}{2}-\frac{7}{3}} + \frac{1}{2}x = \frac{4}{5}$; c) $\frac{\frac{5}{3}+\frac{8}{3}}{\frac{3}{2}-\frac{7}{3}} - x = \frac{4}{5}$

Ej. 4.- En cada uno de los ejercicios, resolver la ecuación dada y comprobar su solución:

a) $\frac{2}{3}x + \frac{7}{3} = \frac{9}{2}$; b) $3(x + 1) + x^2 = x^2 + 12$; c) $\frac{1}{4}(x-3) - \frac{1}{5}(2x-1) = 5$;

d) $\frac{x}{5} + \frac{1}{2}(x+5) = 6$; e) $0{,}3x + 0{,}055 = -0{,}033 - 0{,}5x$; f) $\frac{x+1}{2} - \frac{2x}{5} = \frac{x-1}{2}$;

Ej. 5.- Resolver en **Q**:

a) $x^2 - 1 = 0$; b) $4x^2 + 8 = 24$; c) $x^2 + 2x = 0$; d) $4x^2 - 8x = 0$.

Ej. 6.- Resolver en **Q**:

a) $x^3 - 1 = 0$; b) $x^3 + 1 = 0$; c) $x^3 - x^2 = 0$; d) $x^3 - 9x^2 = 0$.

Ej. 7.- Resolver en **Q**:

a) $x^4 - x^3 = 0$; b) $x^4 - x^2 = 0$; c) $x^4 + x^3 = 0$; d) $x^4 + x^2 = 0$.

Ej. 8.- Resolver, factorear y comprobar el resultado.

a) $9x^2 + 9x - 4 = 0$; b) $3x^2 = 5x + 12$; c) $\frac{x+3}{2x-7} = \frac{2x-1}{x-3}$; d) $\frac{6}{u} - \frac{5}{u+2} = 3$;

e) $x(x + 3) = 18$; f) $\frac{4x}{3x-2} + \frac{5}{x} = \frac{7}{3}$; g) $(x + 3)^2 = x^2 + (x - 3)^2$.

Ej. 9.- Combine la expresión dada en una sola fracción y simplifique.

a) $\frac{x}{x-4} + \frac{-3}{4-x}$;) $\frac{3}{2x-1} + 4 - \frac{x}{1-2x}$; c) $\frac{x+2}{3x-12} + \frac{2x-1}{4-x}$; d) $\frac{9-6x+x^2}{x-1} \cdot \frac{1-x}{x-3}$;

e) $\frac{1}{x+1} + \frac{3}{(x+1)^2} - \frac{2}{x^2-1}$; f) $\frac{1}{x^2-2x+1} - \frac{1}{x^2+2x+1}$; g) $\frac{1-\frac{1}{1+x}}{1+\frac{1}{x-1}}$; h) $\frac{\frac{6x-15}{x^2-4x+4}}{\frac{10-4x}{4-x^2}}$.

Ej. 10.- Desarrollar los siguientes números racionales: a) 1/3; b) 1/7; c) $\frac{212}{999}$

7.- Números reales.

7.1.- Sistema de números reales.

- Introducción

.-Insuficiencia del conjunto de los números racionales para la solución de ecuaciones y medición.

Se sabe que el conjunto de números racionales que satisfacen la ecuación de primer grado con una incógnita: $ax + b = 0$, con a y b números racionales y $a \neq 0$ es distinto de vacío. Una proposición similar no es cierta, por lo menos para la ecuación de segundo grado; puede suceder que para a, b, $c \in \mathbf{Q}$:

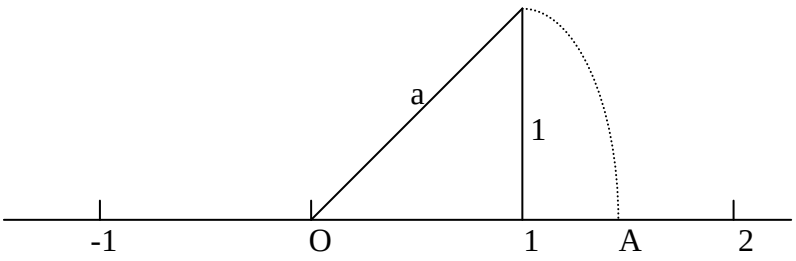
$$\{x \in \mathbf{Q} / ax^2 + bx + c = 0\} = \varnothing$$

Como ejemplo, se probará que $\{x \in \mathbf{Q} / x^2 - 2 = 0\} = \varnothing$; debemos demostrar que no existe un número racional cuyo cuadrado sea 2. Es decir, el conjunto de los números racionales es insuficiente para proporcionar soluciones a todas las ecuaciones de segundo grado. Esta insuficiencia también puede establecerse en términos geométricos:

Se sabe, que entre dos números racionales distintos cualesquiera, existe un conjunto infinito de números racionales. Por consiguiente, podríamos conjeturar que a cada punto de una recta le corresponde un número racional. Esta conjetura es falsa. Mediante una sencilla construcción geométrica vamos a localizar un punto de la recta y demostrar que no existe número racional que se corresponda con ese punto.

Supongamos un triángulo isósceles, donde cada uno de los catetos tiene longitud 1. De acuerdo al Teorema de Pitágoras nos asegura que $a^2 = 1^2 + 1^2$, o también $a^2 = 2$, donde "a" es la hipotenusa del triángulo.

Por consiguiente, si existe un número que se corresponda con la longitud de la hipotenusa, su cuadrado será 2. Construimos el triángulo de manera que uno de sus catetos, coincida con una recta.



El círculo con centro en "o" y radio "a" corta la recta en A, es decir que la longitud del segmento OA, es la longitud de la hipotenusa "a". Por lo tanto si existe un número racional que corresponda al punto A, su cuadrado debe ser 2; es decir un número racional p se corresponderá con el punto A si y solo si $p^2 = 2$.

Antes de demostrar que no existe un número racional con la propiedad de que su cuadrado vale 2, tenemos que recordar los siguientes:

Teorema 1.

Dado el magma $(\mathbf{Z}, \cdot)$,

i) el producto es una ley de composición interna en el conjunto de los enteros pares; es decir $(\mathbf{Z_p}, \cdot)$ es un magma. Es decir el producto de dos enteros pares es par.

ii) el producto es una ley de composición interna en el conjunto de los enteros impares, es decir $(\mathbf{Z_{imp}}, \cdot)$ es un magma. Es decir el producto de dos enteros impares es impar.

La demostración de i) y ii) queda como ejercicio para el estudiante.

Teorema 2.

Sea n un entero: n^2 es par $\Rightarrow$ n es par.

Demostración

Recordamos que:

$$(n^2 \text{ es par} \Rightarrow n \text{ es par}) \quad \Leftrightarrow \quad (n \text{ no es par} \Rightarrow n^2 \text{ no es par}).$$

(Implicación contrarrecíproca), entonces es cierta de acuerdo al Teorema 1.

Teorema 3.

No existe un número racional p con la propiedad de que $p^2 = 2$

Demostración

Hacemos una demostración por contradicción: suponemos que existe un número racional p con la propiedad de que $p^2 = 2$. Cómo p es un número racional, existe una fracción a/b con las propiedades de que a y b son enteros sin factores enteros comunes diferentes a 1 y -1, entonces:

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

De ésta igualdad se observa:

$$a^2 = 2b^2$$

y como b es un entero, a^2 es un entero par. Por lo tanto a es un entero par y existe un entero k con la propiedad de que $a = 2k$. Substituyendo $2k$ por a se obtiene:

$$4k^2 = 2b^2 \quad ó \quad 2k^2 = b^2,$$

donde podemos observar que b^2 *es par* y por consiguiente b es par.

Hemos demostrado que si la suposición: $p^2 = 2$. Con $p \in \mathbf{Q}$ es cierta, entonces existen enteros a y b con las siguientes propiedades.

i) a y b no tienen factores enteros comunes excepto 1 y -1 y
ii) a y b son ambos múltiplos enteros de 2.

Esto constituye una contradicción, por lo tanto la suposición es falsa y el teorema queda demostrado.

Se ha demostrado que en el conjunto de números racionales, no existe una solución para la ecuación $x^2 = 2$ y que además el punto en la recta correspondiente a la medida de la hipotenusa de un triángulo isósceles, con catetos de longitud uno, no se corresponde con ningún número racional, es decir no puede ser medido por un número racional.

El cuerpo de los números reales nos dará una solución a estos problemas. De cualquier manera conviene aclarar en este punto que, si bien el conjunto de los números reales proporciona soluciones para más ecuaciones que el conjunto de número racionales, no es adecuado para dar soluciones a todas las ecuaciones.

7.2.- El cuerpo ordenado de los números reales.

7.2.1.- Axioma del supremo.

Sea E un conjunto ordenado y A una parte no vacía y acotada superiormente de E.

Si el conjunto de las cotas superiores de A admite un mínimo m (la menor de las cotas superiores de A), entonces m se llama supremo de A, y se denota SupA. Si toda parte no vacía y acotada superiormente posee esta propiedad se dice que E satisface el ***axioma del supremo***.

Es decir: Toda parte no vacía y acotada superiormente de un conjunto ordenado E tiene supremo.

Ejemplos.

1.- El anillo ordenado **Z** (números enteros) verifica éste axioma. En efecto toda parte A no vacía y acotada superiormente de **Z** admite un elemento máximo y evidentemente MáxA = SupA.

2.- $(P(E), \subset)$ Verifica el axioma.

Propiedad 1. Sea un grupo ordenado $(G, +)$ que satisface el axioma del supremo, entonces toda parte no vacía y minorada de G admite un ínfimo, la mayor de las cotas inferiores.

Observemos primero que toda parte $A \neq \varnothing$ de un grupo G (denotado aditivamente), si a minora A entonces $(-a)$ mayora $(-A)$ y recíprocamente, pues

$$(\forall x \in A) \quad a \leq x \iff -a \geq -x$$

Supongamos que A sea minorado. Entonces $(-A)$ es mayorado y por hipóteses existe $m = \sup(-A)$. Por consiguiente $(-m)$ es minorante de A. Mostremos que $(-m)$ es el más grande minorante de A es decir, para todo minorante a de A, se tiene $a \leq -m$. En efecto, si existiera un minorante a de A tal que $a > -m$, entonces $(-a)$ sería moyorante de $(-A)$ con $-a < m$. que contradice que $m = \sup(-A)$. La propiedad queda demostrada. Se dice que G satisface también el axioma de la cota inferior.

Caracterización del supremo de A.

Sea A una parte no vacía de un grupo ordenado G y $m \in G$. Las proposiciones siguientes son equivalentes:

(1) $m = \sup A$.
(2) m es cota superior de A y, para todo $\varepsilon > 0$ en G, existe un $x \in A$ tal que, $m - x < \varepsilon$.

Demostración.

(1) $\Rightarrow$ (2). Verificar ésta implicación es equivalente a verificar su contrarrecíproca : $(\sim 2) \Rightarrow (\sim 1)$

Si se supone que existe $\varepsilon > 0$ en G tal que, para todo $x \in A$, se tiene $m - x \geq \varepsilon$, entonces $x \leq m - \varepsilon$ para todo $x \in A$ y m no es el más pequeño de las cotas superiores. Se contradice la hipótesis (1).

(2) $\Rightarrow$ (1). El método a usar para verificar ésta implicación es el mismo empleado en la anterior.

Si se supone que existe en G una cota superior de A verificando $m' < m$, entonces, eligiendo $\varepsilon = m - m' > 0$;

$$(\forall x \in A) \qquad x \leq m' < m \quad \Rightarrow \quad -x \geq -m' > -m \quad \Rightarrow \quad m - x \geq m - m' = \varepsilon$$
$$\Rightarrow \quad m - x \geq \varepsilon.$$

Y se contradice la hipótesis (2)

7.2.2.- Cuerpo de los números reales.

Se llama cuerpo de los números reales (y se lo denota **R**), a todo cuerpo conmutativo ordenado que satisface el axioma del supremo.

En consecuencia **R** satisface las tres condiciones siguientes:

1. **R** es un cuerpo conmutativo
2. Existe un orden total sobre **R**, que confiere a **R**, la estructura de cuerpo ordenado.
3. Toda parte no vacía y mayorada de **R** admite un supremo (la menor de las cotas superiores). Y el resultado de la propiedad 1, que toda parte no vacía y acotada inferiormente de **R** admite un ínfimo (la mayor de las cotas inferiores).

Se puede probar que, dos cuerpos ordenados cualesquiera respondiendo a ésta definición son isomorfos.

Se denota $\mathbf{R}_+$ el conjunto de números reales positivos, y $\mathbf{R}_+^*$ el de los números reales estrictamente positivos.

El anillo ordenado **Z** de los enteros y el cuerpo ordenado **Q** de los racionales verifican:

$$\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R};$$

Q es un sub-cuerpo de **R**.

1.- Cuerpo de los números reales

La terna $(\mathbf{R}, +, \cdot)$ tiene estructura de Cuerpo conmutativo. El alumno deberá escribir los axiomas que caracterizan a un cuerpo conmutativo.

2.- El cuerpo ordenado de los números reales

En el cuerpo ordenado **R**, se destaca un subconjunto $\mathbf{R}_*^+ \subset K$, llamado el conjunto de los elementos *estrictamente positivos* de **R** o *cono positivo*, de manera que se satisfacen las siguientes condiciones:

1.- La suma y producto de elementos estrictamente positivos son estrictamente positivos. Es decir

$$\forall\ x, y \in \mathbf{R}_*^+, \quad (x + y) \in \mathbf{R}_*^+ \quad \text{e} \quad (x \cdot y) \in \mathbf{R}_*^+ .$$

2.- $\forall\ x \in \mathbf{R}$, exactamente una y sólo una de las tres alternativas siguientes es válida:

$$\text{o bien } x = 0, \quad \text{o bien } x \in \mathbf{R}_*^+, \quad \text{o bien } -x \in \mathbf{R}_*^+$$

Asimismo, si tomamos $x \in \mathbf{R}_*^+$, indicaremos como $(-\mathbf{R}_*^+)$ al conjunto de los elementos opuestos, es decir será: $-x \in (-\mathbf{R}_*^+)$.

Tenemos entonces que $\mathbf{R} = \mathbf{R}_*^+ \cap (-\mathbf{R}_*^+) \cap \{0\}$, siendo dos a dos disjuntos (no tienen elementos comunes). A los elementos de $(-\mathbf{R}_*^+)$ les llamaremos *estrictamente negativos* o *cono negativo.* En lo que sigue lo denotaremos $\mathbf{R}_*^-$

Propiedad: En un cuerpo ordenado, cualquiera sea $a \neq 0$ entonces $a^2 \in \mathbf{R}_*^+$

En efecto, siendo $a \neq 0$, tendrá que ser: o bien $a \in \mathbf{R}_*^+$ o bien $(-a) \in \mathbf{R}_*^+$. En el primer caso, $a^2 = a \cdot a \in \mathbf{R}_*^+$. En el segundo caso $a^2 = (-a) \cdot (-a) \in \mathbf{R}_*^+$. En particular, en un cuerpo ordenado $1 \cdot 1 = 1$ y es siempre positivo. De esto se sigue que $(-1) \in \mathbf{R}_*^-$.

Por otra parte podemos asegurar que no existe ningún elemento del cuerpo ordenado **R** cuyo cuadrado sea (-1).

Ejemplos.

1.- El conjunto de los números racionales es un cuerpo ordenado.

2.- El cuerpo {0, 1} (definir las operaciones de manera que el conjunto dado tenga estructura de cuerpo), no puede ser ordenado, ya que $1 + 1 = 0$ y en un cuerpo ordenado 1 debe ser positivo y su suma también debe ser positiva.

3.- Tampoco el cuerpo $\mathbf{C_Q} = \mathbf{Q} \times \mathbf{Q}$ (conjunto de números complejos racionales) puede ser ordenado, dado que el cuadrado de $i = (0,1)$ es igual a (-1). En un cuerpo ordenado ningún cuadrado puede ser negativo y (-1) es negativo.

Notación.

En un cuerpo ordenado escribiremos $x < y$, y decimos que "x es menor que y", para significar que $z = y - x \in \mathbf{R}_*^+$, o sea que $y = x + z$, donde $z \in \mathbf{R}_*^+$ es la diferencia positiva. O también escribiremos $y > x$, que se leerá "y es mayor que x".

En particular $x > 0$ significa que $x \in \mathbf{R}_*^+$, es decir que x es positivo, en cambio $x < 0$ quiere decir que x es negativo, esto es que $(-x) \in \mathbf{R}_*^+$. Si $x \in \mathbf{R}_*^+$ e $y \in \mathbf{R}_*^-$ siempre se tendrá $x > y$.

Propiedades.

La relación de orden $x < y$ en el cuerpo ordenado **R** tiene las siguientes propiedades:

1.- **Transitividad**. Si $x < y$ e $y < z$ entonces $x < z$

2.- **Tricotomía**. Dados $x, y \in K$, ocurre un y sólo una de las alternativas siguientes: o bien $x = y$, o bien, $x < y$, o bien $x > y$.

3.- **Monotonía de la adición**. Si $x < y$ entonces, para todo $z \in \mathbf{R}$, se tiene $x + z < y + z$.

4.- **Monotonía del producto**. Si $x < y$ entonces, para todo $z > 0$, se tiene $x \cdot z < y \cdot z$.

Ahora si $z < 0$, tendrá que ser $x \cdot z > y \cdot z$.

Para demostrar estas propiedades, deberemos usar las condiciones de orden enunciados antes.

Demostración de la propiedad 1.

Decir que $x < y$ e $y < z$ significa afirmar que $y - x \in \mathbf{R}_*^+$ y $z - y \in \mathbf{R}_*^+$. Entonces sabemos que $(y - x) + (z - y \in \mathbf{R}_*^+$, simplificando será $z - x \in \mathbf{R}_*^+$, lo que significa que $x < z$.

Demostración de la propiedad 2.

Dados $x, y \in \mathbf{R}$, s e tendrá que o bien $y - x \in \mathbf{R}_*^+$, o bien $x - y = 0$, o bien $x - y \in \mathbf{R}_*^-$. Entonces por el axioma 2 de orden, tendrá que ser $x < y$, o bien $x = y$, o bien $x > y$. Y estas alternativas se excluyen mutuamente.

Demostración de la propiedad 3.

Si $x < y$ entonces $y - x \in \mathbf{R}_*^+$, sumando y restando z, se puede escribir:

$y - x = (y + z) - (x + z) \in \mathbf{R}_*^+$ y esto significa que $x + z < y + z$.

Demostración de la propiedad 4.

-Si $x < y$ e $z > 0$ tendrá que ser $y - x \in \mathbf{R}_*^+$ y $z \in \mathbf{R}_*^+$. Por consiguiente:

$(y - x)\cdot z \in \mathbf{R}_*^+$, y esto significa que $y\cdot z - x\cdot z \in \mathbf{R}_*^+$, por consiguiente $x\cdot z < y\cdot z$.

-Si $x < y$ e $z < 0$, entonces $y - x \in \mathbf{R}_*^+$ y $(-z) \in \mathbf{R}_*^+$, de donde:

$(y - x)\cdot(-z) \in \mathbf{R}^*$, es decir $x\cdot z - y\cdot z \in \mathbf{R}^*$, es decir $y\cdot z < x\cdot z$.

- En particular en el cuerpo ordenado **R**, $x < y$ implica que $-y < -x$. Basta multiplicar ambos miembros de cualesquiera de estas desigualdades por (-1) para obtener la otra.

Asimismo, podemos decir que a partir de las propiedades de orden establecidas se pueden formular unas cuantas más, algunas de ellas aparecen como ejercicios propuestos al final del tema. .

En el cuerpo ordenado **R**, escribiremos $x \leq y$ para significar que $x < y$ o $x = y$. y leeremos "x es menor o lo sumo igual que y". O también podemos escribir $y \geq x$ que leemos "y es mayor o a lo sumo igual que x", y en consecuencia, las dos expresiones son equivalentes. Es indudable que esto quiere decir que $y - x \in \mathbf{R}_*^+ \cap \{0\}$.

Al conjunto $\mathbf{R}_*^+ \cap \{0\}$ le denotaremos como $\mathbf{R}^+$, es decir tomamos $\mathbf{R}^+ = \mathbf{R}_*^+ \cap \{0\}$. A los elementos de $\mathbf{R}^+$ los denominaremos elementos *no negativos* del cuerpo **R**. A un elemento x del conjunto $\mathbf{R}^+$ se lo caracteriza como $x \geq 0$.

- Se tiene evidentemente que $x \leq x$ para todo elemento de **R**.

- Dados $x, y \in \mathbf{R}$, se tiene $x = y$ si y solamente si $x \leq y$ e $y \leq x$.

Con excepción de la propiedad 2 (tricotomía), que es sustituída por las propiedades $x \leq x$ (reflexividad) y $(x \leq y \wedge y \leq x) \Rightarrow x = y$ (antisimetría), ($\wedge$, es la conjunción y), todas las demás propiedades enunciadas antes y demostradas y por demostrar para la relación $x < y$, valen también para la relación $x \leq y$.

Considerando al conjunto de los números reales como un cuerpo conmutativo y ordenado se puede definir al conjunto de los números naturales como un conjunto inmerso en **R,** y particularmente como subconjunto de **R**. En este curso suponemos que esta definición es conocida por el alumno. Considerando a los opuestos de **N**, se puede definir al conjunto de los enteros **Z,** de manera que tenemos la siguiente relación $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{R}$

.

Más aún, dados $m, n \in \mathbf{Z}$, con $n \neq 0$, existe el inverso $n^{-1} \in \mathbf{R}$. Podemos por consiguiente definir un nuevo conjunto que contenga a todos los $m\cdot n^{-1} = \frac{m}{n} \in \mathbf{R}$, donde

m, n$\in$**Z**, y n $\neq$ 0. Evidentemente, este conjunto tendrá que ser un subcuerpo de y lo identificamos como **Q** el cuerpo de los números racionales. De manera natural podemos establecer ahora las siguientes inclusiones **N** $\subset$ **Z** $\subset$ **Q** $\subset$ **R**.

3.- El axioma del supremo.

En el cuerpo ordenado (**R, +, · , <)** se verifica el axioma del supremo. (Ver 7.2.1.) Decimos entonces que **R** es un cuerpo totalmente ordenado y completo (o continuo).

7.2.3.- Desigualdad de Bernoulli.

En el cuerpo ordenado **R**, si n$\in$**N** y $x \geq -1$, entonces $(1 + x)^n \geq 1 + nx$.

Demostración:

Esta desigualdad se demuestra por inducción sobre n. Para n = 1 es evidente.

A partir de $(1 + x)^n \geq 1 + nx$ se debe deducir que $(1 + x)^{n+1} \geq 1 + (n + 1)x$

Sabemos que $(1 + x)^{n+1} = (1 + x)^n \cdot (1 + x) \geq (1 + nx) \cdot (1 + x)$, (por hipótesis).

Desarrollando el producto podemos escribir:

$$(1 + x)^{n+1} \geq (1 + nx) \cdot (1 + x) = 1 + nx + x + nx^2 = 1 + (n + 1)x + n \cdot x^2,$$

finalmente

$$(1 + x)^{n+1} \geq 1 + (n + 1)x + n \cdot x^2 \geq 1 + (n + 1) \cdot x.$$

Cuando n > 1, n $\in$ **N** y x > -1, por el mismo argumento se tiene que:

$$(1 + x)^n > 1 + nx$$

En este punto, conviene recordar algunos conceptos que nos van a permitir estudiar con mayor amplitud las propiedades del cuerpo ordenado **R**.

Otra alternativa de explicar esta propiedad de los números reales es estudiar el problema, considerando las dos operaciones básicas, la adición y el producto en forma separada y, lo exponemos a continuación para poner en evidencia que la conmutatividad del cuerpo de los reales, puede ser obviada.

7.2.4.- Cuerpos arquimedianos

Teorema 4.

Para todo a y b de $\mathbf{R}_+^*$, existe un entero natural $n \in \mathbf{N^*}$ tal que: $an > b$.

Demostración

Supongamos lo contrario:

$$(\forall n \in \mathbf{N^*}) \qquad an \leq b$$

y mostremos que esto conduce a una contradicción. Sea $A = \{ na \}_{n \in \mathbf{N^*}}$ el conjunto de los múltiplos positivos de a.

El conjunto A está acotado superiormente por b, luego $s = \sup A$ existe. Entonces,

$$(\forall n \in \mathbf{N^*}) \qquad (n+1)a \leq s \;\Rightarrow\; na + a \leq s \;\Rightarrow\; na \leq s - a$$

Luego $s - a$ será una cota superior de A, estrictamente inferior a $s = \sup A$, lo cual constituye una contradicción.

El teorema se traduce diciendo que el *grupo aditivo de* $\mathbf{R}$ *es arquimediano*

Teorema 4 bis.

Para todo número real a y b estrictamente superiores a 1, existe un $n \in \mathbf{N}^*$ tal que, $a^n > b$.

Demostración.

En efecto, $a > 1$ implica la existencia de $\alpha \in \mathbf{R}_+^*$ tal que $a = 1 + \alpha$. Asimismo, existe $\beta \in \mathbf{R}_+^*$ tal que $b = 1 + \beta$. Ahora, la fórmula del binomio de Newton dá:

$$(\forall n \in \mathbf{N}) \qquad a^n = (1 + \alpha)^n \geq 1 + n\alpha;$$

pues, todos los términos suprimidos son positivos. Por el teorema 4, ya que $\alpha > 0$ y $\beta > 0$, existe un entero natural n tal que $n\alpha > \beta$. Por consiguiente,

$$a^n \geq 1 + n\alpha > 1 + \beta = b$$

el teorema queda demostrado.

Este teorema se traduce diciendo que, el *grupo multiplicativo* $\mathbf{R}^*$ *es arquimediano.*

Los teoremas 4 y 4 bis se traducen diciendo que **R** es un *cuerpo arquimediano.*

OBSERVACIÓN.- En las demostraciones de los dos teoremas, no hemos utilizado la conmutatividad del cuerpo **R**, enunciado en la definición. Se puede demostrar que si **R*** es un grupo multiplicativo arquimediano, es entonces un grupo conmutativo. Por consiguiente *la conmutatividad del cuerpo **R** es una consecuencia del axioma de la cota superior y puede ser obviado sin inconveniente en la definición*.

7.2.5.- Parte entera de un número real

Teorema 5.

Para todo $a \in \mathbf{R}$, *existe un entero* $q \in \mathbf{Z}$, *y sólo uno, tal que:*

$$q \leq a < q + 1$$

Definición.

q se llama parte entera de a y se denota $[a]$.

Unicidad.

Si existen q y q' en **Z** tales que $q \leq a < q+1$ y $q' \leq a < q'+1$; entonces por transitividad,

$$q < q' + 1 \qquad \text{y} \qquad q' < q + 1$$

de donde:

$$q - q' < 1 \qquad \text{y} \qquad q' - q < 1$$

que implica:

$$q - q' = 0.$$

Existencia.

1.- Supongamos $a > 0$ (si $a = 0 \Rightarrow q = 0$). Sea $A = \{n \in \mathbf{N} / n > a\}$.

A es distinto de vacío (teorema 4) y $A \subset \mathbf{N}$. Luego A admite un elemento mínimo (al menos igual a 1) que se puede denotar $q + 1$ con $q \in \mathbf{N}$. Se tiene evidentemente $a < q + 1$. Se tiene también $a \geq q$, de lo contrario $a < q$ contradice que $q + 1 = \text{mín.}A$.

2.- Finalmente supongamos $a < 0$. Entonces $(-a) > 0$, y de acuerdo a lo que precede existe un $q' \in \mathbf{N}$ tal que:

$$(q' \leq -a < q' + 1) \Rightarrow (-q' \geq a > -q' - 1) \Rightarrow (-q' - 1 < a \leq -q').$$

Si $-a = q'$, se toma $q = q'$ y la existencia queda demostrada.
Si no, se toma $q = -q' - 1$ y la existencia queda demostrada.

7.2.6.- Valor absoluto.

Definición.

Se llama valor absoluto sobre **R**, a la aplicación de **R** en $\mathbf{R}_+$, denotada

$$x \mapsto |x|$$

y definida por:

$$x \geq 0 \Rightarrow |x| = x$$
$$x < 0 \Rightarrow |x| = -x$$

OBSERVACIONES.

1º Para todo $x \in \mathbf{R}$, se tiene

$$-|x| \leq x \leq |x|$$

(Si $x \geq 0$, se tiene: $-|x| < x = |x|$. Si $x < 0$, se tiene: $-|x| = x \leq |x|$).

2º $(a \geq 0 \wedge -a \leq x \leq a) \Rightarrow |x| \leq a.$

(Si $a \geq 0$, la consecuencia es: $x \leq a$. Si $x \leq 0$, es: $-a \leq x$).

Teorema 6.

Cualesquiera que sean x e y de **R**, se tiene

1.- $|x| = 0 \Leftrightarrow x = 0;$
2.- $|x \cdot y| = |x| \cdot |y|;$
3.- $|x + y| \leq |x| + |y|;$

La demostración de 1 y 2 la debe hacer el alumno, para probar la propiedad 3, aplicamos dos veces la Observación 1º, esto es:

$$-|x| \leq x \leq |x|, \qquad -|y| \leq y \leq |y|.$$

Sumando miembro a miembro:

$$-(|x| + |y|) \leq x + y \leq |x| + |y|.$$

Es suficiente entonces aplicar la observación 2, para obtener:

$$|x + y| \leq |x| + |y|;$$

Esta relación se llama *desigualdad triangular*.

Propiedad. Para todo x e y de **R**, se tiene:

$$||x| - |y|| \leq |x - y|.$$

Observemos primero que esta relación es invariante cuando se cambia x por y. Se puede entonces suponer $|x| \geq |y|$. Tomamos $x - y = z$. Entonces,

$$x = y + z \quad \Rightarrow \quad |x| \leq |y| + |z| \quad \Rightarrow \quad |x| - |y| \leq |z|$$

La relación queda demostrada. Esta puede parangonarse a la desigualdad conocida en el triángulo: todo lado es mayor que la diferencia de los otros dos, propiedad que se deduce de la desigualdad triangular como se acaba de hacer.

OBSERVACIÓN.- Se puede definir el valor absoluto sobre todo anillo A totalmente ordenado. Se ve sin dificultad que el teorema y las propiedades son válidas cuando se reemplaza $\mathbf{R}$ por el anillo A y $\mathbf{R}_+$ por el cono positivo de A.

EJEMPLOS

1.1.- Resolver la ecuación de primer grado

$$2x + 3 = 5x - 6 \qquad (1)$$

Solución. Si x es una solución de $2x + 3 = 5x - 6$, entonces si sumamos el opuesto de 5x, y el opuesto de 3, a ambos miembros de la igualdad

$$2x + 3 + (-5x) + (-3) = 5x - 6 + (-5x) + (-3), \text{ queda}$$
$$2x + (-5x) = -6 + (-3)$$
$$-3x = -9$$

multiplicando por el inverso de (-3) o, lo que es lo mismo dividimos ambos miembros por (-3), se tendrá:

$$x = 3.$$

Esto demuestra que si x es una solución, entonces x deberá ser 3 y, por lo tanto x = 3 es la única solución posible.

Prueba. Para hacer la prueba reemplazamos x = 3 en la ecuación (1), y la igualdad tendrá que verificarse:

$$2 \cdot 3 + 3 = 5 \cdot 3 - 6$$
$$9 = 9$$

En la práctica la resolución podría ser acortada usando el conectivo lógico "si y sólo si", que se simboliza $\Leftrightarrow$, y los pasos serán "reversibles", se hace de la siguiente manera:

$$2x + 3 = 5x - 6 \quad \Leftrightarrow \quad 2x + 3 + (-5x) + (-3) = 5x - 6 + (-5x) + (-3)$$
$$\Leftrightarrow \quad -3x = -9$$
$$\Leftrightarrow \quad x = 3.$$

Finalmente escribimos el conjunto solución $S = \{3\}$.

1.2.- Resolver la ecuación cuadrática: $x^2 + x - 6 = 0$. (2)

Solución.

$$\begin{aligned} x^2 + x - 6 = 0 &\Leftrightarrow (x - 2)(x + 3) = 0 \\ &\Leftrightarrow x - 2 = 0 \quad o \quad x + 3 = 0 \\ &\Leftrightarrow x = 2 \ o \ x = -3 \end{aligned}$$

Es decir, 2 y -3 son soluciones y además son las únicas soluciones de la ecuación (2). La comprobación de este resultado la puede hacer el alumno y la solución se escribirá

$$S = \{2, -3\}$$

OBSERVACIÓN. $a^2 = b^2 \Leftrightarrow (a = b \ o \ a = -b)$.

Prueba.

$$\begin{aligned} & a^2 = b^2 \\ \Leftrightarrow \ & a^2 - b^2 = 0 \\ \Leftrightarrow \ & (a - b) \cdot (a + b) = 0 \\ \Leftrightarrow \ & a - b = 0 \quad o \quad a + b = 0 \\ \Leftrightarrow \ & (a = b \quad o \quad a = -b). \end{aligned}$$

Volviendo al Ejemplo 1.2, podemos ahora resolver la ecuación $x^2 + x - 6 = 0$, completando el cuadrado, de la siguiente manera:

$$x^2 + x - 6 = 0 \Leftrightarrow x^2 + x = 6,$$

Ahora sumamos a ambos miembros $\left(\frac{1}{2}\right)^2 = \frac{1}{4}$ de manera que el término de la izquierda de la igualdad $x^2 + x = 6$ sea un cuadrado perfecto, es decir:

$$\begin{aligned} x^2 + x - 6 = 0 &\Leftrightarrow x^2 + x = 6 \\ &\Leftrightarrow x^2 + x + \left(\frac{1}{2}\right)^2 = 6 + \frac{1}{4} \\ &\Leftrightarrow (x + \tfrac{1}{2})^2 = \frac{25}{4} \\ &\Leftrightarrow (x + \tfrac{1}{2} = \sqrt{\tfrac{25}{4}} \quad o \quad x + \tfrac{1}{2} = -\sqrt{\tfrac{25}{4}}) \\ &\Leftrightarrow (x = -\tfrac{1}{2} + \tfrac{5}{2} \quad o \quad x = -\tfrac{1}{2} - \tfrac{5}{2}) \\ &\Leftrightarrow (x = 2 \ o \ x = -3) \end{aligned}$$

Así que, el conjunto $S = \{2, -3\}$ es solución de la ecuación $x^2 + x - 6 = 0$.

1.3 – DESIGUALDADES. Para resolver desigualdades se debe recurrir a la definición axiomática de los números reales y también a algunas propiedades que surgen de esos axiomas.

- Supongamos una desigualdad del tipo $ax + b \leq 0$; con $a \neq 0$

Encontrar la solución de una desigualdad (inecuación de primer grado con una indeterminada) será, entonces determinar el conjunto de números reales para los cuales se satisface la desigualdad dada.

Solución.- Sumamos el opuesto de b a ambos miembros de $ax + b \leq 0$, es decir:

$$ax + b \leq 0 \quad \Leftrightarrow \quad ax \leq -b.$$

Para eliminar el número a del primer miembro de la desigualdad, se tienen dos casos.

1º) $a > 0$: $ax \leq -b \quad \Leftrightarrow \quad x \leq -\frac{b}{a}$ (multiplicamos por el inverso de a), y la solución vendrá dada por $S = \{x \in \mathbf{R} / x \leq -\frac{b}{a}\} =]-\infty, -b/a]$.

2º) $a < 0$: $ax \leq -b \quad \Leftrightarrow \quad x \geq -\frac{b}{a}$ (multiplicamos por el inverso de a, *como es un número menor a cero, debemos cambiar el sentido de la desigualdad*), y la solución vendrá dada por $S = \{x \in \mathbf{R} / x \geq -\frac{b}{a}\} = [-b/a, \infty[$.

1.4.- Si tenemos la desigualdad $5x + 7 > 3x - 5$, recordando que a una desigualdad, se le pueden sumar o restar números, que sigue siendo del mismo sentido, vamos a restar 7 y 3x de manera que:

$$\begin{aligned} 5x + 7 > 3x - 5 \quad &\Leftrightarrow \quad 5x + 7 - 7 - 3x > 3x - 5 - 7 - 3x \\ &\Leftrightarrow \quad 5x - 3x > -5 - 7 \\ &\Leftrightarrow \quad 2x > -12 \\ &\Leftrightarrow \quad x > -6 \end{aligned}$$

El conjunto solución lo podemos escribir con notación de intervalo como $S =]-6, \infty[$

1.5.- Desigualdades que están expresadas como productos o cociente.

Consideremos las siguientes situaciones, $(\forall a,b \in \mathbf{R})$ i) $a \cdot b < 0$, ii) $a \cdot b \geq 0$.

i) Para encontrar el conjunto solución de una desigualdad de este tipo, debemos recordar que:

$$a \cdot b < 0 \Leftrightarrow \begin{cases} 1º) \quad a > 0 \quad y \quad b < 0 \\ \qquad\qquad o \\ 2º) \quad a < 0 \quad y \quad b > 0 \end{cases}$$

El producto es negativo si los factores tienen signos distintos)

La solución se determinará encontrando las soluciones parciales S_1 y S_2 de 1º) y 2º) y finalmente la solución S de la desigualdad $a \cdot b < 0$ vendrá dada por la unión de las soluciones parciales.

ii) Para encontrar el conjunto solución de una desigualdad de este tipo, debemos recordar que:

$$a \cdot b \geq 0 \Leftrightarrow \begin{cases} 1^o) & a \geq 0 \quad y \quad b \geq 0 \\ & \quad o \\ 2^o) & a \leq 0 \quad y \quad b \leq 0 \end{cases}$$

(El producto es positivo si los factores tienen el mismo signo)

El procedimiento para escribir la solución de la desigualdad será el mismo que en el caso anterior.

NOTA.- En el caso de un cociente el concepto para encontrar la solución de la desigualdad respectiva es el mismo, en todos los casos se debe considerar la regla de los signos, como se verá en los ejemplos siguientes.

1.6.- Resolver la siguiente desigualdad de segundo grado: $x^2 + x - 6 < 0$.

Solución

Primero expresamos a la desigualdad como un producto, es decir:

$x^2 + x - 6 < 0 \Leftrightarrow (x - 2) \cdot (x + 3) < 0$, de manera que:

$$(x-2)\cdot(x+3) < 0 \Leftrightarrow \begin{cases} 1^o \begin{cases} x-2>0 \\ x+3<0 \end{cases} \Leftrightarrow \begin{cases} x > 2 \\ x < -3 \end{cases} \Rightarrow S_1 = \Phi \\ 2^o \begin{cases} x-2<0 \\ x+3>0 \end{cases} \Leftrightarrow \begin{cases} x < 2 \\ x > -3 \end{cases} \Rightarrow S_2 =]-3, 2[\end{cases}$$

y finalmente $S = S_1 \cap S_2 = \Phi \cap]-3, 2[=]-3, 2[$

1.7.- Encontrar el conjunto solución de la desigualdad dada por: $\dfrac{-x-7}{x+3} \geq 0$

Solución

En ésta desigualdad, numerador y denominador deberán tener mismo signo, ya que el cociente deberá ser positivo o cero, el denominador será distinto de cero. Es decir:

$$\frac{-x-7}{x+3} \geq 0 \Leftrightarrow \begin{cases} 1^o \begin{cases} -x-7 \geq 0 \\ x+3>0 \end{cases} \Leftrightarrow \begin{cases} -x \geq 7 \\ x > -3 \end{cases} \Leftrightarrow \begin{cases} x \leq -7 \\ x > -3 \end{cases} ; S_1 = \Phi \\ 2^o \begin{cases} -x-7 \leq 0 \\ x+3<0 \end{cases} \Leftrightarrow \begin{cases} -x \leq 7 \\ x < -3 \end{cases} \Leftrightarrow \begin{cases} x \geq -7 \\ x < -3 \end{cases} ; \quad S_2 = [-7, -3[\end{cases}$$

Es decir $S = S_1 \cap S_2 = \Phi \cap [-7, -3[= [-7, -3[$

1.8—Resolver la siguiente: $\dfrac{x-4}{x+8} < 2$.

Solución.

Sumamos (-2) a ambos miembros, para obtener una desigualdad comparable con el 0. Es decir:

$$\frac{x-4}{x+8} < 2 \Leftrightarrow \frac{x-4}{x+8} - 2 < 0 \Leftrightarrow \frac{x-4-2x-16}{x+8} < 0 \Leftrightarrow \frac{-x-20}{x+8} < 0$$

$$\frac{-x-20}{x+8} < 0 \Leftrightarrow \begin{cases} 1^o \begin{cases} -x-20>0 \\ x+8<0 \end{cases} \Leftrightarrow \begin{cases} -x>20 \\ x<-8 \end{cases} \Leftrightarrow \begin{cases} x \le -7 \\ x>-3 \end{cases} \Leftrightarrow x<-20; \quad S_1 =]-\infty,-20[\\ 2^o \begin{cases} -x-20<0 \\ x+8>0 \end{cases} \Leftrightarrow \begin{cases} -x<20 \\ x>-8 \end{cases} \Leftrightarrow \begin{cases} x>-20 \\ x>-8 \end{cases} \Leftrightarrow x>-8; \quad S_2 =]-8,\infty[\end{cases}$$

Entonces: $S = S_1 \cap S_2 =]-\infty, -20[\cap]-8, \infty[$

Ejemplos de ecuaciones y desigualdades con valor absoluto.

1.9.- Resolver las siguientes ecuaciones:

i) $|x| = 3$; ii) $|x - 5| = 10$; iii) $|2x + 4| = 8$; iv) $|2x + 4| = 8x - 1$.

Resolución: i) $|x| = 3$

i) Por definición
- si $x \ge 0$ entonces $|x| = x = 3$;
- si $x < 0$, $|x| = -x = 3$, es decir $x = -3$.

Por consiguiente el conjunto solución será: $S = \{-3, 3\}$.

Resolución: ii) $|x - 5| = 10$

ii) - si $x - 5 \ge 0$, será $|x - 5| = x - 5 = 10$, de donde $x = 10 + 5 = 15$;
- si $x - 5 < 0$, se tiene $|x - 5| = -(x - 5) = 10$, de donde $-x + 5 = 10$, es decir $x = -5$.

Luego el conjunto solución es: $S = \{-5, 15\}$

La prueba de la solución se hace reemplazando – 5 y 15 por x en las hipótesis y en la ecuación dada.

Resolución: iii) $|2x + 4| = 8$.

iii) - si $2x + 4 \geq 0$, será $|2x + 4| = 2x + 4 = 8$, de donde $x = 2$;
- si $2x + 4 < 0$, $|2x + 4| = -(2x + 4) = 8$, es decir, $2x + 4 = -8$, por lo tanto $x = -6$.

Conjunto solución : $S = \{-6, 2\}$. El Alumno debe hacer la prueba.

Resolución: iv) $|2x + 4| = 8x - 1$.

iv) - si $2x + 4 \geq 0 \Rightarrow |2x + 4| = 2x + 4 = 8x - 1 \Rightarrow 2x + 4 = 8x - 1 \Rightarrow 6x = 5 \Rightarrow$

$$x = \frac{5}{6};$$

- si $2x + 4 < 0 \Rightarrow |2x + 4| = -(2x + 4) = 8x - 1 \Rightarrow 10x = -3 \Rightarrow x = -\frac{3}{10}$.

Prueba. Si tomamos $x = -\frac{3}{10}$ y, reemplazamos en la hipótesis, $2x + 4 < 0$, nos queda $2(-3/10) + 4 < 0$ que es una contradicción. Tampoco satisface la ecuación $|2x + 4| = 8x - 1$, por consiguiente $-\frac{3}{10}$ no es un elemento del conjunto solución, en cambio $\frac{5}{6}$ si lo es, por lo tanto el conjunto solución será:

$$S = \left\{ \frac{5}{6} \right\}.$$

1.10.- Resolver las siguientes desigualdades: i) $| 6x | \leq 12$; ii) $|x - 4| < 8$; iii) $|x + 2| > 4$.

Para resolver estas desigualdades, conviene repasar la definición de valor absoluto y, las propiedades del valor absoluto.

Resolución: i) $| 6x | \leq 12$

i) Por una de las propiedades: $| 6x | \leq 12 \Leftrightarrow (-12 \leq 6x \leq 12)$; (div. todo por 6)
$\Leftrightarrow (-2 \leq x \leq 2)$,

de manera que el conjunto solución es $S = [- 2, 2]$.

Resolución: ii) $|x - 4| < 8$;

ii) $|x - 4| < 8 \Leftrightarrow (- 8 \leq x - 4 \leq 8) \Leftrightarrow (-4 \leq x \leq 12)$, (se sumó 4).

En concecuencia el conjunto solución es: $S = [-4, 12]$.

Resolución: iii) $|x + 2| > 4$

iii) Por propiedad: $|x + 2| > 4 \Leftrightarrow (x + 2 > 4 \vee x + 2 < -4)$
$\Leftrightarrow (x > 2 \vee x < -6)$.

El conjunto solución es: $S =]-\infty, -6[\cap]2, \infty[$

7.3.-Propiedades topológicas de **R**

7.3.1.-Topología.

En lo que sigue, solamente hacemos referencia al conjunto de los números reales, y hacemos un estudio sin mayores pretensiones, que la de precisar algunos conceptos relacionados con la topología y, ponernos de acuerdo en la notación de éstos.

*Como fundamento de la topología tenemos la idea de "*proximidad*" o* continuidad*. Es decir, nuestro estudio se basará en precisar que se entiende por continuo y que transformaciones conservan esta continuidad.*

Es decir la topología es la parte de la matemática que se ocupa de estudiar los conjuntos estructurados mediante relaciones que nos permitan decir cuando un elemento del conjunto es "contiguo" o próximo a una parte del mismo.

En primer lugar nos interesa definir la ***distancia*** en este conjunto y para ello necesitamos del valor absoluto que ya se ha estudiado.

7.3.2.- Distancia.

La distancia entre dos puntos $x, y \in \mathbf{R}$ se define como el valor absoluto de su diferencia:

$$d(x, y) = |x - y|$$

por ejemplo, la distancia entre -2 y 4 es igual a:

$$d(-2, 4) = |-2 - 4| = |-6| = 6$$

mientras que la distancia entre 5 y 0 es:

$$d(5, 0) = |5 - 0| = 5$$

La distancia verifica las propiedades:

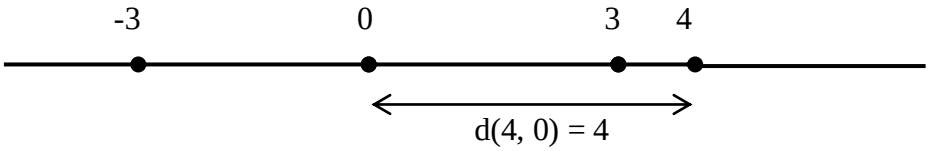
i) $d(x, y) \geq 0$, $\forall x, y \in \mathbf{R}$. La distancia entre dos puntos es siempre no negativa.
ii) $d(x,y) = 0 \Leftrightarrow x = y$. La distancia entre dos puntos es nula si y solo si ambos coinciden.
iii) $d(x, y) = d(y, x)$ $\forall x, y \in \mathbf{R}$. La distancia entre x e y es la misma que entre y y x.
iv) $d(x, y) \leq d(x, z) + d(z,y)$. $\forall x,y,z \in \mathbf{R}$. La distancia entre dos puntos es siempre menor que la suma de distancias de estos dos puntos a un tercero (desigualdad triangular).

El lector puede comprobar que estas propiedades son deducibles a partir de las del valor absoluto. Los números reales son, a menudo, representados geométricamente como puntos de una recta (que llamaremos eje real o recta real). Se elige un punto para que represente al 0 y otro a la derecha del cero para que represente al 1. Esta elección determina la escala.

Con un conjunto adecuado de axiomas para la geometría euclídea, a cada punto de la recta real le corresponde un número real y uno sólo, y recíprocamente, cada número real está representado por un punto de la recta real y uno solo. Acostumbramos a referirnos al punto x en lugar del punto de la recta asignado al número real x.

La relación de orden puede interpretarse ahora de una manera gráfica. Si $x < y$, entonces el punto x está a la izquierda del punto y :

Esta recta es también un marco apropiado para interpretar la anterior definición de distancia. En efecto, comprobaremos que lo que entendemos por distancia entre dos números reales coincide con la "distancia" entre los puntos de la recta que representan a tales números.



A nivel práctico, mediante la definición de distancia y estas representaciones podemos deducir algunas propiedades adicionales y resolver inecuaciones donde interviene el valor absoluto.

Ejemplo.-

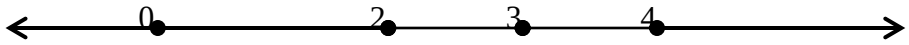
Hallar la solución de la siguiente inecuación:

$$|x - 3| \geq 1.$$

Podemos interpretar la desigualdad en el sentido de las distancias, de lo que resulta:

$$d(x, 3) \geq 1.$$

Gráficamente significa que debemos encontrar todos los puntos cuya distancia a 3 sea mayor o a lo sumo igual que uno. Es decir



Así la solución está formada de todos los números reales mayores o iguales que 4 unión con el conjunto de todos los números reales menores o iguales que 2. En símbolos:

$$]-\infty, 2] \cup [4, +\infty]$$

¿Cómo podemos determinar "la mayor o menor proximidad" de un punto $x \in \mathbf{R}$ a un subconjunto $A \subset \mathbf{R}$?. Esto se logra mediante los conjuntos que llamamos entornos de un punto.

7.3.3.- Entornos de un punto.

Un entorno abierto *centrado en un punto de la recta real "x" y de radio $r \geq 0$ es el conjunto formado por todos aquellos puntos que se encuentran a una distancia estrictamente menor de dicho punto que el valor del radio. En símbolos:*

$$E(x, r) = \{y \in \mathbf{R} / d(x, y) < r\}.$$

Ejemplo.

Hallar el entorno abierto de centro 3 y radio r = 1.

Según la definición debemos encontrar los puntos y que se encuentren a una distancia menor que 1 del punto 3. En símbolos:

$$d(3, y) < 1 \Rightarrow |3 - y| < 1.$$

Para ello podemos usar las propiedades del valor absoluto:

$$|3 - y| < 1 \Rightarrow -1 < 3 - y < 1$$

y sumando a todos los miembros el valor -3 resulta:

$$-1 < 3 - y < 1 \Rightarrow -1 + (-3) < 3 - y + (-3) < 1 + (-3) \Rightarrow -4 < -y < -2.$$

Multiplicamos todos los miembros por (-1) (lo que invierte el sentido de los símbolos de desigualdad).

$$-4 < -y < -2 \Rightarrow (-4)(-1) > (-y)(-1) > (-2)(-1) \Rightarrow 4 > y > 2.$$

El entorno abierto de centro 3 y radio 1 es pues el intervalo abierto]2, 4[

Es decir en otros términos:

Se llama entorno abierto centrado en $x_0 \in \mathbf{R}$ a todo intervalo abierto de la forma:

$]x_0 - r;\ x_0 + r[$, donde r es el radio del entorno y es un número real estrictamente positivo, $r > 0$; es decir la longitud es igual al doble del radio.

En el caso de que radio sea cero se obtiene el conjunto vacío ya que la inecuación:

$d(y, x) < 0$ no puede ser satisfecha por ningún número real.

Se llama entorno abierto de $x_0 \in \mathbf{R}$ a todo intervalo abierto que contenga a x_0. Habitualmente se entenderá que es centrado en x_0 y se designará simplemente entorno de x_0; en caso contrario se indicará.

Se designará a los entornos de x_0 de la forma U_{x_0} y, si fuese necesario, se indicará el radio del entorno escribiendo

$$U(x_0, r) =]x_0 - r, x_0 + r[= \{x \in \mathbf{R} / x_0 - r < x < x_0 + r\} =$$
$$= \{x \in \mathbf{R} / -r < x - x_0 < r\} = \{x \in \mathbf{R} / |x - x_0| < r\}$$

Se llama entorno reducido (o perforado) de x_0, y se escribe $U^*_{x_0}$ o $U^*(x_0, r)$, al conjunto $U^*_{x_0} = U_{x_0} - \{x_0\}$, es decir:

$$U^*_{x_0} =]x_0 - r, x_0[\cup]x_0, x_0 + r[= \{x \in R / 0 < |x - x_0| < r\}$$

que es el entorno de centro x_0 y radio r, excluido el punto x_0.

La primera definición sobre "proximidad" que podemos dar mediante el uso de entornos es la que sigue:

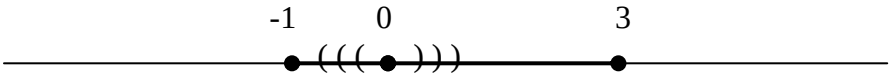
7.3.4.- Punto adherente y adherencia de un conjunto.

Un punto x es contiguo (adherente) a un determinado conjunto A si todos los entornos de x tienen puntos del conjunto A. La colección de todos los puntos adherentes a A se denomina adherencia de A y se denota por adh(A) o bien $\overline{A}$.

O sea, x es un punto adherente a $\varnothing \neq A \subset \mathbf{R}$, si y solo sí cualquiera que sea el entorno de x E(x, r) se verifica que: $A \cap E(x, r) \neq \varnothing$. Es decir la intersección del entorno de x con el conjunto A es distinta de vacío.

Ejemplo.

El punto 0 es adherente al conjunto A = [-2, 3], ya que todo entorno de 0 (cuyos extremos representamos con paréntesis "corta" a este intervalo.



Del mismo modo el punto 3 es adherente al conjunto A pues también todos sus entornos tiene puntos de dicho conjunto.

Asimismo si A = [-2, 3[, el punto 3 es de adherencia. (verificar la definición).

¿Es adherente el punto 3 si A =]-1, 2] $\cup$ {3}?.

Y el punto 0, ¿es adherente al conjunto a = {x$\in$**R**/ x = 1/n, n$\in$**N**}?.

Si el alumno hace una representación gráfica de este conjunto A podrá observar que todo entorno abierto de cero corta a algún punto de A ya que los elementos de este conjunto se "acercan" todo lo que queramos a cero. Esto significa que 0 es adherente a A. (aunque no pertenece al conjunto).

OBSERVACIÓN.-

- *Si x es un **punto adherente** al conjunto A.*
- o bien, existe un entorno U de x tal que $(U - \{x\}) \cap A = \varnothing$ y entonces x pertenece a A. Se dice que x es un ***punto aislado*** de A;
- o bien, todo entorno U de x es tal que $(U - \{x\}) \cap A \neq \varnothing$ y entonces decimos que x es un ***punto de acumulación*** de A.

Es decir un punto de adherencia, o es un punto aislado o es de acumulación.

Propiedades.

1.- Se verifica la siguiente inclusión: $A \subset \overline{A}$.

Todo punto de $\overline{A}$ es límite de una sucesión de puntos de A.

Ejemplos.

1.- La adherencia del intervalo [a, b[es [a, b].

2.- La adherencia de **Q** es **R**.

7.3.5.- Recta real ampliada.

Definición.

La recta real ampliada es el conjunto $\overline{\mathbf{R}} = \mathbf{R} \cup \{-\infty, +\infty\}$ sobre la cual es extendida la relación de orden total de **R** escribiendo:

$$\forall x \in \mathbf{R}, \qquad -\infty < x < +\infty$$

Operaciones sobre $\overline{\mathbf{R}}$.-

La adición en $\mathbf{R}$ se extiende en $\overline{\mathbf{R}}$ tomando:

* $\forall x \in \mathbf{R}$, $\quad x + (+\infty) = (+\infty) + x = +\infty; \quad (-\infty) + x = x + (-\infty)$

* $\quad (+\infty) + (+\infty) = +\infty; \quad (-\infty) + (-\infty) = -\infty$

La multiplicación en $\mathbf{R}$ se extiende en $\overline{\mathbf{R}}$ conviniendo que:

* $\forall x \in \mathbf{R}$, $\quad x > 0,\ x(+\infty) = (+\infty)\,x = +\infty; \quad x(-\infty) = (-\infty)x = -\infty;$

* $\forall x \in \mathbf{R}$, $\quad x < 0,\ x(+\infty) = (+\infty)\,x = -\infty; \quad x(-\infty) = (-\infty)x = +\infty;$

* $(+\infty)(+\infty) = +\infty; \quad (+\infty)(-\infty) = (-\infty)(+\infty) = -\infty; \quad (-\infty)(-\infty) = +\infty$

OBSERVACIÓN. La adición y la multiplicación no son dos operaciones sobre $\overline{\mathbf{R}}$ pues no están definidas:

$$(+\infty) + (-\infty); \quad (-\infty) + (+\infty); \quad 0(+\infty); \quad (+\infty)0; \quad 0(-\infty); \quad (-\infty)0.$$

También se puede extender la noción de entornos en $\overline{\mathbf{R}}$, conviniendo que una parte $\overline{U}$ de $\overline{\mathbf{R}}$ es un entorno de $+\infty$ si, y solamente si existe un $a \in \mathbf{R}$, tal que $]a, +\infty] \subset \overline{U}$, con

$$]a, +\infty] = \{ x \in \mathbf{R} / x > a\} \cup \{+\infty\}$$

y que una parte $\overline{W}$ de $\overline{\mathbf{R}}$ es un entorno de $-\infty$ si, y solamente si existe un $b \in \mathbf{R}$, tal que

$$[-\infty, b] \subset \overline{W}, \text{ con } [-\infty, b[= \{ x \in \mathbf{R} / x < b\} \cup \{-\infty\}.$$

7.4.- Punto interior, exterior y frontera. Propiedades.

7.4.1. Punto interior y conjunto interior de un conjunto.

Sea $A \subset \mathbf{R}$, se dice que $x_0 \in A$, es un *punto interior* de A, si existe un entorno de x_0 contenido en A.

x_0 es *interior* de A si y sólo sí $\exists\, U_{x0},\ U_{x0} \subset A$

Al conjunto de puntos interiores de A se le designa int(A) y se lee *interior* de A:

$$Int(A) = \{x \in A / \text{ x interior de A}\}$$

Es claro que si $x_0 \notin A$, x_0 no puede ser interior del conjunto A, es decir, $\forall U_{x0},\ U_{x0} \not\subset A$ (ya que $x_0 \in U_{x0}$ y $x_0 \notin A$). Sin embargo, no basta que $x_0 \in A$ para que sea interior, puesto que para el conjunto [0,1], $1 \in [0, 1]$ y $\forall\, U_1 \not\subset [0, 1]$, ya que $U_1 =]1 - r, 1 + r[$ con $r > 0$ y $]1 - r, 1 + r[\not\subset [0,1]$ puesto que $U_1 =]1 - r, 1 + r[$ con $r > 0$ y $]1 - r, 1 + r[\not\subset [0, 1]$ (los $x \in R$ tales que $1 < x < 1 + r$ pertenecen al entorno pero no pertenecen a [0, 1].

Por lo tanto, $Int(A) \subset A$; $\forall A \subset \mathbf{R}$.

7.4.2. Punto exterior y conjunto exterior de un conjunto.

Sea $A \subset \mathbf{R}$, se dice que $x_0 \in \mathbf{R}$, es un *punto exterior* de A si existe un entorno x_0, U_{xo} , contenido en el complemento de A, A^c, es decir $x_0 \in int(A^c)$.

Al conjunto de puntos exteriores se le designa ext(A) y se lee exterior de A.

x_0 es *exterior* de A si y sólo si $\exists\, U_{x0},\ U_{x0} \subset A^c$

7.4.3. Punto frontera y conjunto frontera de un conjunto.

Sea $A \subset \mathbf{R}$, se dice que $x_0 \in \mathbf{R}$, es *frontera* de A si todo entorno de x_0, U_{xo}, contiene puntos de A y de A^c, Al conjunto de puntos frontera de A se le designa front(A) y se lee frontera de A.

x_0 es *frontera* de A si y sólo si $\forall U_{x0}$, $U_{x0} \subset A$

Bibliografía

-Ayres, F.: Algebra Moderna.
-Doneddu, A.: Algebra y Geometría.
-Gentile, E.: Notas de Álgebra.
-Lentin-Rivaud: Álgebra Moderna
-Pecastaigns, F.: Chemins vers l'Algèbre
-Pinzón, A. Conjuntos y estructuras.
-Queysanne, M.: Algebra Básica.
-Taylor, H- Wade, T.: Matemáticas Básicas.

Ejercicios Propuestos

1.- A partir de la fundamentación axiomática de los números reales probar que:
a) $\forall\ x \in \mathbf{R}$, $x.0 = 0 = 0.x$; b) $\forall\ x \in \mathbf{R}$, $-x = (-1)\,x$; c) $\forall\ x, y \in \mathbf{R}$, $x(-y) = -(xy) = (-x)y$; d) $\forall\ x \in \mathbf{R}$, $-(-x) = x$; e) $\forall\ x, y \in \mathbf{R}$, $(-x)(-y) = xy$.

2.- Pruebe que:
a) $\forall x, y \in \mathbf{R}$, $xy = 0 \Leftrightarrow (x = 0 \vee y = 0)$; b) $\forall x, y \in \mathbf{R}$, $x^2 = y^2 \Leftrightarrow (x = y \vee x = -y)$.

3.- Pruebe que si $a, b, x \in \mathbf{R}$ y $a \neq 0$, entonces
$$ax + b = 0 \Leftrightarrow x = -a^{-1} b.$$

4.- Resuelva las siguientes ecuaciones:
a) $3x + 5 = x - 3$; b) $2x - 1 = 2x + 4$; c) $x - 2 = 7$; d) $3x + 2 = 6x + 4$.

5.- Resuelva las siguientes ecuaciones por factorización.:
a) $x^2 - 4x + 5 = 0$; b) $x^2 - 4x - 21 = 0$; c) $5x^2 + 13x + 6 = 0$; d) $x^3 + x^2 - 2x = 0$.

6.- Exprese la desigualdad dada en notación de intervalos.
a) $a \le x \le b$; b) $a < x < b$; c) $a \le x < b$; d) $x < -2$;
e) $x \ge 5$; f) $-4 \le x < 20$; g) $1/2 < x < 7/4$.

7.- Represente el intervalo dado como una desigualdad.
a) $]3/6, 6[$ b) $[-1, 5]$ c) $[20, \infty[$ d) $]-\infty, -7[$

8.- Represente gráficamente el intervalo o conjunto dados.
a) $[2, 6]$; b) $]2, 6[$; c) $[2, 6[$; d) $]2, 6]$; e) $\{x / 1 \le x \le 5\}$;
f) $\{x / -3 < x < 2\}$; g) $\{x / -2 \le x < 3\}$; h) $\{x / x \ge -1\}$; i) $\{x / x \le -3/2\}$;
j) $\{x / x > 1 \vee x > 4\}$; k) $\{x / x < 2\} \cup \{x / x \ge 0\}$; l) $\{x / x \ge -1\} \cap \{x / -3 < x < 2\}$.

9.- Expresar $A \cap B$ y $A \cup B$ como un intervalo cada uno, donde:
a) $A = [-2, 5]$, $B = [0, 8]$; b) $A = [-7, -2]$, $B = [-3, \infty[$;
c) $A =]-\infty, 0]$, $B = [0, \infty[$; d) $A = [-10, 2[$, $B =]3, 10]$.

10.- Recordando las definiciones de $\subset$, $\not\subset$, indique cuáles de las siguientes proposiciones es cierta o falsa:
a) $[1, 4] \subset [0, 5]$; b) $[2, 3] \subset]2, 3[$; c) $[1, 2] \not\subset [2, 3]$; d) $]-4, 4[\subset]-\infty, \infty[$.

11.- Resuelva las siguientes ecuaciones completando el cuadrado.:
a) $x^2 - 4x + 5 = 0$; b) $3x^2 - 11x + 6 = 0$; c) $5x^2 + 3x + 2 = 0$; d) $5x^2 + 3x - 2 = 0$.

12.- Pruebe que, para $x, y, z, u, v \in \mathbf{R}$
a) $(x < y \wedge u < v) \Rightarrow (x + u < y + v)$; b) $x < y \Rightarrow -x > -y$;
c) $(x < y \wedge z < 0) \Rightarrow (xz > yz)$; d) $x \neq 0 \Rightarrow x^2 > 0$;
e) $(0 \le x < y \wedge 0 \le u < v) \Rightarrow xu < yv$; f) Si x, y tienen el mismo signo: $xy > 0$;
g) Si x, y tienen signo distinto: $xy < 0$.

13.- Pruebe que para $x, y \in \mathbf{R}$:

a) x^{-1} tiene el mismo signo que x; b) Si x, y tienen el mismo signo e $x < y$, entonces $x^{-1} > y^{-1}$; c) $[(x \geq 0 \ \wedge \ y \geq 0) \Rightarrow x^2 > y^2 \ ] \Leftrightarrow x > y$.

14.- Demuestre que:

a) $x \in [2, 4] \Rightarrow (2x + 3) \in [7, 11]$; b) $x \in]2, 4[\Rightarrow 1/(2x + 3) \in]1/11, 1/7 [$;
c) $(x - 5) \in [-2, 2] \Rightarrow x \in [3, 7]$; d) $(2x - 6) \in]-4, 4[\Rightarrow x \in]1, 5[$;
e) $(x - x_0) \in [-a, a] \Rightarrow x \in [x_0 - a, x_0 + a]$; f) $x \in [x_0 - a, x_0 + a] \Rightarrow (x - x_0) \in [-a, a]$.

15.- Resuelva las siguientes desigualdades:

a) $x + 5 > 2 - x$; b) $4x + 1 < 2x + 3$; c) $11x - 7 \leq 4x + 2$.

16.- Pruebe que: a) $x > 1 \Rightarrow x^2 > x$; b) $0 < x < 1 \Rightarrow x^2 < x$.

17.- Resuelva las siguientes desigualdades:

a) $x^2 - 5x + 6 < 0$; b) $x^2 - 3x - 4 > 0$; c) $- x^2 + 3x - 2 > 0$; d) $-1 \geq 4x - 7 \geq -2$;
e) $\frac{1}{2x+1} < -3$; f) $\frac{10 - x}{4x - 7} < 5$; g) $\frac{2x^2 - 1}{x + 2} < 3$.

18.- Para los siguientes conjuntos de números reales, determinar, en caso que existan, cota superior, cota inferior, supremo, ínfimo, máximo y/o mínimo.

a) $A = \{x^2; -1 < x < 1\}$; b) $B = \{x^2; 0 \leq x < 1\}$; c) $]-\infty, b[$ d) $S_1 = \{n/n \in Z^+\}$;
e) $S_2 = \{(1/n)/ \ n \in Z^+\}$; f) $]2, 7[$ g) $[-3, 5]$.

19.- Pruebe que:

a) $|x| = y \Leftrightarrow (y \geq 0 \ \wedge (-x = y \ \vee \ x = y))$; b) $|x| < y \Leftrightarrow (-y < x < y)$;
c) $|x| > y \Leftrightarrow (x < -y \vee x > y)$.

20.- Pruebe que: $|x| = |y| \Leftrightarrow x = y \ \vee \ x = -y$.

21.- Recordando la definición de valor absoluto de un número real, completar las líneas de punto.

a) Si $4 - a$ es un número negativo, $|4 - a| =$ .....
b) Si a es mayor o igual que -10, $|a + 10| =$ .....

22.- Represente gráficamente las siguientes relaciones:

a) $|x - 3| < 2$; b) $|x - 3| > 2$; c) $|x - 3| = 2$.

23.- Resolver:

a) $|x| = 2$ b) $|- x| = 2$; c) $|2x - 5| = 4$; d) $|x^2 - 1| = 0$; e) $|(1/2)x^2 + 3| = -2$.

24.- Resuelva las siguientes ecuaciones:

a) $|x + 3| = 7$; b) $|2x + 3| = 2x + 3$; c) $|x^2 - 4| = -2x + 4$;
d) $|x^2 + 2| = 2x + 1$; e) $|3x - 5| + x - 7 = 0$.

25.- Resuelva las siguientes desigualdades:

a) $|5x| < 2$; b) $|x/3| < 2$; c) $|x - 2| < 3$; d) $|x + 3| > 7$; e) $|x + 3| \leq 5$;
f) $|x - 4| \leq 3$; g) $|x + 5| < 2x - 3$; h) $|x^2 - 4| < -2x + 4$; i) $|x^2 - 4| > -2x + 4$.

26.- Encuentre un número positivo δ apropiado para el cual se satisfacen las siguientes implicaciones:

a) $|x - 1| < \delta \Rightarrow |4x - 4| < 1$; b) $(|x + 1| < \delta \wedge \delta < 1) \Rightarrow |x^2 - 1| < 1/2$;

c) $(|x - 1| < \delta \wedge \delta < 1) \Rightarrow |2x^2 - 4x + 2| < 1/10$;

d) $(|x + 2| < \delta \wedge \delta < 2) \Rightarrow |x^2 - 4| < \varepsilon$, en donde ε es un número positivo arbitrario.

27.- Escribir como intervalos y como entornos (si es posible), los siguientes conjuntos de números reales:

$A = \{x / 2 \leq x \leq 4\}$; $B = \{x / -1 < x < 3\}$; $C = \{x / -1 < x \leq 3\}$

$D = \{x / -7 \leq x < -2\}$; $E = \{x / -3 < x < -1\}$; $F = \{x / |x - 2| < 5\}$

$G = \{x / 0 < |x - 3| < 1\}$; $H = |x - 2| < \delta$, $\delta > 0$.

28.- Para cada uno de los siguientes conjuntos, dar un entorno con centro en el origen, que lo incluya:

$A = \{x / -2 \leq x \leq 4\}$; $B = \{x / -10 < x < 7\}$; $C = \{x / |x| < 2\}$

29.- Si $M =]1, 3] \cup \{4\} \cup [6, 7[$, decir cuál es la adherencia de M (conjunto de puntos adherentes a M)

30.- Para los siguientes subconjuntos de R, hállese el conjunto derivado (conjunto de los puntos de acumulación):

a) $\{(1/n), n \in N\}$ b) $\{x / x \in Q \wedge (|x - 1| < 3 \vee x = -3\}$ c) $]1, 2] \cup \{3\}$

31.- Determine el conjunto derivado del conjunto C, si $C = [a, b]$; $C =]a, b[$; $C = N$

$C = Q$; $C = R$.

CONTENIDO de ÁLGEBRA CUADERNO 1.

v.w.