ÁLGEBRA BÁSICA

RESÚMENES TEÓRICOS

TEORÍA DE CONJUNTOS

RESUMEN TEÓRICO

1.- Conjuntos.

Un **CONJUNTO** es cualquier clase, colección o familia de objetos. A dichos objetos los llamaremos **ELEMENTOS**.

Los conjuntos se representan por letras mayúsculas y sus elementos por letras minúsculas.

Diremos que un elemento **a** pertenece a un conjunto **A** si forma parte de él **($a \in A$)**.

Un conjunto puede definirse:

- **POR EXTENSIÓN**: enumerando todos sus elementos uno a uno, normalmente se hace entre llaves. A = { a, e, i, o, u }

- **POR COMPRENSIÓN**: dando una propiedad que caracterice inequívocamente a todos sus elementos. A = { vocales }

SUBCONJUNTO: Si todo elemento del conjunto B también pertenece a A, diremos que B es subconjunto de A o que B está incluido en A **($B \subset A$)** o sea:

$$\forall x \in B,\ x \in A \rightarrow B \subset A$$

CONJUNTO VACÍO: Se representa por ϕ y es el conjunto que no tiene

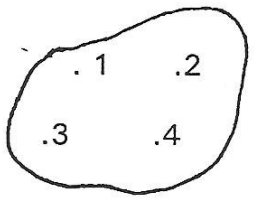
elementos.

CONJUNTO FINITO/INFINITO: cuando tiene un número finito/infinito de elementos.

CARDINAL DE UN CONJUNTO FINITO A (Card(A)) es el número de elementos del conjunto.

DIAGRAMAS DE VENN: Son líneas cerradas arbitrarias que, se supone, encierran a los elementos de los conjuntos representados:

A = { 1, 2, 3, 4 }



D. Venn.

2.- Operaciones entre conjuntos.-

Dos conjuntos **A** y **B** son **IGUALES** (A = B) cuando tienen los mismos elementos.

Para demostrar que dos conjuntos son iguales se empleará, normalmente, la doble inclusión:

$$A = B \leftrightarrow (A \subset B) \; y \; (B \subset A)$$

Dado un conjunto A, subconjunto de un conjunto de referencia U (llamado conjunto universal), llamamos **CONJUNTO COMPLEMENTARIO DE A,** escrito **A'**, al conjunto de los elementos de U que no pertenecen a A, es decir:

$$A' = \{ x \in U / \; x \notin A \}$$

Se llama **INTERSECCIÓN DE LOS CONJUNTOS A y B,** y se representa por **A ∩ B,** al subconjunto de ambos que está formado por los elementos comunes a **A** y a **B,** es decir:

$$A \cap B = \{ x / \; x \in A \; y \; x \in B \}$$

Se llama **UNIÓN DE LOS CONJUNTOS A y B,** y se representa por **A U B,** al conjunto formado por los elementos que pertenecen, al menos, a uno de los dos conjuntos, **A ó B,** es decir:

$$A \cup B = \{ x / \ x \in A \text{ ó } x \in B \}$$

Se llama **DIFERENCIA DE LOS CONJUNTOS A y B**, y se representa **A-B**, al conjunto de los elementos que perteneciendo a **A**, no pertenecen a **B**, simbólicamente:

$$A-B = \{ x / \ x \in A \text{ y } x \notin B \} = A \cap B'$$

Las propiedades más interesantes de la unión, intersección y complementario son:

LEYES DEL ALGEBRA DE CONJUNTOS

LEYES	UNIÓN	INTERSECCIÓN
1. DE IDEMPOTENCIA	$A \cup A = A$	$A \cap A = A$
2. ASOCIATIVAS	$AU(BUC) = (AUB)UC$	$A\cap(B\cap C) = (A\cap B)\cap C$
3. DISTRIBUTIVAS	$AU(B\cap C) = (AUB)\cap(AUC)$	$A\cap(BUC) = (A\cap B)U(A\cap C)$
4. CONMUTATIVAS	$AUB=BUA$	$A\cap B=B\cap A$
5. DE IDENTIDAD	$AU\phi=A, AUU=U$	$A\cap\phi=\phi, A\cap U=A$
6. COMPLEMENTARIO	$AUA'=U, \ (A')'=A, \ U'=\phi$	$\phi'=U, \ A\cap A'=\phi$
7. DE MORGAN	$(AUB)'=A'\cap B'$	$(A\cap B)'=A'UB'$

Se llama **CONJUNTO DE LAS PARTES DE UN CONJUNTO A**, y se representa por **P(A)**, al conjunto cuyos elementos son todos los subconjuntos de **A**, es decir:

$$P(A) = \{ B \ / \ B \subset A \}$$

Dada una familia de subconjuntos de **A**: $A_1, A_2, \ldots, A_n \ldots$ (finita o no), decimos que constituyen un **RECUBRIMIENTO DE A** si verifican:

1) $\forall A_i \subset A; A_i \neq \phi \quad i=1,2,\ldots$

2) $A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots = A$

Se llama **PARTICIÓN DE UN CONJUNTO A**, a todo **RECUBRIMIENTO** de él que verifique:

$$\forall A_i, A_j, i \neq j, A_i \cap A_j = \phi$$

1.3.- Conjunto producto cartesiano.

Dados dos elementos **a** y **b**, se denomina **PAR ORDENADO** a la agrupación de dichos elementos en un cierto orden. Lo representaremos por **(a,b)**, en donde **a** y **b** se denominan **PRIMER y SEGUNDO ELEMENTO DEL PAR.**

Diremos que los pares **(a,b)** y **(c,d)** son **IGUALES** si $a=c$ y $b=d$.

Se llama **PRODUCTO CARTESIANO DE DOS CONJUNTOS A y B,** al conjunto (escrito **AxB**) cuyos elementos son todos los posibles pares ordenados **(a,b)** que se puedan formar, tales que $a \in A$ y $b \in B$, es decir:

$$AxB = \{ (a, b) \ / \ a \in A \ y \ b \in B \}$$

RELACIONES ENTRE CONJUNTOS

RESUMEN TEÓRICO

1.- Relaciones binarias.-

Una **RELACIÓN BINARIA** definida en un conjunto A es un subconjunto G del producto cartesiano AxA. Se representa por R.

Si efectuamos una representación puntual del conjunto AxA, se denomina **GRAFO DE LA RELACIÓN BINARIA R**, al lugar geométrico de todos los puntos del subconjunto G.

$$G = \{(a, b) \in AxA \,/\, aRb\}$$

Al conjunto $\{ a \in A \,/\, \exists b \in A : aRb \}$ se llama **CONJUNTO ORIGEN.**

Al conjunto $\{ b \in A \,/\, \exists a \in A : aRb \}$ se llama **CONJUNTO DE LAS IMÁGENES.**

2.- Propiedades de la relación binaria sobre un conjunto.-

Sea A un conjunto sobre el que se ha definido una relación binaria **R.**

II . 2

1.- Diremos que R es **REFLEXIVA** si:

$$\forall\, a \in A,\ aRa \quad \acute{o} \quad \forall\, a \in A:\ (a, a) \in G$$

2.- La relación binaria R es **SIMÉTRICA** si:

$$\forall\, a, b \in A \,/\ aRb \Rightarrow bRa \quad \acute{o} \quad \forall\, (a, b) \in G:\ (b, a) \in G$$

3.- La relación R es **ANTISIMÉTRICA** si:

$$\forall\, a, b \in A \,/\ aRb \text{ y } bRa \Rightarrow a = b \quad \acute{o} \quad \forall\, (a, b) \in G:\ (b, a) \notin G$$

4.- Se dice que la relación binaria R es **TRANSITIVA** si:

$$\forall\, a, b, c \in A \,/\ aRb \text{ y } bRc \Rightarrow aRc$$

$$\acute{o}$$

$$\forall\, (a, b), (b, c) \in G:\ (a, c) \in G$$

3.- Relación de equivalencia: Clases de equivalencia.-

Una relación binaria R definida sobre un conjunto A, se dice que es una **RELACIÓN DE EQUIVALENCIA** si cumple las propiedades:

- *Reflexiva*
- *Simétrica*
- *Transitiva*

Sea R una relación de equivalencia definida en un conjunto A. Se denomina **CLASE DE EQUIVALENCIA** de un elemento $a \in A$ al conjunto de todos los elementos de A que están relacionados con a:

$$[a] = \{ x \in A \,/\ xRa \} = \{ x \in A \,/\ aRx \} =$$

$$= \{ x \in A \,/\ (a, x) \in G \} = \{ x \in A \,/\ (x, a) \in G \}$$

4.- Teorema fundamental de las relaciones de equivalencia: Conjunto cociente.-

TEOREMA: 1.- Toda relación de equivalencia R definida sobre un conjunto A efectúa en él una partición P = { [a], [b], ... } en clases de equivalencia.

2.- Recíprocamente, toda partición P(A) = { A_1, A_2, ... } define sobre A una relación de equivalencia.

El conjunto o partición P, formado por todas las clases de equivalencia, determinado en A por la relación R, recibe el nombre de **CONJUNTO COCIENTE (A/R).**

5.- Relación de orden.-

Una relación binaria R sobre un conjunto A, se dice **RELACIÓN DE ORDEN** si a la vez es reflexiva, antisimétrica y transitiva.

Cuando en un conjunto se ha establecido una relación de orden, diremos que el conjunto esta ordenado por esa relación.

Cuando cualquier elemento de A esta relacionado con todos los demás se dice que R es de **ORDEN TOTAL** y que **A ESTA TOTALMENTE ORDENADO.**

Si en A existe al menos un elemento no relacionado con todos los demás entonces R es de **ORDEN PARCIAL** y **A ESTA PARCIALMENTE ORDENADO.**

En el caso de que la relación binaria definida sobre A solo cumpla las propiedades antisimétrica y transitiva, se dice que es una relación de **ORDEN ESTRICTO EN A.**

■

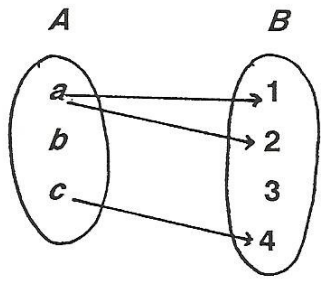
APLICACIONES ENTRE CONJUNTOS

RESUMEN TEÓRICO

1.- Correspondencias.-

Dados dos conjuntos A y B, se llama **GRAFO** a todo subconjunto de AxB.

Dados dos conjuntos no vacíos A y B y un grafo $G \subset AxB$, diremos que G define una **CORRESPONDENCIA** entre A y B, que representaremos por f: A ————> B, y que relaciona elementos de A con elementos de B de forma que un elemento de A esta relacionado con uno de B por f, si el par formado por ellos pertenece al grafo G.



f: $G = \{ (a, 1), (a, 3), (c, 4) \}$

A: Conjunto inicial: In(f)
B: Conjunto final: Fin (f).

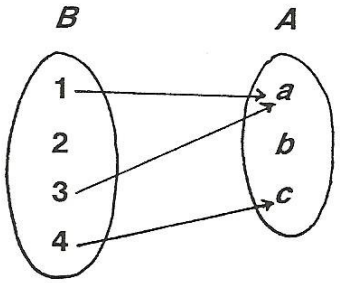
Se llaman **ELEMENTOS ORIGINALES** a aquellos del conjunto A que están relacionados con uno o varios del conjunto final. Su reunión forma el **CONJUNTO ORIGINAL** de la correspondencia, Or(f), o **DOMINIO** de la correspondencia, Dom(f).

Se llaman **IMÁGENES** a aquellos elementos del conjunto final relacionados por f con uno o algunos de los del conjunto inicial, su reunión forma el **CONJUNTO IMAGEN**, Im(f).

$$ORIGINAL(f) \subset INICIAL\ (f)$$
$$IMAGEN(f) \subset FINAL(f)$$

Dos elementos, uno del conjunto original y otro del conjunto imagen, se dicen que son **HOMÓLOGOS** en la correspondencia f cuando el par formado por ellos pertenece a G.

Dada una correspondencia f entre los conjuntos A y B, y su grafo G, se llama **CORRESPONDENCIA INVERSA** de f, y se representa por f^{-1}, a la correspondencia entre B y A que se obtiene al invertir las parejas del grafo G, en el ejemplo anterior:



$$f^{-1}: G^t = \{ (1, a), (3, a), (4, c) \}$$

2.- Aplicaciones o funciones.-

Se llama **APLICACIÓN** o **FUNCIÓN** entre los conjuntos A y B, a una correspondencia en la que todo elemento del conjunto inicial está relacionado con un único elemento del conjunto final.

$$f: A \longrightarrow B \text{ es aplicación o función}$$
$$\forall x \in A,\ \exists |\ y \in B /\ y = f(x)$$

Si f es una aplicación entre los conjuntos A y B, y $A^* \subset A$, se llama

RESTRICCIÓN DE f AL CONJUNTO A^* a la aplicación f_r entre A^* y B tal que:

$$\forall x \in A^*, \quad f_r(x) = f(x)$$

Si f es una aplicación entre los conjuntos A y B, y $A \subset C$, se llama **EXTENSIÓN DE f AL CONJUNTO C** a la aplicación f_e entre C y B tal que:

$$\forall x \in C, \quad f_e(x) = f(x)$$

3.- Aplicaciones inyectivas.-

Una aplicación entre dos conjuntos A y B es **INYECTIVA** cuando todo elemento de B es imagen a lo sumo de un elemento de A. Simbólicamente puede expresarse de dos formas:

1. - $\forall x, x' \in A, \; si \; x \neq x' \Rightarrow f(x) \neq f(x')$
2. - $Si \; f(x) = f(x') \Rightarrow x = x'$

4.- Aplicaciones suprayectivas o sobreyectivas.-

Una aplicación entre dos conjuntos A y B es **SUPRAYECTIVA** cuando todo elemento de B sea imagen de al menos un elemento de A, es decir:

$$\forall y \in B, \; \exists x \in A / \; y = f(x)$$

5.- Aplicaciones biyectivas.-

Una aplicación definida entre dos conjuntos A y B diremos que es **BIYECTIVA** cuando sea inyectiva y suprayectiva a la vez, o también, cuando todo elemento del conjunto final es imagen de un único elemento del conjunto inicial:

$$\forall y \in B, \; \exists! \; x \in A / \; y = f(x)$$

6.- Aplicación o función inversa.-

Dada una aplicación biyectiva f, entre dos conjuntos A y B, se llama **APLICACIÓN INVERSA** de f y se representa por f^{-1}, a la correspondencia inversa de f.

Regla para calcular la aplicación inversa de una aplicación biyectiva:

Sea la aplicación f: A ——————> B
x ——————> y = f(x)

1.- Se despeja la x.
2.- Se sustituye y por x , x por y.

7.- Composición o producto de aplicaciones.-

Sean f: A ——> B y g: B ——> C dos aplicaciones tales que fin(f) = or(g). Se llama **PRODUCTO** de las aplicaciones f y g, y se representa por $g \circ f$ a otra aplicación:

$$h: A \longrightarrow B \quad tal \quad que:$$
$$h(x) = (g \circ f)(x) = g[f(x)]; \quad \forall x \in A$$

NOTA: El producto de aplicaciones no es conmutativo.

8.- Relación de equivalencia asociada a una aplicación.-

Sea f: A ——————> B, si definimos sobre A la siguiente relación binaria:
x ——————> f(x)

$$\forall a, b \in A, \quad a R b \leftrightarrow f(a) = f(b) \quad es\ de\ EQUIVALENCIA$$

■

LEYES DE COMPOSICIÓN: HOMOMORFISMOS

RESUMEN TEÓRICO

1.- Ley de composición.-

Dados 3 conjuntos A, B y C, se llama **LEY DE COMPOSICIÓN U OPERACIÓN**, a toda aplicación del producto cartesiano AxB en C.

$$f: A \times B \longrightarrow C$$

Ejemplo: Sean los conjuntos N, Q^+ y R. La aplicación:

$$f: N \times Q^+ \longrightarrow R$$
$$(a, b) \longrightarrow f(a, b) = \sqrt[a]{b}$$

es una ley de composición.

2.- Ley de composición interna u operación interna (l.c.i.).-

Se denomina **LEY DE COMPOSICIÓN INTERNA** u **OPERACIÓN INTERNA** (**l.c.i.**) entre los elementos de un conjunto A, a toda aplicación f de AxA en A: $f: A \times A \longrightarrow A$. Simbólicamente: l.c.i. "*":

$$f: A \times A \longrightarrow A$$
$$(a,b) \longrightarrow c = f(a,b) = a*b.$$

También se dice que "*" es una l.c.i. en el conjunto A, si $\forall\, a, b \in A$ ó $\forall (a,b) \in A \times A$ se verifica que $a*b \in A$.

Diremos que el conjunto A es **CERRADO** respecto de la operación "*" si la operación "*" definida sobre el conjunto A es interna.

Convencionalmente las leyes de composición interna se representan por signos tales como:

$*$ (*estrella*), $\square$ (*cuadrado*), $\perp$ (*truc*), $\top$ (*antitruc*)

$\triangle$ (*triangulo* (*Dif . simetrica*)), $\diamond$(*rombo*), *etc* .

Como signos particulares tenemos:

$+$ (*adición*), x (*multiplicación*), $\cap$ (*intersección*), *etc* .

3.- Propiedades de las operaciones internas.-

Sea A un conjunto cualquiera y * una operación interna definida en A, veamos una colección de propiedades que puede tener dicha operación:

1.- **ASOCIATIVA**: Diremos que una operación interna *, definida en un conjunto A es asociativa cuando verifique:

$$\forall\, a, b, c \in A: (a*b)*c = a*(b*c)$$

2.- **CONMUTATIVA**: $\forall\, a, b \in A : a*b = b*a$

3.- **ELEMENTO NEUTRO**: Se dice que el elemento $e \in A$ es **ELEMENTO NEUTRO** del conjunto A para la ley de composición interna *, si:

$$\forall\, a \in A,\ a*e = e*a = a$$

Propiedad: Veamos que tiene que ser único:

Supongamos que existieran dos elementos neutros e y e':

$$\left.\begin{array}{l} e*e' = e \text{ (por ser } e' \text{ neutro)} \\ e*e' = e' \text{ (por ser } e \text{ neutro)} \end{array}\right\} \Rightarrow e = e'$$

4.- **ELEMENTO SIMÉTRICO**: Sea el conjunto A, provisto de elemento neutro e con respecto a la l.c.i. *. Se dice que el elemento $a^{-1} \in A$ es **ELEMENTO SIMÉTRICO** de $a \in A$ para la ley de composición interna * si:

$$a*a^{-1} = a^{-1}*a = e$$

O sea que, $a \in A$, $\exists\, a^{-1} \in A$ / $a*a^{-1} = a^{-1}*a = e$. Si todo elemento de A tiene simétrico, se dice que A es un conjunto simetrizable.

5.- **ELEMENTO REGULAR POR LA DERECHA**: Un elemento a∈A es **REGULAR POR LA DERECHA** con respecto a la operación * definida en A, si se verifica:

$$\forall\ b,c \in A:\ b*a = c*a \Rightarrow b = c$$

6.- **ELEMENTO REGULAR POR LA IZQUIERDA**: Diremos que un elemento a ∈ A es **REGULAR POR LA IZQUIERDA** con respecto a la operación * definida en A, si se verifica:

$$\forall\ b,c \in A:\ a*b = a*c \Rightarrow b = c$$

7.- **ELEMENTO REGULAR**: si un elemento de un conjunto A es regular por la derecha y por la izquierda, se llama **REGULAR**. A los elementos **REGULARES** de un conjunto también se les llama **SIMPLIFICABLES**.

8.- **PROPIEDAD DISTRIBUTIVA**: Dadas dos leyes de composición interna * y ⊤ sobre un mismo conjunto A, diremos que la operación * **ES DISTRIBUTIVA CON RESPECTO A LA OPERACIÓN** ⊤ si:

$$\left.\begin{array}{l} \forall\ a,\ b,\ c \in A;\ \ a*(b \top c) = (a*b) \top (a*c) \\ (a \top b)*c = (a*c) \top (b*c) \end{array}\right\}$$

9.- **ELEMENTO IDEMPOTENTE**: Un elemento a∈A se dice idempotente respecto a una l.c.i. * de A si se verifica que $a*a = a$.

10.- **ELEMENTO ABSORBENTE**: Un elemento a∈A se dice **ABSORBENTE** por la izquierda (derecha) respecto a una l.c.i. * definida en A, si se verifica:

$$a*x = a \quad (x*a = a) \quad \forall x \in A$$

11.- **ELEMENTO CENTRAL**: Un elemento a∈A se llama **CENTRAL** respecto a una l.c.i. * definida en A, cuando conmuta con todos los elementos de A. El conjunto de estos elementos constituye el **CENTRO** de A con la operación * [(A,*)]. Para una l.c.i. conmutativa el centro es A.

4.- Ley de composición externa u operación externa (l.c.e.).-

Dado un conjunto A y otro conjunto B, una ley de composición externa en un conjunto B es toda aplicación AxB ————> B.

Al conjunto B se llama conjunto base y al A conjunto auxiliar ó dominio de operadores.

Si $a \in A$, $b \in B$ y al par (a,b) le corresponde $c \in B$, se escribe $c = a \odot b$.

PROPIEDADES OPTATIVAS:

Supóngase, el conjunto B dotado de una l.c.i. $\oplus$, y asimismo definida sobre el conjunto B asociado a A, otra l.c.e. $\odot$, es decir, $(B, \oplus, \odot)$.

Igualmente, supongamos al conjunto A provisto de dos l.c.i.; que representamos por + (suma de operadores de A) y . (producto de operadores de A), o sea $(A, +, .)$.

1.- Se dice que la ley externa $\odot$ es asociativa respecto de la ley interna ., si

$$\forall \alpha, \beta \in A, \forall b \in B, (\alpha . \beta) \odot b = \alpha \odot (\beta \odot b)$$

2.- Se dice que la ley externa $\odot$ es distributiva respecto de la ley interna $\oplus$ si:

$$\forall \alpha \in A, \forall a, b \in B, \alpha \odot (a \oplus b) = (\alpha \odot a) \oplus (\alpha \odot b)$$

3.- La ley externa $\odot$ es distributiva con relación a la ley interna $\oplus$ si:

$$\forall \alpha, \beta \in A, \forall b \in B, (\alpha + \beta) \odot b = (\alpha \odot b) \oplus (\beta \odot b)$$

5.- Morfismos entre dos conjuntos.-

Dados dos conjuntos A y B provistos de las leyes de composición interna * y $\square$ respectivamente, y la aplicación f: A ————> B, se dice que f es un **HOMOMORFISMO** entre A y B, si se verifica que :

$$f(a*b) = f(a) \square f(b), \forall a,b \in A.$$

TIPOS DE HOMOMORFISMOS:

. Si A = B ⇒ f:A ————> A es un **ENDOMORFISMO.**
. Si f es inyectiva ⇒ **MONOMORFISMO.**
. Si f es sobreyectiva ⇒ **EPIMORFISMO.**

. Si f es biyectiva ⇒ **ISOMORFISMO.**
. Si A = B y f es biyectiva ⇒ **AUTOMORFISMO.**

PROPIEDADES DE LOS HOMOMORFISMOS:

En un homomorfismo f: (A,*) ————> (B,□) se cumplen las siguientes propiedades:

1.- Si * es asociativa en A, también lo es □ en f(A).

2.- Si * es conmutativa en A, también lo es □ en f(A).

3.- Si existe en A el elemento neutro **e** de *, existe en f(A) el elemento neutro **e'** de □ y se verifica que **e' = f(e).**

4.- Si a^{-1} es el simétrico de **a** respecto de la ley *, entonces $f(a^{-1})$ es el simétrico de **f(a)** con respecto a □ y además $f(a^{-1}) = [f(a)]^{-1}$.

5.- Si f: (A,*) ————> (B,□) es un isomorfismo, entonces:
f^{-1}:(B,□) ————> (A,*) también es un isomorfismo.

6.- Si f: (A,*) ————> (B,□) y g: (B,□) ————> (C, T) son homomorfismos, la aplicación compuesta g o f: (A,*) ————> (C, T) es homomorfismo.

■

TEORÍA DE GRUPOS

RESUMEN TEÓRICO

1.- Estructuras con una operación: GRUPOS.

Se dice que un conjunto A, que está dotado de una o varias leyes de composición (internas ó externas), posee cierta **ESTRUCTURA ALGEBRAICA** si se verifica un determinado número de propiedades.

Llamamos **GRUPOIDE** a un conjunto en el que se ha definido una operación interna.

Llamamos **SEMIGRUPO** a un grupoide cuya operación interna es asociativa.

LLamamos **MONOIDE** a un semigrupo que tiene elemento neutro.

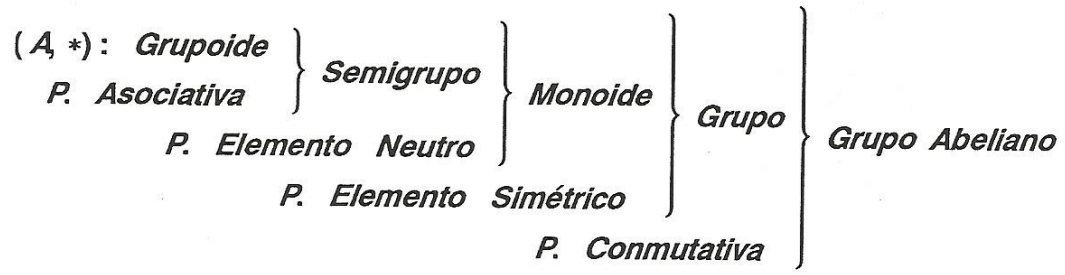
LLamamos **GRUPO** a un semigrupo cuya operación tiene las propiedades de existencia de elemento neutro y simétrico. Lo representaremos, en general, por **G**.

Llamamos **GRUPO ABELIANO ó CONMUTATIVO** a un grupo cuya operación interna es conmutativa.

Llamamos **GRUPO ADITIVO** a un grupo cuya operación interna es la suma, y entonces al elemento neutro se le llama **CERO (0)** y el simétrico de un elemento **a**, se llama **OPUESTO DE a** y se representa por **-a**.

Llamamos **GRUPO MULTIPLICATIVO** a un grupo cuya operación interna es la multiplicación, llamándose **UNIDAD (1)** al elemento neutro e **INVERSO** del elemento **a** al simétrico de **a** y se representa por $\mathbf{a^{-1}}$.

ESTRUCTURAS ALGEBRAICAS CON UNA SOLA OPERACION



Ejemplos: **SEMIGRUPOS:** (N, +), (Z, +), (Q, +), (R, +), (N,.), (Z,.), (Q,.), (R,.), (P(A),U), (P(A),∩) .
GRUPOS ABELIANOS: (Z, +), (Q, +), (R, +), (Q-{0},.), (R-{0},.).

En todo grupo se verifican las siguientes **propiedades:**

1.- El elemento neutro es único.
2.- El elemento simétrico de un elemento cualquiera de un grupo es único.
3.- El elemento simétrico del simétrico de un elemento de un grupo es igual a dicho elemento.
4.- Todos los elementos de un grupo G son regulares.
5.- Las ecuaciones $a*x = b$ y $x*a = b$ tienen solución única en un grupo (G,*).
6.- $\forall\ a,b \in G$, $(a*b)' = b'* a'$.

2.- Subgrupos.

Un subconjunto no vacío **H** de un grupo G se llama **SUBGRUPO de G** cuando H es grupo respecto de la operación de G. La notación es **(H,*)<(G,*)**

Proposición: La condición necesaria y suficiente para que un subconjunto no vacío H, de un grupo (G,*), sea un subgrupo de G, es que **$\forall$ a, b $\in$ H, a*b'$\in$ H.**(Con b' elemento simétrico de b).

Ejemplos: 1.- El conjunto de los enteros pares es un subgrupo de Z respecto de la adición.
2.- (Z, +) es subgrupo de (Q, +) y de (R, +)
3.- (R, +) es subgrupo de (C, +)
4.- Sea el grupo (G,*) y $x \in G$, $H = \{ x^n / n \in Z \}$ es un subgrupo de G,*) con respecto a la operación (*), llamado **SUBGRUPO MONÓGENO DE GENERADOR x.**

Sea el grupo (G,*), se llama **CENTRO de G** al subgrupo Z(G), con

$$Z(G) = \{ a \in G / a*x = x*a; \forall x \in G \}$$

Dado un grupo (G,*), se llaman **SUBGRUPOS IMPROPIOS** a los subgrupos **G** y **{ e }** (e = elemento neutro de *). A los demás los llamaremos **SUBGRUPOS PROPIOS**.

3.- Subgrupos normales.

3.1.- Clases adjuntas a un subgrupo.

Dado un grupo (G,*) y H subgrupo de G, podemos definir dos relaciones binarias que son las siguientes:

$$\begin{array}{l} 1)\ x\ R_1\ y \Leftrightarrow x*y' \in H \\ 2)\ x\ R_2\ y \Leftrightarrow y'*x \in H \end{array} \quad x, y \in G$$

podemos afirmar que estas relaciones son de equivalencia.

La **clase de equivalencia** de R_1 corrrespondiente a un elemento x será:

$$R_1 = [x] = \{ y \in G / x\ R_1\ y \} = H*x \quad (1)$$

Y se llama **CLASE DE x ADJUNTA A H POR LA DERECHA** o **CLASE ADJUNTA DE x POR LA DERECHA MÓDULO H.** Así pues,

$$H*x = \{ y \in G / y = h*x, \forall h \in H \}$$

La **clase de equivalencia** de R_2 corrrespondiente a un elemento x será:

$$R_2 = [x] = \{ y \in G / x\ R_2\ y \} = x*H$$

Y se llama **CLASE DE x ADJUNTA A H POR LA IZQUIERDA** o **CLASE ADJUNTA DE x POR LA IZQUIERDA MÓDULO H.** Así pues,

$$x*H = \{ y \in G / y = x*h, \forall h \in H \}$$

---

(1) $x\ R_1\ y \Leftrightarrow x*y' \in H \Leftrightarrow (x*y')' \in H \Leftrightarrow y*x' \in H \Leftrightarrow$
$\Leftrightarrow y*x' = h \in H \Leftrightarrow y*x'*x = h*x \in H*x \Leftrightarrow y \in H*x$

Podemos observar que:

$$R_1(e) = H*e = H$$
$$R_2(e) = e*H = H$$

es decir, las clases correspondientes al elemento neutro coinciden con el mismo subgrupo.

3.2.- Subgrupo normal.

Dado un grupo (G,*), se dice que el subgrupo (H,*) es un **SUBGRUPO NORMAL, INVARIANTE ó DISTINGUIDO** de G si x*H = H*x, ∀ x ∈ G, o lo que es lo mismo, si para todo elemento de G, las clases adjuntas al subgrupo H por la izquierda y derecha coinciden. La notación es **(H,*)◁(G,*)**.

Proposición: Dado un grupo (G,*) y H subgrupo de G, H es subgrupo normal (H◁G) de G $\Leftrightarrow x*H \subseteq H*x,\ \forall x \in G$ ó $\Leftrightarrow x*H*x' \subseteq H,\ \forall x \in G$ (esto significa que $x*h*x' \in H,\ \forall x \in G,\ \forall h \in H$)

Proposición: Si (G,*) es un grupo abeliano, todos sus subgrupos son normales.(2)

Observación: Todo grupo (G,*) tiene dos subgrupos normales: (G,*) y ({e},*), es decir, los subgrupos impropios son normales.

Ejemplos: El centro de un grupo (G,*), Z(G), es un subgrupo normal de G, pues

$$\forall z \in Z(G) \quad y \quad \forall x \in G:$$
$$x*z*x' = z*x*x' = z \in Z(G)$$
$$\downarrow$$
$$por\ z \in Z(G) \Rightarrow x*z = z*x$$

4.- Grupo cociente.

Si tenemos un grupo (G,*) y H es subgrupo de G, podemos definir los conjuntos:

$$G/H = \{ H*x \,/\, x \in G \}$$
$$H/G = \{ x*H \,/\, x \in G \}$$

---

(2) $\forall x \in G,\ \forall h \in H,\ (H,*) < (G,*)$

$x*h*x' = x*x'*h = h \in H \Rightarrow (H,*)$ *es normal*

Si tenemos un grupo (G,*) y un subgrupo normal H ($H \triangleleft G$), llamamos **CONJUNTO COCIENTE** a **G/H**. Si a este conjunto lo dotamos de la operación interna del grupo G (*), resulta que es un grupo y por tanto a **(G/H,*)** se le llama **GRUPO COCIENTE**.

$G/H = \{ H*x / x \in G \} = \{ x*H / x \in G \}$ ya que por ser H subgrupo normal se cumple que $\forall x \in G$, $x*H = H*x$.

5.- Grupos finitos.

Diremos que un grupo G es **FINITO**, de **ORDEN n**, cuando tiene un número finito (**n**) de elementos.

Al número de elementos de un grupo G se denomina **ORDEN DEL GRUPO G**.

Dado un elemento $a \in G$, **n** es el **ORDEN DE a** si n es el menor número natural distinto de cero para el cual $a*a*\overset{n}{\ldots}*a = e$. Si para cualquier **n** se verifica que $a*a*\overset{n}{\ldots}*a \neq e$, se dice que **a** es de orden infinito.

Ejemplo: El conjunto { 1, -1, i, -i } es un grupo multiplicativo de orden 4.

TEOREMA DE LAGRANGE: El orden de un grupo finito es múltiplo del orden de cada uno de sus subgrupos.

El **ÍNDICE DE UN SUBGRUPO H** es el cociente entre el orden del grupo finito G y el orden del subgrupo H. Por el teoréma de Lagrange, el índice de un subgrupo es un número natural.

$$| G: H | = \frac{O(G)}{O(H)} = \frac{\text{orden de } G}{\text{orden de } H} = \text{índice de } H$$

Proposición: Si el índice de un subgrupo es 2, el subgrupo es normal.

Corolario (del teorema de Lagrange): Si un grupo tiene por orden un número primo, ese grupo no admite subgrupos propios, ya que los únicos subgrupos que admite son: {e} y G que son subgrupos impropios.

6.- Homomorfismos entre grupos.

Dados dos grupos (G,*) y (G',□), una aplicación $f: G \longrightarrow G'$ es **HOMOMORFISMO** si:

$$\forall a,b \in G \quad f(a*b) = f(a) \square f(b)$$

Los distintos tipos: monomorfismo, epimorfismo, endomorfismo, isomorfismo y automorfismo, son análogos a los definidos en el epígrafe de homomorfismos entre conjuntos provistos de una ley de composición interna.

Dado el homomorfismo f: G ————> G', se denomina **NÚCLEO de f**, representándose por **ker f** ó **N(f)** al conjunto siguiente:

$$\ker f = \{ x \in G / f(x) = e' \}$$ (e' = elemento neutro de (G',□))

Propiedades de los homomorfismos entre grupos:

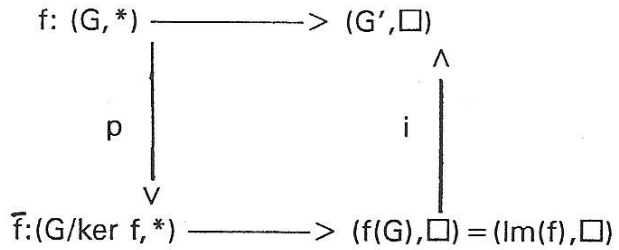
1.- La imagen de un grupo por un homomorfismo es un grupo con respecto a la operación definida en el conjunto imagen.
2.- Ker f es un subgrupo normal ó invariante.
3.- La condición necesaria y suficiente para que f sea inyectivo es que ker f = {e}.

Además tambien se verifican las propiedades de los homomorfismos entre conjuntos provistos de una operación interna.

Descomposición canónica de un homomorfismo entre grupos.

Sea f: (G,*) ————> (G',□), como ker f es un subgrupo normal, (G/ker f,*) es un grupo isomorfo al grupo (f(G),□).

Se puede descomponer f de la siguiente forma:



Donde:

$$p(x) = x * \ker f, \quad \forall x \in G$$

$$\bar{f}(x * \ker f) = f(x), \quad \forall x * \ker f \in G / \ker f$$

$$i(x) = x, \quad \forall x \in f(G)$$

p es siempre epimorfismo, $\bar{f}$ es siempre isomorfismo e i es siempre monomorfismo.

■

ANILLOS Y CUERPOS

RESUMEN TEÓRICO

1.- Anillos y Cuerpos.

Dado un conjunto A, diremos que posee estructura de **ANILLO** cuando sobre él se han definido dos operaciones, que para simplificar la notación llamaremos adición (+) y multiplicación o producto (.), verificándose:

a) (A, +) es grupo abeliano.
b) (A,.) es semigrupo (Es decir, (.) es Operación Interna y Asociativa).
c) (.) es distributiva respecto a (+), es decir:

$$a.(b+c) = a.b + a.c, \forall\ a, b, c \in A.$$
$$(a+b).c = a.c + b.c, \forall\ a, b, c \in A.$$

Si la segunda operación de (A, +,.) , (.), tiene la propiedad conmutativa, se dice que es **ANILLO CONMUTATIVO**.

Si la segunda operación de (A, +,.) , (.) tiene la propiedad de existencia de elemento neutro, el **ANILLO** se llama **ANILLO UNITARIO**.

Un **CUERPO** es un anillo unitario y conmutativo en el que todo elemento , excepto el neutro de la 1ª operación, tiene simétrico para la segunda operación, es decir, que un conjunto (K, +,.) será **CUERPO** cuando verifica que:

a) (K, +) es grupo abeliano.
b) (K-{0},.) es grupo abeliano.
c) (.) es distributiva respecto a (+), es decir:

$$a.(b+c) = a.b + a.c, \forall\ a, b, c \in K.$$
$$(a+b).c = a.c + b.c, \forall\ a, b, c \in K.$$

Al elemento neutro de la primera operación se le llama **CERO (0)** y al neutro de la segunda operación se le llama **UNIDAD(1)**.

Ejemplos: $(Z,+,.)$ $(Q,+,.)$ $(R,+,.)$ son anillos conmutativos y unitarios. $(Q,+,.)$ $(R,+,.)$ $(C,+,.)$ $(Z/7,+,.)$ $(Z/3,+,.)$ son cuerpos.

2.- Propiedades.

2.1.- Anillos.

Cuando en un conjunto se ha definido una **ESTRUCTURA DE ANILLO**, entre sus elementos se cumplen las siguientes propiedades de los grupos abelianos:

1.- El elemento neutro de (+) (Cero) es único.
2.- Todo elemento, **a**, tiene su opuesto, **-a**.
3.- El opuesto del opuesto de un elemento es el mismo elemento.
4.- El opuesto de la suma de elementos es la suma de los opuestos de cada elemento:

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

5.- Se verifican las propiedades simplificativas:

$$a+b = a+c \Rightarrow b=c$$
$$b+a = c+a \Rightarrow b=c$$

6.- Las ecuaciones $x+a = b$; $a+x = b$ tienen solución única: $\mathbf{x = b + (-a)}$.

Además de las anteriores, los anillos cumplen, entre otras, las siguientes propiedades:

I .- $a.0 = 0, \forall\ a \in A$, 0 neutro de (+).
II .- $(-a).b = a.(-b) = -a.b, \forall\ a, b \in A$.
III.- $(-a).(-b) = a.b, \forall\ a, b \in A$.

II y III son conocidas como las **REGLAS DE LOS SIGNOS**.

Dado un anillo unitario $(A,+,.)$, se dice que un elemento $a \in A$ es **INVERSIBLE** cuando posee elemento simétrico con respecto a la segunda operación (.), o sea:

$$a \in A \text{ es inversible} \Leftrightarrow \exists\ a^{-1} \in A \,/\, a.a^{-1} = a^{-1}.a = 1$$

Ejemplo: En $(Z,+,.)$ los únicos elementos inversibles son $\{1\}$ y $\{-1\}$.

El conjunto $(A^*,.)$ de los elementos inversibles de un anillo $(A,+,.)$ se le llama **CONJUNTO DE LAS UNIDADES DE A** y es un **GRUPO MULTIPLICATIVO**.

Un elemento $a \in (A,+,.)$ (Anillo) se llama **NILPOTENTE** cuando existe un número natural $n \neq 0$, tal que:

$$a^n = a.a.a...^n...a = 0$$

Un elemento $a \in (A,+,.)$ (Anillo) se llama **IDEMPOTENTE** si $a^2 = a$.

Ejemplo: En $(Z/12,+,.)$:

$\bar{6}$ ***es nilpotente*** ***pues*** $\bar{6}^2 = \bar{36} = \bar{0}$

$\bar{4}$ ***es idempotente*** ***pues*** $\bar{4}^2 = \bar{16} = \bar{4}$

Se llama **CARACTERÍSTICA** de un anillo $(A,+,.)$ al menor número natural $n \in N^*$, tal que:

$$n.a = a+a+...^n...+a = 0, \forall\, a \in A.$$

Si no existe n, se dice que el anillo es de característica cero o infinita.

La característica ha de ser el mínimo común múltiplo del orden de todos los elementos del anillo en el grupo aditivo, si no existe dicho m.c.m., porque haya algún elemento de orden 0 ó porque los órdenes no estén acotados superiormente, la característica será cero ó infinito.

En un anillo unitario, la característica coincide con el orden del elemento unidad en el grupo aditivo ($n.1 = 0$).

2.2.- Cuerpos.

Cuando un conjunto tiene **ESTRUCTURA DE CUERPO**, entre sus elementos se cumplen las siguientes propiedades:

1.- Como todo cuerpo es un anillo, se verificarán las propiedades de estos, expuestas en 2.1.

2.- Si $x, y \in (K,+,.)$ (Cuerpo), pertenecen a $(K,+,.)$, también, los siguientes elementos:

$$0,\ 1,\ x+y,\ x-y,\ x.y,\ x.y^{-1} = x/y \text{ si } y \neq 0.$$

3.- El hecho de que $(K,+)$ sea grupo aditivo y que $(K-\{0\},.)$ sea grupo multiplicativo, implica la existencia de elementos opuestos e inversos (si el elemento es $\neq 0$) y, por tanto, se verifican las leyes simplificativas:

$$x+y = x+z \Rightarrow y = z.$$
$$x.y = x.z \Rightarrow y = z,\ x \neq 0.$$

4.- Las ecuaciones $x+a = b$ y $x.a = b$ $(a \neq 0)$ tienen solución única.

5.- En todo cuerpo $(K, +, .)$ son válidas las reglas de las fracciones, siempre que los denominadores sean $\neq 0$:

$$a)\ \frac{x}{y} = \frac{z}{t} \Leftrightarrow x.t = y.z,\ y \neq 0,\ t \neq 0$$

$$b)\ si\ y \neq 0,\ \forall\, a \in (K, +, .),\ a \neq 0 \Rightarrow \frac{x}{y} = \frac{x.a}{y.a}$$

$$c)\ \frac{x}{y} + \frac{z}{t} = \frac{x.t + y.z}{y.t},\ y \neq 0,\ t \neq 0$$

$$d)\ \frac{x}{y}.\frac{z}{t} = \frac{x.z}{y.t},\ y \neq 0,\ t \neq 0$$

6.- La característica de un cuerpo, si es finita y $\neq 0$, es un número primo.

3.- Dominios de integridad.

En un anillo $(A, +, .)$ llamamos **DIVISORES DEL CERO** a aquellos elementos de A que verifican:

$$a.b = 0 \text{ con } a \neq 0 \quad y \quad b \neq 0$$

Cuando un anillo A, conmutativo, no posea divisores del cero, se llama **ANILLO DE INTEGRIDAD.**

Si un anillo de integridad es unitario, se llama **DOMINIO DE INTEGRIDAD.**

Un cuerpo no puede tener divisores de cero, por tanto todo **CUERPO** es **DOMINIO DE INTEGRIDAD.**

Todo dominio de integridad con un número finito de elementos es cuerpo.

En un dominio de integridad se verifican las siguientes propiedades simplificativas del producto:

$$a.x = a.y \Rightarrow x = y\ ;\ \forall\, a \neq 0.$$

4.- Subanillos.

Dado un anillo $(A, +, .)$, diremos que B es **SUBANILLO** de A si se verifica:

a) $B \subset A$
b) $(B, +, .)$ es anillo.

La condición necesaria y suficiente para que un subconjunto $(B, +, .) \subset (A, +, .)$ sea **SUBANILLO** de A, es que verifique:

a) $\forall x, y \in B, x - y \in B$.
b) $\forall x, y \in B, x.y \in B$.

$(A, +, .)$ tiene dos **SUBANILLOS IMPROPIOS**: $(\{0\}, +, .)$ y $(A, +, .)$

Propiedades: Sea $(B, +, .)$ subanillo de $(A, +, .)$:

1.- Si A es anillo conmutativo, B también lo es.
2.- Si A es anillo de integridad, B también lo es.
3.- Un anillo $(A, +, .)$ puede tener elemento unidad y $(B, +, .)$ tenerlo ó no, ó tenerlo B y no tenerlo A.
4.- Un anillo $(A, +, .)$ puede tener divisores del cero y $(B, +, .)$ carecer de ellos.

5.- Subcuerpos.

Diremos que H es **SUBCUERPO** del cuerpo $(K, +, .)$, si se verifica que:

a) $H \subset K$
b) $(H, +, .)$ es cuerpo.

La condición necesaria y suficiente para que un subconjunto H de un cuerpo $(K, +, .)$ sea **SUBCUERPO** de $(K, +, .)$ es que verifique:

a) $\forall x, y \in H, x - y \in H$.
b) $\forall x, y \in H, y \neq 0, x.y^{-1} \in H$.

6.- Ideales.

Dado un anillo $(A, +, .)$, se dice que $I \subset A$ es **IDEAL** de A cuando $I \neq \varnothing$ y se verifica:

a) Si $a,b \in I, a - b \in I$.
b) Si $a \in I, h \in A \Rightarrow a.h \in I$ y $h.a \in I$.

Es decir,I es un subgrupo aditivo de $(A, +)$ tal que $\forall a \in I, \forall h \in A$, $a.h \in I$ y $h.a \in I$.

Diremos que el ideal I del anillo unitario $(A,+,.)$ es **PRINCIPAL** cuando existe un elemento **i** de A tal que :

$$\forall\, x \in I,\ \exists\, y \in A \text{ que verifica que } \mathbf{x = y.i}$$

Al elemento **i** se le llama **BASE** del ideal I, y se escribe **I = (i)**.

Propiedades:

1ª.- La suma de dos ideales es un ideal.
2ª.- La intersección de dos ideales es otro ideal.
3ª.- Todo ideal I de un anillo A, es subanillo de A.
4ª.- En todo cuerpo $(K,+,.)$ solo existen dos ideales {0} y {K}.

7.- Anillo cociente.

Sea $(A,+,.)$ un anillo e I un ideal de A. Si en A definimos la siguiente relación binaria:

$$\forall\, x,\ y \in A,\quad x\,R\,y \Leftrightarrow x - y \in I$$

Se puede comprobar que es **R. EQUIVALENCIA** y nos permite clasificar los elementos de A en **CLASES DE EQUIVALENCIA** cuya reunión es el **CONJUNTO COCIENTE A/I.**

Como el ideal I es subanillo de A, y por tanto subgrupo de un grupo abeliano con respecto a la 1ª operación (+), podemos concluir que I es un **SUBGRUPO NORMAL** de A y entonces podemos considerar el **GRUPO COCIENTE** abeliano (A/I, +) cuyos elementos serán las clases I_x, I_y, I_z, etc.

Si ahora definimos la multiplicación en (A/I) como:

$$\forall\, I_x,\ I_y \in A/I,\ I_x.I_y = I_{x.y}$$

Resulta, entonces, que **(A/I, +, .)** es anillo que denominaremos: **ANILLO COCIENTE DEL ANILLO A CON RESPECTO AL IDEAL I.**

8.- Homomorfismos entre anillos.

Dados dos anillos $(A,+,.)$ y $(A',\oplus,\odot)$, una aplicación
$f: (A,+,.) \longrightarrow (A',\oplus,\odot)$ es un homomorfismo entre anillos si verifica:

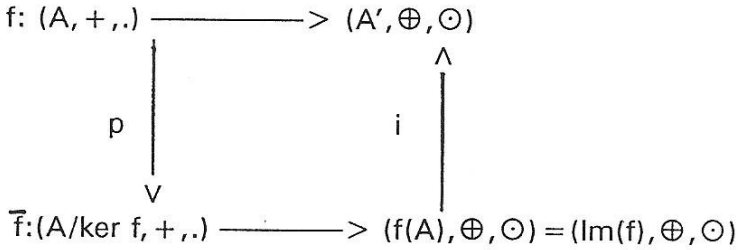
a) $f(a+b) = f(a) \oplus f(b), \forall\ a, b \in A.$
b) $f(a.b) = f(a) \odot f(b), \forall\ a, b \in A.$

Propiedades:

1.- Por ser un homomorfismo entre anillos un homomorfismo entre grupos con la 1ª operación, tiene las mismas propiedades que aquellos con respecto a la 1ª operación.
2.- $\text{Ker } f = \{ x \in A / f(x) = 0' \}$ es ideal de A, (0' neutro de $\oplus$)
3.- $f(A) \subset A'$ es subanillo de $(A', \oplus, \odot)$.
4.- $\ker f = \{0\} \Leftrightarrow$ f es inyectivo.

Descomposición canónica de un homomorfismo entre anillos:

Veamos en el siguiente diagrama, donde todos los conjuntos son anillos, como podemos descomponer el homomorfismo f de la forma ($f = i \circ \bar{f} \circ p$) :



Donde:

$$p(x) = x + \ker f, \quad \forall\ x \in A$$
$$\bar{f}(x + \ker f) = f(x), \quad \forall\ x + \ker f \in A/\ker f$$
$$i(x) = x, \quad \forall\ x \in f(A)$$

p es siempre epimorfismo, $\bar{f}$ es siempre isomorfismo e i es siempre monomorfismo.

9.- Homomorfismos entre cuerpos.

Se tratará a todos los efectos como un homomorfismo entre anillos.

10.- Equivalencia entre las notaciones.

En este tema y para simplificar solo hemos utilizado las operaciones (+) y (.), pero para que el tema alcance toda la generalidad se pueden transformar todas las afirmaciones en él vertidas a las operaciones (*) y (⊥), por ejemplo:

Con *, ⊥, e, u	Con +, ., 0, 1
$(a*b)*c = a*(b*c)$	$(a+b)+c = a+(b+c)$
$a*e = e*a = a$	$a+0 = 0+a = a$
$a*a' = a'*a = e$	$a+(-a) = (-a)+a = 0$
$(a \perp b) \perp c = a \perp (b \perp c)$	$(a.b).c = a.(b.c)$
$a \perp e = e$	$a.0 = 0$
$a \perp u = a$	$a.1 = a$
$a \perp b = e \Leftrightarrow a = e$ ó $b = e$	$a.b = 0 \Leftrightarrow a = 0$ ó $b = 0$
$a \perp (b*c) = (a \perp b)*(a \perp c)$	$a.(b+c) = (a.b)+(a.c)$
$a' \perp b' = a \perp b$	$(-a).(-b) = a.b$
$a*a*\ldots^{n}\ldots*a = na$	$a+a+\ldots^{n}\ldots+a = na$
$a \perp a \perp \ldots^{n} \ldots \perp a = a^n$	$a.a.\ldots.^{n}\ldots.a = a^n$
$a*b = b*a$	$a+b = b+a$

11.- Resumen.

ESTRUCTURAS ALGEBRAICAS CON DOS OPERACIONES

Consideremos un conjunto $(A, *, \circ)$

$$(*)\ \left\{\begin{array}{l}\textit{Asociativa}\\ \textit{Elem. Neutro}\\ \textit{Elem. Simétrico}\\ \textit{Conmutativa}\end{array}\right\}\ \textit{Grupo Abeliano}$$

$$\left.\begin{array}{l}(*)\ \textit{Grupo Abeliano}\\ (\circ)\ \textit{Asociativa} \longrightarrow \textit{Semigrupo}\\ (\circ)\ \textit{Distributiva respecto a } (*)\end{array}\right\}\ \textit{Anillo}$$

Si además $(\circ)$ *Conmutativa* $\longrightarrow$ *Anillo Conmutativo*

Si además $(\circ)$ *E Neutro* $\longrightarrow$ *Anillo Unitario*

$$(A, *)\ \left\{\begin{array}{l}\textit{Asociativa}\\ \textit{Elem. Neutro}\\ \textit{Elem. Simétrico}\\ \textit{Conmutativa}\end{array}\right\}\ \textit{Grupo Abeliano}$$

$$(A-\{e\}, \circ)\ \left\{\begin{array}{l}\textit{Asociativa}\\ \textit{Elem. Neutro}\\ \textit{Elem. Simétrico}\\ \textit{Conmutativa}\end{array}\right\}\ \textit{Grupo Abeliano}$$

$$\left.\begin{array}{l}\textit{Grupo Abeliano}\\ \textit{Grupo Abeliano}\\ (\circ)\ \textit{es distributiva respecto a } (*)\end{array}\right\}\ \textit{CUERPO}$$

■

POLINOMIOS EN UNA INDETERMINADA

RESUMEN TEÓRICO

1.- Definiciones.

Decimos que un **POLINOMIO CON COEFICIENTES EN UN ANILLO CONMUTATIVO K EN UNA INDETERMINADA** es una sucesión infinita de elementos de tal anillo, tales que a partir de uno, en adelante, todos los elementos de la sucesión son nulos.

Se representa por: $P = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$, $a_i \in K$, $\forall\, i = 0, 1, 2, \ldots, n$. Designando por $x = (0, 1, 0, 0, \ldots)$; a tal polinomio se le denomina **INDETERMINADA.**

En general: $x^n = (0, 0, \ldots, 0, \underset{n}{1}, 0, \ldots, 0, \ldots)$.

De esta forma, el polinomio $P = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ se escribe:

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$$

Al conjunto de todos los polinomios en una indeterminada con coeficientes en el anillo K, lo representamos por $K[x]$.

Al polinomio en el que un único coeficiente es distinto de cero se llama **MONOMIO**. Su fórmula general es: a_nx^n con $a_n \neq 0$, $n \in N$.

El **GRADO DE UN POLINOMIO**, es el mayor índice n de manera que $a_n \neq 0$. El monomio $a_n x^n$ será el **TÉRMINO PRINCIPAL o DOMINANTE** del polinomio y su coeficiente a_n, el **PRINCIPAL o DIRECTOR.**

Llamaremos **POLINOMIO CERO** al que tiene todos sus coeficientes nulos. Se simboliza por $0 = (0, 0, 0, \ldots)$.

Llamaremos **POLINOMIO UNIDAD** al que tiene todos sus coeficientes nulos a excepción de $a_0 = 1$. Se simboliza por $1 = (1, 0, 0, \ldots)$

Decimos que dos polinomio $P(x) = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ y $Q(x) = (b_0, b_1, b_2, \ldots, b_n, 0, 0, \ldots)$ son **IGUALES** $\Leftrightarrow a_i = b_i \; \forall \, i \in N$.

2.- Operaciones entre polinomios.

SUMA: Dados dos polinomios $P(x) = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ y $Q(x) = (b_0, b_1, b_2, \ldots, b_m, 0, 0, \ldots)$, $n<m$ definimos la **ADICIÓN DE DOS POLINOMIOS** como otro polinomio de la forma:

$$P(x)+Q(x) = (a_0+b_0, a_1+b_1, a_2+b_2, \ldots, a_n+b_n, b_{n+1}, b_{n+2}, \ldots, b_m, 0, 0, \ldots)$$

PRODUCTO: Así mismo, dados dos polinomios $P(x) = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ y $Q(x) = (b_0, b_1, b_2, \ldots, b_m, 0, 0, \ldots)$, $n<m$, definimos la **MULTIPLICACIÓN DE POLINOMIOS** como otro polinomio de la forma:

$$P(x).Q(x) = (c_0, c_1, c_2, \ldots, c_{n+m}, 0, \ldots), \quad c_k = \sum_{i+j=k}^{n+m} a_i b_j$$

PRODUCTO DE UN POLINOMIO POR UN ESCALAR: Sea el polinomio $P(x) = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ y sea $\lambda \in K$. Se define el **PRODUCTO DE UN POLINOMIO POR UN ESCALAR** como otro polinomio de la forma:

$$\lambda.P(x) = \lambda.(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) = (\lambda a_0, \lambda a_1, \lambda a_2, \ldots, \lambda a_n, 0, 0, \ldots)$$

3.- Divisibilidad de polinomios con una indeterminada.

Se dice que $P(x) \in K[x]$ divide a $Q(x) \in K[x]$ si existe $C(x) \in K[x]$ tal que:

$$\mathbf{Q(x) = P(x).C(x)}$$

Propiedades:

1) Si un polinomio divide a otros dos, también divide a su suma y diferencia.

2) Si P(x) divide a Q(x), entonces P(x) divide a λ.Q(x), $\forall\lambda \in K$, $\forall P(x), Q(x) \in K[x]$.

3) Si P(x) divide a Q(x), entonces P(x) divide a Q(x).R(x), $\forall P(x), Q(x), R(x) \in K[x]$.

El **VALOR NUMÉRICO DE UN POLINOMIO EN UNA INDETERMINADA** es el valor que se obtiene al sustituir la variable por su valor correspondiente.

Ejemplo: El valor numérico del polinomio:

$$P(x) = x^2+2x-1 \text{ en } x = 2 \text{ es } P(2) = 2^2+2.2-1 = 7$$

Dado un polinomio P(x), se llaman **CEROS DEL POLINOMIO** P(x) a los valores de la indeterminada x para los cuales el valor numérico de P(x) es cero. También se llaman **RAÍCES DEL POLINOMIO.**

Se llama **MÁXIMO COMÚN DIVISOR DE LOS POLINOMIOS P(x) y Q(x)** al polinomio de grado máximo perteneciente al conjunto intersección entre los divisores de P(x) y los divisores de Q(x). Se simboliza por M.C.D.(P,Q) o bien m.c.d. (P,Q).

Cuando una serie de polinomios no tienen un divisor común (distinto del polinomio unidad), se dice que son **PRIMOS ENTRE SI o COPRIMOS.**

Se llama **MÍNIMO COMÚN MÚLTIPLO DE DOS POLINOMIOS P(x) y Q(x)** al polinomio de grado mínimo del conjunto $M(P) \cap M(Q)$, donde M(P) y M(Q) son los múltiplos de P(x) y Q(x) respectivamente. Se simboliza por M.C.M.(P,Q) ó m.c.m.(P,Q).

Un polinomio $P(x) \in K[x]$ decimos que es **IRREDUCIBLE o PRIMO SOBRE EL CUERPO K** si **NO** se puede descomponer en producto de polinomios de grado inferior que pertenezcan a K[x]. En caso contrario, el polinomio es **REDUCIBLE.**

CRITERIO DE IRREDUCIBILIDAD DE EISENSTEIN:

Sea $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$ un polinomio con coeficientes enteros y sea p un número primo. Si se cumple:

p no divide a a_n.
p divide a $a_0, a_1, a_2, a_3, .., a_{n-1}$
p^2 no divide a a_0,

entonces el polinomio P(x) es irreducible en Z[x].

Podemos observar que los únicos polinomios primos o irreducibles en C[x] son las constantes complejas no nulas y los polinomios de grado 1.

4.- Cálculo de las raíces de un polinomio de grado menor o igual a tres.

Raíces de un polinomio de grado 1:

La raíz de un polinomio $ax+b \in C[x]$, con $a \neq 0$ es

$$-\frac{b}{a}, \quad ya\ que\ ax+b = 0 \Rightarrow x = -\frac{b}{a}.$$

Este mismo razonamiento prueba que todo polinomio de grado uno de R[x] tiene una raíz real.

Raíces de un polinomio de grado 2:

Las raíces del polinomio $ax^2+bx+c \in C(x)$, con $a \neq 0$ son:

$$\frac{-b+\sqrt{b^2-4ac}}{2a} \qquad \frac{-b-\sqrt{b^2-4ac}}{2a}$$

La cantidad b^2-4ac se llama **DISCRIMINANTE** y se representa por Δ

Si el polinomio ax^2+bx+c tiene coeficientes reales y se considera que pertenece a R[x], entonces se le puede aplicar el razonamiento precedente, pues:

$$ax^2+bx+c \in R[x] \subset C[x]$$

Lo que ya no puede asegurarse es la existencia de dos raíces reales, ya que esto depende del valor del discriminante:

Si $\Delta > 0$, $a^2+bx+c \in R[x]$ tiene 2 raíces reales.
Si $\Delta = 0$, las dos raíces reales son iguales (raíz doble).
Si $\Delta < 0$, $ax^2+bx+c \in R[x]$ carece de raíces reales.

En R[x] los polinomios de segundo grado y discriminante negativo son primos. Es evidente que también son primos los polinomios de primer grado y las constantes no nulas.

Raíces de un polinomio de grado 3:

Vamos a calcular las raíces del polinomio de grado 3: $a_3x^3+a_2x^2+a_1x+a_0 \in C[x]$. Siempre podremos suponer que $a_3 = 1$, puesto que al dividir el polinomio considerado por a_3 se obtiene otro polinomio asociado que tiene las mismas raíces.

Aún podemos simplificar más la resolución de las raíces del polinomio $x^3+a_2x^2+a_1x+a_0$, puesto que el cambio $x = x'-a_2/3$ anula el término en x^2. Este cambio es lícito pues podemos suponer que $x \in C$.

Por tanto solo nos vamos a ocupar en calcular 3 raíces de los polinomios de C[x] del tipo:

$$x'^3+px'+q$$

Por tanto, se trata de calcular los valores de $x' \in C$ que anulen la función polinómica $x'^3+px'+q$, y ello se consigue fácilmente haciendo el cambio $x' = u+v$, donde:

$$u = \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} \qquad v = \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

5.- Fracciones algebraicas.

Se llama **FRACCIÓN ALGEBRAICA** a un par de polinomios A(x) y B(x) con $B(x) \neq 0$ dados en un cierto orden. Al primero de ellos se le llama **NUMERADOR** y al segundo **DENOMINADOR**. Se escriben ambos separados por una raya horizontal $\frac{A(x)}{B(x)}$.

OPERACIONES:

Consideremos el conjunto K[x]xK[x], definamos la siguiente relación de equivalencia:

$\frac{A(x)}{B(x)} \; R \; \frac{A'(x)}{B'(x)}$, que se lee, la fracción algebraica

$\frac{A(x)}{B(x)}$ *es equivalente a* $\frac{A'(x)}{B'(x)} \Leftrightarrow A(x) \cdot B'(x) = A'(x) \cdot B(x)$

Esta relación de equivalencia produce una clasificación de K[x]xK[x] en clases de equivalencia, a cada una de ellas se le llama **RAZÓN ALGEBRAICA**.

a) Si se multiplican el numerador y denominador de una fracción algebraica por un mismo polinomio (distinto del nulo), la fracción algebraica obtenida es equivalente a la dada. Es decir:

$$\frac{A(x)}{B(x)} \text{ y } \frac{A(x) \cdot P(x)}{B(x) \cdot P(x)} \text{ son equivalentes} \quad .$$

b) Si se dividen el numerador y denominador de una fracción algebraica por un mismo polinomio (distinto del nulo), se obtiene otra fracción algebraica equivalente a la dada:

$$\frac{A(x)}{B(x)} \text{ y } \frac{\frac{A(x)}{M(x)}}{\frac{B(x)}{M(x)}} \text{ son equivalentes .}$$

c) **Suma de razones algebraicas**: En K[x]xK[x]/R definimos la operación:

$$\left\{\frac{A(x)}{B(x)}\right\}+\left\{\frac{C(x)}{D(x)}\right\} = \left\{\frac{A(x)\,D(x)+B(x)\,C(x)}{B(x)\,D(x)}\right\}$$

Con esta operación, el conjunto de las razones algebraicas tiene estructura de grupo aditivo abeliano, siendo el elemento neutro $\left\{\frac{0(x)}{B(x)}\right\}$, con 0(x) el polinomio nulo, B(x) $\neq$ 0(x); el elemento simétrico de $\left\{\frac{A(x)}{B(x)}\right\}$ es $\left\{-\frac{A(x)}{B(x)}\right\}$.

d) **Producto de razones algebraicas**: En K[x]xK[x]/R definimos la siguiente operación, llamada producto de razones algebraicas:

$$\left\{\frac{A(x)}{B(x)}\right\}.\left\{\frac{C(x)}{D(x)}\right\} = \left\{\frac{A(x)\,.\,C(x)}{B(x)\,.\,D(x)}\right\}$$

Con esta operación, el conjunto de las razones algebraicas tiene estructura de grupo multiplicativo abeliano, siendo el elemento unidad $\frac{A(x)}{A(x)}$, con A(x) $\neq$ $\neq$ 0(x); el elemento simétrico de $\left\{\frac{A(x)}{B(x)}\right\}$ es $\left\{\frac{B(x)}{A(x)}\right\}$.

Podemos concluir que (K[x]xK[x]/R, +,.) es un cuerpo, llamado cuerpo de las **RAZONES o FRACCIONES ALGEBRAICAS** y que representaremos por K(x).

6.- División de polinomios.

La **DIVISIÓN ORDINARIA** de dos polinomios A(x) y B(x) consiste en encontrar dos polinomios H(x) y G(x), con grado G(x) < grado B(x), y tales que verifiquen: **A(x) = H(x).B(x) + G(x).**

Si dividimos la expresión anterior entre B(x), tenemos:

$\frac{A(x)}{B(x)} = H(x) + \frac{G(x)}{B(x)}$ con grado G(x) < grado B(x).

Se dice que **H(x) ES LA PARTE ENTERA** de la fracción racional $\frac{A(x)}{B(x)}$ y que $\frac{G(x)}{B(x)}$ **ES LA PARTE RACIONAL.**

7.- Descomposición de fracciones algebraicas en fracciones simples.

Sea B(x) un polinomio de K[x], si encontramos los polinomios P(x), Q(x), ..., R(x) primos entre sí y tales que $B(x) = \lambda(P(x))^{\alpha}.(Q(x))^{\beta}. \ldots(R(x))^{\gamma}$ decimos que $\lambda(P(x))^{\alpha}.(Q(x))^{\beta}. \ldots(R(x))^{\gamma}$ es la descomposición de B(x) en factores irreducibles (Para simplificar representaremos por $B = \lambda P^{\alpha}.Q^{\beta}. \ldots R^{\gamma}$.

Sea R(x) un elemento de k(x). Se llama **FORMA REDUCIDA DE R(x)** a un representante de R(x) de la forma $\frac{A(x)}{B(x)}$, donde A(x) y B(x) son elementos de K[x] primos entre sí.

Veamos algunas descomposiciones:

Sea $\frac{A(x)}{B(x)}$ una fracción racional reducida del cuerpo (K(x), +,.), cuya parte entera es H(x). Sea $B = \lambda P^{\alpha}.Q^{\beta}. \ldots R^{\gamma}$ la descomposición de B(x) en factores irreducibles. Existe una descomposición única:

$$\frac{A(x)}{B(x)} = H(x) + \frac{C_{\alpha}}{P^{\alpha}} + \frac{C_{\alpha-1}}{P^{\alpha-1}} + \ldots + \frac{C_1}{P} +$$

$$+ \frac{D_{\beta}}{Q^{\beta}} + \frac{D_{\beta-1}}{Q^{\beta-1}} + \ldots + \frac{D_1}{Q} +$$

$$\ldots\ldots\ldots\ldots$$

$$+ \frac{E_{\gamma}}{R^{\gamma}} + \frac{E_{\gamma-1}}{R^{\gamma-1}} + \ldots + \frac{E_1}{R}$$

Donde $H, C_\alpha, \ldots, C_1, D_\beta, \ldots D_1, \ldots, E_\gamma, \ldots, E_1$ son elementos de K[x] tales que grado $C_i <$ grado P, grado $D_i <$ grado Q, ..., grado $E_i <$ grado R, $\forall$ i.

Las fracciones racionales en las que se han descompuesto $\frac{A(x)}{B(x)} - H(x)$ se llaman **FRACCIONES RACIONALES SIMPLES.**

Consideremos ahora **K = C** (Cuerpo de los números complejos).

Sea $\frac{A(x)}{B(x)}$ un elemento de C(x), y sea $B(x) = \lambda(x-\rho)^h \ldots (x-\sigma)^k$, donde $\rho, \ldots, \sigma$ son las raíces de B(x) distintas dos a dos. Existe una descomposición única:

$$\frac{A(x)}{B(x)} = H(x) + \frac{\lambda_h}{(x-\rho)^h} + \frac{\lambda_{h-1}}{(x-\rho)^{h-1}} + \ldots + \frac{\lambda_1}{x-\rho} +$$

$$\ldots\ldots\ldots\ldots$$

$$+ \frac{\mu_k}{(x-\sigma)^k} + \frac{\mu_{k-1}}{(x-\sigma)^{k-1}} + \ldots + \frac{\mu_1}{x-\sigma}$$

Donde $H(x) \in C[x]$ ***y*** $\lambda_h, \ldots, \lambda_1, \ldots, \mu_k, \ldots, \mu_1 \in C$

Consideremos **K = R** (Cuerpo de los números reales).

Sea $\frac{A(x)}{B(x)}$ un elemento de R(x), y sea

$B(x) = \lambda(x-r)^h \ldots (x-s)^k . (x^2+ax+b)^l \ldots . (x^2+cx+d)^m$ la descomposición de B(x) en elementos irreducibles de R(x). Existe, entonces una descomposición única:

$$\frac{A(x)}{B(x)} = H(x) + \frac{\lambda_h}{(x-r)^h} + \frac{\lambda_{h-1}}{(x-r)^{h-1}} + \ldots + \frac{\lambda_1}{x-r} +$$

$$\ldots\ldots\ldots\ldots$$

$$+\frac{\mu_k}{(x-s)^k}+\frac{\mu_{k-1}}{(x-s)^{k-1}}+\ldots+\frac{\mu_1}{x-s}$$

$$+\frac{v_l x+p_l}{(x^2+ax+b)^l}+\frac{v_{l-1}x+p_{l-1}}{(x^2+ax+b)^{l-1}}+\ldots+\frac{v_1 x+p_1}{x^2+ax+b}+$$

$$\ldots\ldots\ldots\ldots$$

$$+\frac{\sigma_m x+\tau_m}{(x^2+cx+d)^m}+\frac{\sigma_{m-1}x+\tau_{m-1}}{(x^2+cx+d)^{m-1}}+\ldots+\frac{\sigma_1 x+\tau_1}{x^2+cx+d}$$

Donde $H(x) \in R[x]$ y $\lambda_n \ldots, \lambda_1, \ldots, \mu_k \ldots, \mu_1, v_l, p_l, \ldots, v_1, p_1$,

$, \ldots, \sigma_m \tau_m \ldots, \sigma_1, \tau_1 \in R$

■