

UNA INTRODUCCION AL ESTUDIO DE LAS ESTRUCTURAS  
ALGEBRAICAS DE GRUPO Y ANILLO

IVAN FRANCISCO ASMAR CHARRIS

TRABAJO PRESENTADO COMO REQUISITO PARCIAL  
PARA PROMOCION A PROFESOR ASOCIADO

UNIVERSIDAD NACIONAL  
BIBLIOTECAS CENTRALES

---

UNIVERSIDAD NACIONAL DE COLOMBIA

SECCIONAL MEDELLIN

FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMATICAS .

CONTENIDO

INTRODUCCION	v
LEYES DE COMPOSICION Y ESTRUCTURA ALGEBRAICA	1
LEY DE COMPOSICION INTERNA BINARIA	1
LEY DE COMPOSICION EXTERNA BINARIA	6
ESTRUCTURA ALGEBRAICA	9
CAPITULO I : PERMUTACIONES	11
DEFINICION DE PERMUTACION	11
MULTIPLICACION O COMPOSICION DE PERMUTACIONES	12
DEFINICION DE CICLO	14
LONGITUD DE UN CICLO	16
ORDEN DE UNA PERMUTACION	16
INVERSO DE UNA PERMUTACION	18
CONEXION ENTRE ECUACIONES Y PERMUTACIONES	19
CAPITULO II : GRUPOS	23
INTRODUCCION	23
DEFINICION DE GRUPO	24
GRUPO ABELIANO O CONMUTATIVO	24
ORDEN DE UN GRUPO	25
EJEMPLOS DE GRUPOS	27
SIMETRIAS DEL TRIANGULO EQUILATERO	30
ROTACIONES DEL TRIANGULO EQUILATERO	37
GRUPO DE PERMUTACIONES DE TRES ELEMENTOS	38
EL GRUPO CUATRO DE KLEIN	41

ALGUNAS PROPIEDADES ELEMENTALES DE UN GRUPO	43
$\eta$ -ASOCIATIVIDAD EN UN GRUPO	45
APLICACIÓN DE LAS PROPIEDADES DE UN GRUPO PARA CONSTRUIR SU TABLA	48
POTENCIAS ENTERAS EN UN GRUPO	55
DEFINICIÓN DE SEMIGRUPO	60
CARACTERIZACIÓN DE GRUPO	60
SUBGRUPOS	65
DEFINICIÓN DE SUBGRUPO	65
CARACTERIZACIÓN DE SUBGRUPO	66
SUBGRUPOS TRIVIALES	70
CARACTERIZACIÓN DE LOS SUBGRUPOS DE $(\mathbb{K}, +)$	70
SUBGRUPO CÍCLICO	71
EL GRUPO CIRCULAR	73
LAS RAÍCES $\eta$ -ESIMAS DE LA UNIDAD	75
INTERSECCIÓN DE SUBGRUPOS	78
GENERALIZACIÓN A UN GRUPO $(G, \cdot)$ DE LA RELACIÓN DE CONGRUENCIA	79
TEOREMA DE LAGRANGE	81
<b>CAPITULO III : HOMOMORFISMOS</b>	<b>83</b>
HOMOMORFISMO DE GRUPOS	83
ALGUNAS PROPIEDADES ELEMENTALES DE UN HOMOMORFISMO DE GRUPOS	84
EL NÚCLEO DE UN HOMOMORFISMO	86
TEOREMA DE CAYLEY	89
<b>CAPITULO IV : ANILLOS</b>	<b>93</b>
DEFINICIÓN DE ANILLO	93

CASOS ESPECIALES DE ANILLO	93
PROPIEDADES ELEMENTALES	95
ESTUDIO DE $\mathbb{Z}$	95
DIVISIBILIDAD	95
ALGUNAS PROPIEDADES DE LA DIVISIBILIDAD	96
DIVISORES NO TRIVIALES	98
ELEMENTOS INVERTIBLES	100
NUMERO PRIMO	100
DIVISOR COMUN	101
MAXIMO COMUN DIVISOR (M.C.D.)	103
PRIMOS RELATIVOS	105
LEMA DE EUCLIDES	105
TEOREMA DE EUCLIDES	106
TEOREMA FUNDAMENTAL DE LA ARITMETICA	107
ALGORITMO DE LA DIVISION Y ALGORITMO DE EUCLIDES	113
ALGORITMO DE LA DIVISION	113
ALGORITMO EUCLIDIANO	115
UN METODO PARA DETERMINAR EL M.C.D	116
MINIMO COMUN MULTIPLO (M.C.M.)	121
OTRO METODO PARA DETERMINAR EL M.C.D. Y EL M.C.M.	122
CONGRUENCIAS	130
DEFINICION DE LA RELACION DE CONGRUENCIA MODULO $m$	130
ALGUNAS PROPIEDADES DE LA RELACION DE CONGRUENCIA MODULO $m$	130
SUMA Y MULTIPLICACION DE CONGRUENCIAS	132

CRITERIO DE DIVISIBILIDAD POR 3	133
CRITERIO DE DIVISIBILIDAD POR 11	134
LOS ENTEROS MODULO $m : \mathbb{Z}_m$	141
CONGRUENCIAS LINEALES	145
ECUACION LINEAL DIOFANTICA	148
TEOREMA DEL RESIDUO CHINO	160

## INTRODUCCION

Con este trabajo he querido hacer un estudio elemental de las estructuras algebraicas de GRUPO y ANILLO, incluyendo lo que quisiera que quienes las estudien adquieran los conocimientos básicos indispensables para una mayor comprensión en los cursos de Algebra moderna (algebra abstracta) dictados en la carrera de matemáticas; por esto preparo este material para ser desarrollado en el curso FUNDAMENTOS II de esta carrera (Debo advertir que todo el material es perfectamente desarrollable en un semestre academico con una intensidad de 6 horas por semana).

En el primer capítulo desarrollo el tema de las permutaciones ya que históricamente los primeros grupos estudiados fueron los grupos llamados de permutaciones; en el capítulo II trato la estructura de grupo poniendo especial interés en desarrollar ejemplos que permitan captar aspectos generales de la teoría; en el tercer capítulo hago un estudio de los homomorfismos de grupos resaltando aquellas propiedades elementales más importantes; finalmente en el capítulo IV sobre la estructura de anillo he dedicado todo el trabajo a estudiar a los números enteros  $\mathbb{Z}$ , porque creo que este es el modelo básico de esta estructura, en el estudio de  $\mathbb{Z}$  se demuestran entre otras cosas: el teorema fundamental de la aritmética, la existencia del máximo común divisor y el mínimo común múltiplo para dos enteros no nulos y se dan unos métodos para determinarlos; también se hace un estudio de la relación de congruencia modulo  $m$ .

Al final de cada capítulo he incluido una colección de ejercicios

eios con el fin de que el lector al leerlos afirme sus conocimientos sobre el tema respectivo.

Estas notas son el fruto de varios semestres en los cuales he tenido a mi cargo las asignaturas FUNDAMENTOS I y FUNDAMENTOS II de la carrera de matemáticas.

Agradezco la colaboración que tuve por parte de los profesores Abraham Asmar y Rafael Ahumada.

# LEYES DE COMPOSICION Y ESTRUCTURA ALGEBRAICA

Comenzaremos nuestro estudio con los conceptos de ley de composici3n (interna y externa) y estructura algebraica.

## LEYES DE COMPOSICION.

DEFINICION. (LEY DE COMPOSICION INTERNA BINARIA U OPERACION BINARIA) Una

ley de composici3n interna binaria sobre un conjunto no-vac3o es cualquier regla que asigna a cada par ordenado de elementos del conjunto un 3nico elemento del conjunto.

De manera m3s precisa, si  $E$  es un conjunto no-vac3o, cualquier funci3n de  $E \times E$  hacia  $E$  se llama una ley de composici3n interna binaria en  $E$  o sobre  $E$ .

Usualmente una ley de composici3n interna binaria sobre un conjunto es llamada operaci3n binaria en el conjunto. Nosotros usaremos estos t3rminos indistintamente.

NOTACION. Si  $* : E \times E \longrightarrow E$  es una operaci3n binaria, entonces para  $\alpha, \beta \in E$ ,  $*(\alpha, \beta)$  se notara  $\alpha * \beta$  y se leera "  $\alpha$  compuesto  $\beta$ ".

OBSERVACIONES. Si  $* : E \times E \longrightarrow E$  es una ley de composici3n interna binaria (L.C.I.B.), entonces:

i) Para todo  $\alpha, \beta \in E$ ,  $\alpha * \beta \in E$ ; es decir, mediante  $*$  obtenemos a partir de un par de elementos de  $E$ , un elemento tambi3n de  $E$ , de aqu3 lo de INTERNA BINARIA.

ii) Para todo  $\alpha, \beta, \delta$  en  $E$ ,  $\alpha = \beta$  implica  $\alpha * \delta = \beta * \delta$  y  $\delta * \alpha = \delta * \beta$ .

En efecto; sean  $\alpha, \beta$  y  $\delta$  en  $E$  cualesquiera :

$$\alpha = \beta \implies (\alpha, \alpha') = (\beta, \alpha') \wedge (\alpha', \alpha) = (\alpha', \beta)$$

$$\implies *(\alpha, \alpha') = *(\beta, \alpha') \wedge *(\alpha', \alpha) = *(\alpha', \beta)$$

$$\implies \alpha * \alpha' = \beta * \alpha' \wedge \alpha' * \alpha = \alpha' * \beta.$$

Las observaciones son consecuencias de ser  $*$  función de  $E \times E$  hacia  $E$ .

DEFINICION. Una operación binaria  $*$  sobre un conjunto no vacío  $E$  es conmutativa si  $a * b = b * a$  para todo  $a, b \in E$ . La operación  $*$  se dice asociativa o simplemente asociativa si para todo  $a, b$  y  $c$  en  $E$ ,  $(a * b) * c = a * (b * c)$ .

EJEMPLOS DE OPERACIONES BINARIAS..

$$1. \quad + : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} \quad ; \quad \cdot : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$$

$$(\gamma, \lambda) \longmapsto \gamma + \lambda \quad \quad \quad (\gamma, \lambda) \longmapsto \gamma \cdot \lambda = \gamma \lambda$$

$$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \quad ; \quad \cdot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

$$(a, b) \longmapsto a + b \quad \quad \quad (a, b) \longmapsto a \cdot b = ab.$$

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

$$(\alpha, \beta) \longmapsto \alpha + \beta \text{ donde si } \alpha = a + ib, \beta = c + id, \text{ entonces}$$

$$\alpha + \beta = (a+c) + i(b+d).$$

$$\cdot : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$$

$$(\alpha, \beta) \longmapsto \alpha \cdot \beta = \alpha \beta \text{ donde si } \alpha = a + ib, \beta = c + id$$

$$= (ac - bd) + i(bc + ad)$$

Aquí  $\mathbb{Q}$  es el conjunto de los números racionales,  $\mathbb{R}$  es el conjunto de los números reales,  $\mathbb{C}$  es el conjunto de los números complejos,  $+$  y  $\cdot$ , son la suma y el producto usuales entre números.

Es bien conocido que estas operaciones son conmutativas y asociativas.