Álgebra Lineal

Tema 2: Estructuras Algebraicas

`ingenierocontracabrones.blogspot.com`

`mclnaranjito@gmail.com`

25 de agosto de 2016

Índice general

2. Estructuras algebraicas **5**

2.1. Operación interna 5

2.2. Operación externa 6

2.3. Homomorfismos 6

2.4. Grupo 7

2.5. Anillo 10

Capítulo 2

Estructuras algebraicas

2.1. Operación interna

Sea A un conjunto no vacío. Se llama operación interna definida en A a cualquier aplicación de $A \times A$ en A que asocia a cada par (a, b) de elementos de A un único elemento c, resultado de operar a con b. Mátemáticamente, para el operador "$*$", se expresa de la siguiente forma:

$$\begin{array}{c} A \times A \xrightarrow{*} A \\ (a, b) \rightarrow c := a * b \end{array} \qquad \text{con } a, b, c \in A$$

Ejemplo:

El producto de números reales $(\mathbb{R}, \cdot)$ es una operación interna del conjunto de los números reales, ya que cualquier producto de números reales da como resultado otro número real.

$$x \cdot y \in \mathbb{R} \quad \forall x, y \in \mathbb{R}$$

Propiedades

Sea $(A, *)$ un conjunto no vacío (A) donde hay definida una operación interna $(*)$. Diremos que la operación es:

- **Asociativa** $\Leftrightarrow a * (b * c) = (a * b) * c \quad \forall a, b, c \in A$
- **Conmutativa** $\Leftrightarrow a * b = b * a \quad \forall a, b \in A$

Añadamos una nueva operación interna a nuestro par, obteniendo $(A, *, \circ)$. Diremos que $\circ$ es **distributiva** respecto de $*$ si

$$\forall a, b, c \in A, \begin{cases} a \circ (b * c) = (a \circ b) * (a \circ c), \\ (a * b) \circ c = (a \circ c) * (b \circ c) \end{cases}$$

Elementos particulares

- Elemento neutro e: $\quad a * e = e * a = a$
- Elemento simétrico a': $\quad a * a' = a' * a = e$

Ejemplo:

Sea $(\mathbb{R}, +, \cdot)$ el conjunto de los números reales con las operaciones internas de producto y suma. Podemos comprobar que tanto el producto como la suma son asociativos y conmutativos. Además el producto es distributivo respecto de la suma ya que:

$$\forall a, b, c \in \mathbb{R}, \begin{cases} a \cdot (b + c) = (a \cdot b) + (a \cdot c), \\ (a + b) \cdot c = (a \cdot c) + (b \cdot c) \end{cases}$$

2.2. Operación externa

Dados dos conjuntos A y K, se llama operación externa definida en A y con dominio de escalares K, a cualquier aplicación:

$$\begin{array}{c} K \times A \xrightarrow{\perp} A \\ (k, a) \to b := k \perp a \end{array} \qquad \text{con} \quad \begin{array}{c} k \in K \\ a \in A \end{array}$$

Ejemplo:

Sea $V_3 \equiv \{v = (x, y, z) \quad \forall x, y, z \in \mathbb{R}\}$ el conjunto de los vectores reales de tres dimensiones y el conjunto de los escalares enteros $K \equiv \{k \quad \forall k \in \mathbb{Z}\}$. El producto de escalares por vectores es operación externa ya que $k \cdot v \in V_3$.

2.3. Homomorfismos

Sean $(A, *)$ y $(B, \circ)$ dos conjuntos con operaciones internas definidas. Una aplicación $f : A \to B$ es un **homomorfismo** si

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in A$$

Si f es un homomorfismo y además

- es inyectivo se llamará **monomorfismo**.
- es sobreyectivo se llamará **epimorfismo**.
- es biyectivo se llamará **isomorfismo**.
- $A = B$ se llamará **endomorfismo**.
- es endomorfismo biyectivo se llamará **automorfismo**

Ejemplo:

Sean $G = (\mathbb{R}, +)$ y $H = (\mathbb{R}^+, \cdot)$. Definamos una aplicación

$$\begin{gathered} f : G \leftarrow H \\ x \mapsto e^x \end{gathered}$$

Podemos afirmar que se trata de un homomorfismo ya que

$$\begin{gathered} f(x + y) = f(x) \cdot f(y) \\ e^{x+y} = e^x + e^y \end{gathered}$$

2.4. Grupo

Un **grupo** es una pareja $(G, *)$, donde G es un conjunto en el que está definida una operación interna $*$ que verifica:

1. Asociativa.
2. Existencia de elemento neutro e, es decir, $g * e = g$
3. Todo elemento g posee simétrico g', es decir, $g * g' = e$

Si además la operación interna $*$ es conmutativa, el grupo se llamara **abeliano**.

Propiedades de un grupo

- El elemento neutro es único
- $(a * b)' = b' * a'$
- $(a')' = a$
- $a * x = a * y \Rightarrow x = y$

Orden de un grupo

Sea $(G, *)$ un grupo. El **orden** de un elemento $a \in G$ es el menor entero positivo $k \in \mathbb{N}^*$ para el que $a^k = e$. Si no existe k, el orden es infinito o cero.

Al número de elementos de un grupo se le llama **orden** de G y se denota por $|G|$.

Ejemplo:

El conjunto de los números enteros con la suma $(\mathbb{Z}, +)$ es un grupo abeliano ya que:

1. La suma de numeros enteros es otro número entero.
2. El elemento neutro de los enteros con la suma es el cero: $z + 0 = z$.
3. Todo z posee un simétrico $-z$: $z + (-z) = 0$.
4. La suma de enteros es conmutativa: $z_1 + z_2 = z_2 + z_1$.

A modo de ejemplo diremos que el orden del grupo es infinito $|\mathbb{Z}| = \infty$. El orden de los elementos son

$$
\begin{aligned}
&|1| = 1 \\
&|-1| = 2 \\
&|z| = \infty \quad \forall z \in \mathbb{Z} - \{-1, 1\}
\end{aligned}
$$

Subgrupo

Sea $(G, *)$ un grupo y $H \subset G$, un subconjunto suyo no vacío. $(H, *)$ es **subgrupo** si también posee estructura de grupo.

Caracterización

Un subconjunto H es subgrupo si se cumple que

$$\forall a, b \in H \Rightarrow a * b \in H \tag{2.1}$$
$$\forall a \in H \Rightarrow a' \in H \tag{2.2}$$

Las ecuaciones 2.1 y 2.2 se pueden resumir en la siguiente

$$\forall a, b \in H \Rightarrow a * b' \in H$$

Clases de un grupo

Dado un grupo G, un subgrupo H y un elemento $a \in G$ arbitrario fijo, a los conjuntos

$$aH = \{x/x \in G, x = a * h, h \in H\}$$
$$Ha = \{x/x \in G, x = h * a, h \in H\}$$

se les denomina respectivamente **clases** del grupo G a la izquierda y a la derecha módulo el subgrupo H. Se les llama así por ser clases de cierta relación de equivalencia [1] y, por tanto, forman particiones del grupo G.

Si $aH = Ha$ entonces, H es un subgrupo **normal o invariante**.

Supongamos que el grupo G es finito y que posee n clases a la izquierda módulo H. Entonces,

$$G = a_1H \cup a_2H \cup \cdots \cup a_nH$$

$$|G| = |a_1H| + |a_2H| + \cdots + |a_nH| = n|H|$$

por lo que el orden de un grupo finito G será múltiplo del orden de cualquier subgrupo suyo (**teorema de Lagrange**).

Al cociente $n = |G|/|H|$ se le denomina **índice del subgrupo** H.

Un grupo G se dice **finitamente generado** si existe una parte finita A de G que engendra todo G. Si A se reduce a un elemento, el grupo G se llama **monógeno**.

El grupo G es **cíclico** si es monógeno y finito.

$$G =< a >= \{a^n : n \in \mathbb{Z}\}$$

Nota: Con a^n nos referimos a aplicar n veces el operador $*$ sobre a. Ésto coincidirá con la potencia en el caso de que la operación sea el producto pero, en general, no es así.

[1] La relación es $x \sim y \Leftrightarrow x' * y \in H$, aunque no es de interés para ésta explicación.

Homomorfismo de grupos

Al igual que en la sección anterior, dos grupos $(G_1, *)$, $(G_2, \circ)$ y una aplicación $f : G_1 \to G_2$ es **homomorfismo** si

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in G_1$$

Llamamos **núcleo** de f, representándose por $Ker(f)$, al conjunto de los elementos del dominio cuya imagen es el elemento neutro de G_2.

$$Ker(f) = \{x \in G_1 : f(x) = e_2\} = f^{-1}(e_2)$$

Llamamos **imagen** de f, denotándose por $Im(f)$, como el subconjunto de G_2 formado por aquellos elementos que son imagen de algún elemento de G_1. Es decir,

$$Im(f) = \{y \in G_2 : \exists x \in G_1, f(x) = y\}$$

Por tanto, podemos decir que

$$\begin{aligned} &f \ es\ inyectiva\ \Leftrightarrow Ker(f) = \{e_1\} \\ &f \ es\ sobreyectiva\ \Leftrightarrow Im(f) = G_2 \end{aligned}$$

2.5. Anillo

Un anillo es un conjunto dotado con dos operaciones internas llamadas suma y producto. El anillo $(R, +, \cdot)$ cumple que:

1. $(R, +)$ es un grupo abeliano.

2. El producto es asociativo.

3. Existe un elemento neutro para la multiplicación.

4. El producto es distributivo respecto a la suma.

Si el producto es conmutativo se dice que el anillo es conmutativo. Si el producto posee elemento neutro es unitario.

El elemento neutro de la suma será 0 y el del producto 1.

Subanillo

Cuerpo

Un cuerpo es un anillo conmutativo y unitario en el que todo elemento distinto de cero es invertible respecto del producto, es decir, un anillo de división conmutativo.

Por ejemplo, los números reales con la suma y el producto algebraicos $(\mathbb{R}, +, \cdot)$ es un cuerpo ya que:

1. $(\mathbb{R}, +)$ es un grupo abeliano (siendo 0 el elemento neutro de la suma)

2. El producto de números reales es asociativo.

3. El elemento neutro de la multiplicación es el 1.

4. El producto es distributivo respecto de la suma (propiedades de anillo cumplidas).

5. El anillo es conmutativo, ya que el producto de números reales lo es.

6. El anillo es unitario ya que el neutro de la multiplicación es distinto del de la suma.

7. Todo elemento distinto de cero es invertible respecto del producto: Sea $r \in \mathbb{R}$ y $r \neq 0$, entonces $\frac{1}{r} \in \mathbb{R}$.

Así lo serían también $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ y $(\mathbb{Q}, +, \cdot)$.