Tema 1

Estructuras Algebraicas

Definición 1 *Sea A un conjunto no vacío. Una* ***operación binaria*** *(u* ***operación interna****) en A es una aplicación*

$$* : A \times A \to A.$$

Es decir, tenemos una regla que a cada par de elementos x, y de A les asocia un único elemento de A, denotado por $x * y$.

Un conjunto con una o más operaciones internas se llama ***álgebra binaria, estructura algebraica*** *o* ***sistema algebraico****, y se denota $(A, *, \#, ...)$.*

Las estructuras se caracterizarán atendiendo a las propiedades que verifiquen las operaciones definidas en el conjunto.

Ejemplos: Las siguientes son estructuras algebraicas

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$.
2. $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$.
3. El conjunto de matrices de orden 2 con coeficientes enteros (racionales o reales) con la suma o el producto de matrices.
4. La composición es una operación interna en X^X, siendo $X^X = \{f : X \to X / \ f \text{ aplicación } \}$
5. En $\mathbb{R}^* = \mathbb{R} - \{0\}$, la regla $x * y = x/y$ define una operación interna, mientras que en $\mathbb{Z}^* = \mathbb{Z} - \{0\}$, $x * y = x/y$ no lo es.
6. En $\mathbb{N}$, $x * y =$ (un número natural menor que x, y) no es una operación, pues $*$ no es aplicación.

Si el conjunto A es finito, $A = \{a_1, a_2, \cdots, a_n\}$, una operación binaria en A puede definirse mediante una tabla:

$*$	a_1	$\cdots$	a_j	$\cdots$	a_n
a_1	$a_1 * a_1$	$\cdots$	$a_1 * a_j$	$\cdots$	$a_1 * a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	$a_i * a_1$	$\cdots$	$a_i * a_j$	$\cdots$	$a_i * a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_n	$a_n * a_1$	$\cdots$	$a_n * a_j$	$\cdots$	$a_n * a_n$

Ejemplo: Sea S_3 el conjunto de permutaciones de tres elementos, $S_3 = \{1, \alpha, \beta, \gamma, \delta, \epsilon\}$. Definimos en S_3 la operación $\circ$ dada por la siguiente tabla:

$$1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \quad \alpha = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$\beta = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \quad \gamma = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

$$\delta = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \quad \epsilon = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

$\circ$	1	α	β	γ	δ	ϵ
1	1	α	β	γ	δ	ϵ
α	α	1	δ	ϵ	β	γ
β	β	γ	1	α	ϵ	δ
γ	γ	β	ϵ	δ	1	α
δ	δ	ϵ	α	1	γ	β
ϵ	ϵ	δ	γ	β	α	1

Nota $\delta = \alpha \circ \beta$.

Definición 2 *Sea $(A, *)$ una estructura algebraica. Se dice que*

1. *La operación interna * es **asociativa** si $(a * b) * c = a * (b * c)$, $\forall\, a, b, c \in A$.*
2. *La operación interna * es **conmutativa** si $a * b = b * a$, $\forall\, a, b \in A$.*
3. *La operación interna tiene **elemento neutro** si $\exists\, e \in A$ tal que $a * e = a = e * a$, $\forall\, a \in A$.*

   *Si * tiene elemento neutro, es único.*

   *En efecto, si e, e' son neutros de *, entonces $e = e * e' = e'$.*
4. *Supuesto que exista elemento neutro e, un elemento $a \in A$ tiene **simétrico** (o inverso) si $\exists\, a' \in A$ tal que $a * a' = e = a' * a$.*

   *Si * es asociativa y a tiene inverso, éste es único.*

   En efecto, si a' y a'' son inversos de a, $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$. El inverso de a se representa por a^{-1}.
5. *Un elemento $a \in A$ es **regular** o simplificable si*

$$\forall\, b, c \in A,\ (a * b = a * c \Rightarrow b = c)\ y\ (b * a = c * a \Rightarrow b = c).$$

   *Si * es asociativa y a tiene inverso, a es simplificable.*
6. *Un elemento $a \in A$ es **idempotente** si $a * a = a$.*
7. *La operación * es **distributiva respecto a otra operación interna** $\#$ en A si, $\forall\, a, b, c \in A$*

$$a * (b \# c) = (a * b) \# (a * c) \qquad y \qquad (b \# c) * a = (b * a) \# (c * a)$$

Notación Sea $(A, *)$ una estructura algebraica.

1. Si * es asociativa, se puede escribir $a * b * c$ en lugar de $a * (b * c)$, pues $(a * b) * c = a * (b * c)$. En general, escribiremos $a_1 * a_2 * \cdots * a_n$, pues se operan agrupándolos de dos en dos de cualquier forma (manteniendo el orden de los elementos).
2. El elemento $a * a * \overset{(n}{\cdots} * a$ se escribe a^n.
3. Con notación aditiva, el simétrico de un elemento a se llama opuesto y se representa por $-a$, y $a + a + \overset{(n}{\cdots} + a$ puede denotarse na.

Ejemplos:

1. En $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ las operaciones indicadas son asociativas, conmutativas y $\cdot$ es distributiva respecto a $+$.

2. Sea X un conjunto. En $\mathcal{P}(X)$ la unión y la intersección son operaciones internas, asociativas, conmutativas, tienen elemento neutro ($\emptyset$ y X, respectivamente), y ese elemento es el único simplificable e inversible con la operación correspondiente. Además, la unión es distributiva respecto a la intersección y viceversa.

3. En $X^X = \{f : X \to X / f \text{aplicación}\}$ la composición es una operación interna asociativa, no conmutativa, donde el elemento neutro es la aplicación identidad de X y sólo tienen inverso las aplicaciones biyectivas.

4. En $\mathbb{N}$, la operación $n * m = n(n+m)$ no es asociativa, ni conmutativa.

5. En el conjunto de cadenas finitas de 0's y 1's la concatenación es una operación interna, asociativa, no conmutativa y la secuencia vacía es el elemento neutro.

1.1 Grupos

Definición 3 *Un **grupo** es una estructura algebraica $(G, *)$ tal que la operación binaria $*$ verifica:*

1. ** es asociativa*
2. ** tiene elemento neutro*
3. *todo elemento de G tiene simétrico.*

*Si, además, * es conmutativa se dice que $(G, *)$ es un **grupo conmutativo** o abeliano (en honor al matemático noruego Niels Henrik Abel, 1802-1829).*

Ejemplos: Las siguientes estructuras algebraicas son grupos.

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}_m, +)$.

   Recordemos que en el conjunto $\mathbb{Z}$ se definió la relación "ser congruente módulo m", $\equiv_m$, para un entero $m > 1$, de la forma

   $$\forall a, b \in \mathbb{Z},\ a \equiv_m b \Leftrightarrow a - b = \dot{m} \Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } a - b = km.$$

   Esta relación permite definir en el conjunto cociente $\mathbb{Z}/\equiv_m = \mathbb{Z}_m$ las operación suma módulo m: $[a]+[b] = [a+b]$, con $a, b \in \mathbb{Z}$ sin que dependan del representante elegido, puesto que, para cualesquiera a, b, a' y b' números enteros de modo que $[a] = [a']$ y $[b] = [b']$ se tiene que

   $$\left.\begin{array}{l}[a] = [a'] \Leftrightarrow a - a' = k_1 m,\ \text{con } k_1 \in \mathbb{Z} \\ [b] = [b'] \Leftrightarrow b - b' = k_2 m,\ \text{con } k_2 \in \mathbb{Z}\end{array}\right\} \Rightarrow (a+b) - (a'+b') = (a-a') + (b-b') = (k_1+k_2)m$$

   y, por tanto, $[a] + [b] = [a+b] = [a'+b'] = [a'] + [b']$.

2. $(\mathbb{Q}^*, \cdot)$ $(\mathbb{R}^*, \cdot)$, $(\mathbb{Z}_p^*, \cdot)$ con p primo.

   La relación $\equiv_p$ también permite definir en el conjunto cociente $\mathbb{Z}_p$ la operación producto módulo p: $[a]\cdot[b] = [a \cdot b]$, con $a, b \in \mathbb{Z}$, sin que dependan del representante elegido, puesto que, para cualesquiera a, b, a' y b' números enteros de modo que $[a] = [a']$ y $[b] = [b']$ se tiene que

   $$\left.\begin{array}{l}[a] = [a'] \Leftrightarrow a - a' = k_1 p,\ \text{con } k_1 \in \mathbb{Z} \\ [b] = [b'] \Leftrightarrow b - b' = k_2 p,\ \text{con } k_2 \in \mathbb{Z}\end{array}\right\} \Rightarrow \left\{\begin{array}{l}a \cdot b - a' \cdot b = k_1 bp, \\ a' \cdot b - a' \cdot b' = k_2 a' p,\end{array}\right.$$

   y, por tanto, $a \cdot b - a' \cdot b' = (a \cdot b - a' \cdot b) + (a' \cdot b - a' \cdot b') = (k_1 b + k_2 a')p$; luego

   $$[a] \cdot [b] = [a \cdot b] = [a' \cdot b'] = [a'] \cdot [b'].$$

Además, para cualquier $[a] \in \mathbb{Z}_p^*$, $0 < a < p$, como p es primo $\mathrm{m.c.d.}(a,p) = 1$ y, por tanto, $1 = \alpha a + \beta p$, con α, $\beta \in \mathbb{Z}$. Tomando clases en la expresión anterior, se tiene que

$$[1] = [\alpha a + \beta p] = [\alpha][a] + [\beta][p] = [\alpha][a] + [\beta][0] = [\alpha][a] \Rightarrow [1] = [\alpha][a],$$

por tanto $[\alpha] = [a]^{-1}$.

3. El conjunto de matrices de orden 2 con coeficientes enteros (o reales) con la suma es un grupo conmutativo.

4. $(S_3, \circ)$, con la operación dada anteriormente.

Proposición 1 *En un grupo $(G, *)$ se verifica:*

1. *El elemento neutro es único (suele denotarse por e).*

2. *El simétrico de un elemento g de G es único (se escribe g^{-1}).*

3. *Para cada $g \in G$, $(g^{-1})^{-1} = g$.*

4. *Dados $g, h \in G$, $(g * h)^{-1} = h^{-1} * g^{-1}$.*

5. *Todo elemento de G es simplificable.*

6. *Para cualesquiera $g, h \in G$, la ecuación $g * x = h$ (también, $x * g = h$) tiene solución única en G.*

7. *El neutro es el único elemento idempotente de G.*

8. *Cada elemento de un grupo finito aparece exactamente una vez en cada fila y en cada columna de la tabla de la operación del grupo.*

(Demostración.)

Nota. Cuando la operación del grupo es + (adición), el grupo se dice aditivo, el elemento neutro se denota por 0 y el simétrico de a se escribe $-a$.

Definición 4 *Sean $(G_1, *)$ y $(G_2, \circ)$ dos grupos. Consideremos, en el conjunto $G_1 \times G_2$, la operación interna $(x, y) \cdot (x', y') = (x * x', y \circ y')$. Se verifica que $(G_1 \times G_2, \cdot)$ tiene estructura de grupo, que llamaremos el* ***grupo producto*** *de $(G_1, *)$ y $(G_2, \circ)$. Observemos que su neutro es (e, e'); y para cada $(x, y) \in (G_1 \times G_2)$ su simétrico es $(x, y)^{-1} = (x^{-1}, y^{-1})$.*

Ejemplos: Otros ejemplos de grupos:

1. $G = \{e\}$ se llama grupo trivial.

2. Sean $H = \{0, 2\} \subseteq \mathbb{Z}_4$ y $H' = \{0, 1\} \subseteq \mathbb{Z}_4$. Se verifica que H, con la suma definida en $\mathbb{Z}_4$, es grupo, sin embargo, H'; no lo es.

3. Sean $H = \{1, 6\} \subseteq \mathbb{Z}_7$ y $H' = \{1, 5\} \subseteq \mathbb{Z}_7$. Se verifica que $(H, \cdot)$ es grupo pero $(H', \cdot)$ no lo es.

4. Sean $H = \{1, \alpha\}$ y $H' = \{1, \gamma, \delta\}$ dos subconjuntos de S_3. Se verifica que $(H, \circ)$ es grupo, sin embargo $(H', \circ)$ no lo es.

1.2 Anillos

Hemos utilizado estructuras en las que hay dos operaciones, como la suma y el producto en $\mathbb{Z}$. El objeto más básico de este tipo es un anillo, cuyos axiomas son bastante parecidos a los axiomas aritméticos de los enteros, aunque ligeramente más débiles; y, por lo tanto, más generales.

Definición 5 *Un **anillo** es un conjunto A en el que hay definidas dos operaciones binarias $+$ y $\cdot$ que cumplen los axiomas siguientes:*

1. *$(A, +)$ es un grupo conmutativo*
2. *$\cdot$ es asociativa*
3. *$\cdot$ es distributiva respecto a $+$.*

Nota. Las operaciones $+$ y $\cdot$ se llaman **suma** y **producto** en el anillo (aunque pueden ser diferentes de la suma y producto usuales). El elemento neutro para $+$ se representa con el símbolo 0 (**elemento cero**) y el simétrico aditivo de a se escribe $-a$ y se denomina **opuesto de** a.

Si la operación $\cdot$ es conmutativa se dice que A es un **anillo conmutativo**. Si existe neutro para $\cdot$ se dice que A es un **anillo unitario** y el neutro se denota por el símbolo 1 (**elemento uno**).

Ejemplos:

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_m, +, \cdot)$.
2. El conjunto de matrices 2×2 con coeficientes enteros (o reales) con la suma y producto de matrices. Este anillo no es conmutativo, pero sí es unitario.
3. $(\mathbb{Z}, \oplus, \otimes)$ con $\oplus$ y $\otimes$ definidas, para cada par de números enteros x, y por
$$x \oplus y = x + y - 1, \qquad x \otimes y = x + y - xy,$$
es un anillo conmutativo y unitario en el cual el neutro para $\oplus$ es el número entero 1 y el neutro para $\otimes$ es el número entero 0.
4. En $A = \{a, b, c, d, e\}$ se define las operaciones $+$ y $\cdot$ dadas por la tablas siguientes

$+$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

$\cdot$	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

Es un anillo finito conmutativo y unitario. El elemento a es el neutro para la suma, mientras que b es el neutro para el producto.

A partir de aquí, consideraremos que $(A, +, \cdot)$ es un anillo.

Proposición 2

1. *Para todo elemento $a \in A$ se verifica que $0 = 0 \cdot a = a \cdot 0$.*
2. *Si A es unitario y $A \neq \{0\}$ entonces $0 \neq 1$.*
   En efecto, para $a \neq 0$, $a \cdot 1 = a \neq 0 = a \cdot 0$, por lo tanto $0 \neq 1$.
3. *$(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$, $\forall a, b \in A$.*
4. *$(-a) \cdot (-b) = a \cdot b$, $\forall a, b \in A$.*

(Demostración.)

1.3 Divisores de cero y unidades. Dominios y cuerpos

Definición 6 *Un elemento a de un anillo A se llama **divisor de cero** si existe un elemento no nulo $b \in A$ tal que $a \cdot b = 0$ ó $b \cdot a = 0$. Cuando $a \neq 0$ se denomina divisor de cero propio.*

*Un elemento a de un anillo unitario A se llama **inversible** (o **unidad**) si a posee inverso multiplicativo, es decir, si existe un elemento $b \in A$ tal que $a \cdot b = 1 = b \cdot a$.*

Observación 1 *Con la notación anterior, si a es unidad el elemento b es único, se denomina **inverso de** a y se representa por a^{-1}. Se denota por $U(A)$ el **conjunto de los elementos inversibles del anillo** A, que es un grupo con la operación producto, llamado **grupo multiplicativo de** A.*

Ejemplos:

1. $\mathbb{Z}$ no tiene divisores de cero propios y $U(\mathbb{Z}) = \{1, -1\}$.
2. En $\mathbb{R}$ no hay divisores de cero propios y $U(\mathbb{R}) = R - \{0\}$.
3. En $\mathbb{Z}_m^*$ un elemento $[a]$ es inversible si, y sólo si, $\text{m. c. d.}(a, m) = 1$.
   Para cualquier $[a] \in \mathbb{Z}_m^*$, $0 < a < p$,

$$\begin{aligned}\text{m. c. d.}(a, m) = 1 &\Leftrightarrow 1 = \alpha a + \beta m, \text{con } \alpha,\ \beta \in \mathbb{Z} \\ &\Leftrightarrow [1] = [\alpha a + \beta m] = [\alpha] \cdot [a] + [\beta] \cdot [m] = [\alpha] \cdot [a] + [0] = [\alpha] \cdot [a] \\ &\Leftrightarrow [1] = [\alpha] \cdot [a] = [a] \cdot [\alpha] \Leftrightarrow [\alpha] = [a]^{-1},\end{aligned}$$

   De este hecho se deduce, por ejemplo, que el cardinal de $U(\mathbb{Z}_m)$ es $\phi(m)$[1]. Así $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$.
4. En el conjunto de matrices cuadradas de orden 2 con coeficientes reales, la matriz B es un divisor de cero, y las matrices inversibles son aquellas cuyo determinante es no nulo; por ejemplo, D es inversible.

$$B = \begin{pmatrix} 2 & 4 \\ 3 & 6 \end{pmatrix} \quad D = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}$$

5. En el anillo $A = \{a, b, c, d, e\}$ del apartado 4 de la sección de ejemplos anterior, todo elemento no nulo es inversible.

Observación 2 *Si $[a] \in \mathbb{Z}_m^*$, $0 < a < p$, y $\text{m. c. d.}(a, m) = d \neq 1$, entonces $a = a_1 d$ y $m = m_1 d$ con $a_1,\ m_1 \in \mathbb{Z}$ y $\text{m. c. d.}(a_1, m_1) = 1$. Así*

$$[a] \cdot [m_1] = [am_1] = [a_1 d m_1] = [a_1 m] = [0],$$

es decir $[a]$ es un divisor de cero.

Proposición 3 *Sea $a \in A$, $a \neq 0$.*

1. *El elemento a es un divisor de cero si, y sólo si, a no es simplificable para el producto.*
2. *Si a es un elemento inversible, a no es divisor de cero.*

(Demostración.)

Los conceptos de divisor de cero e inversible conducen a dos tipos importantes de anillos: los dominios y los cuerpos.

[1] Recordemos que dado un número natural m, se designa por $\phi(m)$ al número de enteros positivos r que no exceden a m y son primos con m. Su expresión es: $\phi(m) = |\{0 < r \leq m \mid \text{m. c. d.}(r, m) = 1\}|$. La función $\phi(m)$ se denomina *función ϕ de Euler*. Claramente $\phi(1) = 1$, $\phi(2) = 1$ y, en general, si p es un primo, todos los enteros menores que p son primos con p, así que $\phi(p) = p - 1$. De hecho, si p es un primo y r un natural, $\phi(p^r) = p^{r-1}(p - 1)$.

Definición 7 *Un anillo conmutativo unitario A, se denomina*

1. ***dominio de integridad*** *(o, simplemente, dominio) si el único divisor de cero es el elemento cero se A;*

2. ***cuerpo*** *(conmutativo) si todo elemento distinto de 0 tiene inverso (es decir, $U(A) = A - \{0\}$).*

Observación 3 *Un cuerpo es un dominio. En efecto, si $a \cdot b = 0$ con $a \neq 0$ en un cuerpo K entonces existe $a^{-1} \in K$ y por tanto $b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$.*

Sin embargo, no todos los dominios son cuerpos, por ejemplo $\mathbb{Z}$ el anillo de los números enteros es un dominio pero no es cuerpo ya que, por ejemplo 2 no tiene inverso multiplicativo.

Proposición 4 *El anillo de enteros módulo n, $\mathbb{Z}_n$, es un cuerpo si y sólo si, n es un número primo.*

Demostración. Veamos en primer lugar que $\mathbb{Z}_n$ cuerpo implica que n es un número primo. Haremos un razonamiento por contradicción.

Supongamos que n no es un número primo. con a y b enteros estrictamente menores que n. En $\mathbb{Z}_n$, tenemos que $[a][b] = [ab] = [n] = [0]$. Si $\mathbb{Z}_n$ fuese un cuerpo, necesariamente $[a] = [0]$ o bien $[b] = [0]$. Pero eso se cumple si $n \mid a$ o $n \mid b$ lo que contradice la hipótesis.

Veamos ahora que si n es primo entonces $\mathbb{Z}_n$, es un cuerpo. Para ello, probaremos que todo elemento no nulo tiene inverso multiplicativo. En efecto, consideremos $[m] \in \mathbb{Z}_n$ con $m < n$. Por ser n primo tenemos que m y n son primos entre sí y por tanto existen enteros tales que $1 = am + bn$, de donde $[1] = [a][m] + [b][n] = [a][m] + [b][0] = [a][m]$. Luego $[m]$ tiene inverso en $\mathbb{Z}_n$. □

Ejemplos:

1. $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ son cuerpos.

2. Dado $a \in \mathbb{Z}_m$, $a \neq 0$, si $\mathrm{m.c.d.}(a, m) = 1$ entonces a es inversible en $\mathbb{Z}_m$, si $\mathrm{m.c.d.}(a, m) \neq 1$, entonces a es divisor de cero. En consecuencia, $\mathbb{Z}_m$ es cuerpo si, y sólo si, $\mathbb{Z}_m$ es un dominio si, y sólo si, m es primo.

3. El conjunto de las matrices de orden 2 con coeficientes en $\mathbb{Z}_3$ de la forma $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ es un cuerpo.

1.4 Característica de un cuerpo

Sea $(K, +, \cdot)$ un cuerpo. Puede ocurrir que:

1. Exista el menor entero positivo $n \in \mathbb{N}$ para el cual $1 + \overset{n}{\cdots} + 1 = 0$. En este caso, es un número primo (por ejemplo, cuando K es finito) y diremos que la característica de K es el primo n.

   Además, $\forall x \in K$, $x \neq 0$, $x + \overset{n}{\cdots} + x = 0$.

2. En otro caso, $1 + \overset{n}{\cdots} + 1 \neq 0$, $\forall n \in \mathbb{N}$ (por ejemplo, $\mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$). En este caso se dice que K es un cuerpo de característica 0.

   Además, $\forall x \in K$, $x \neq 0$ y $\forall n \in \mathbb{N}$, $x + \overset{n}{\cdots} + x \neq 0$.

Ejercicio. Si K es un cuerpo de característica $p \neq 0, (x + y)^p = x^p + y^p$.

Observación 4 *Si K es un cuerpo finito de característica p, entonces $|K| = p^n$, para algún entero positivo n. Recíprocamente, para cualquier entero positivo n, existe un cuerpo finito de cardinal p^n. En la construcción de estos cuerpos se utilizan polinomios con coeficientes en el cuerpo $\mathbb{Z}_p$.*

1.5 Morfismos

Para señalar que dos estructuras algebraicas son esencialmente análogas se dice que son *homomorfas* (semejantes en las formas). La idea se concreta recurriendo a una aplicación entre los conjuntos que *conserve* las operaciones definidas en ellos.

Definición 8 *Sean $(A,*)$, $(B,\#)$ estructuras algebraicas y $f: A \to B$ una aplicación. Diremos que f es un* **morfismo** *si $f(a_1 * a_2) = f(a_1)\#f(a_2)$ para todos $a_1, a_2 \in A$.*

Si f es inyectiva, se llama monomorfismo*; si es sobreyectiva,* epimorfimo*, y si f es biyectiva,* isomorfismo*. En este último caso se dice que $(A,*)$ y $(B,\#)$ son estructuras isomorfas.*

Ejemplos:

1. $f: (\mathbb{N},+) \to (\mathbb{Z},+)$, con $f(x) = -x$ es un monomorfismo.
2. $f: (\mathbb{Z},+) \to (\mathbb{Z}_m,+)$, con $f(x) = [x]$ es un epimorfismo.
3. $f: (\mathbb{R},+) \to (\mathbb{R}^+,\cdot)$, con $f(x) = exp(x)$ es un isomorfismo y $f^{-1}(x) = Ln(x)$.
4. $f: (P(X),\cap) \to (P(X),\cup)$ con $f(Y) = Y^c$ (complementario de Y en X) es un isomorfismo y $f^{-1} = f$.

Proposición 5 *Sea $f: A \to B$ un morfismo.*

1. *Si f es un isomorfismo, entonces f^{-1} es un (iso)morfismo.*
2. *La composición de morfismos es un morfismo.*

(Demostración.)

En el caso particular de que las estructuras algebraicas que intervienen sean grupos, se tiene la siguiente definición.

Definición 9 *Sean $(G,*)$ y $(G',\#)$ dos grupos. Una aplicación $f: G \to G'$ se denomina* ***morfismo de grupos*** *si f conserva la operación. Es decir, $f(g_1 * g_2) = f(g_1)\#f(g_2)$ para todos $g_1, g_2 \in G$.*

Proposición 6 *Sea $f: G \to G'$ un morfismo de grupos*

1. *$f(e) = e'$, siendo e y e' los elementos neutros de G y G', respectivamente.*
2. *$f(g^{-1}) = f(g)^{-1}$, para todo $g \in G$.*
3. *$\mathrm{Im}(f) = f(G)$ es un grupo, $\mathrm{Im}(f) \subseteq G'$.*
4. *$\mathrm{Ker}(f) = \{g \in G / f(g) = e'\}$ es un grupo, $\mathrm{Ker}(f) \subseteq G$.*
5. *f es inyectiva si, y sólo si, $\mathrm{Ker}(f) = \{e\}$.*

(Demostración.)

Ejemplos:

1. $f: (\mathbb{R},+) \to (\mathbb{R}^+,\cdot)$, con $f(x) = e^x$ es un isomorfismo y $f^{-1}(x) = Ln(x)$.
2. $f: (\mathbb{Z},+) \to (\mathbb{Z}_m,+)$, con $f(x) = [x]$ es un epimorfismo.
3. El morfismo de grupos $f: (\mathbb{Z}_4,+) \to (\mathbb{Z}_5^*,\cdot)$, con $f(1) = 2$, es un isomorfismo.

Definición 10 *Sean $(A,+,\cdot)$ y $(B,+,\cdot)$ anillos. Una aplicación $f: A \to B$ se denomina* ***morfismo de anillos*** *si para todos $a_1, a_2 \in A$ se verifica*

1. *$f(a_1 + a_2) = f(a_1) + f(a_2)$ (es decir, es morfismo de grupos)*
2. *$f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$.*

Proposición 7 *1.* $f(0_A) = 0_B$.

2. $f(-a) = -f(a), \forall a \in A$.

3. f *es inyectiva si, y sólo si,* $\mathrm{Ker}(f) = \{0_A\}$.

4. Sean A *un cuerpo y* $f : A \to B$ *un morfismo de anillos. Si* $f \neq 0$ *entonces* f *es un morfismo de anillos inyectivo.*

(Demostración.)

Ejemplos:

1. $f : Z \to \mathbb{Z}_m$, con $f(x) = [x]$ es un epimorfismo.
2. $f : Z \to \mathbb{Z}_6$, definida por $f(2n) = 0$, $f(2n+1) = 3$ es un morfismo de anillos, ambos son unitarios, pero $f(1) \neq 1$.
3. $f : \mathbb{Z}_4 \to \mathbb{Z}_8$, definida por $f(a) = a^2$ no es un morfismo de anillos, pues conserva el producto, pero no la suma (por ejemplo, $f(2+3) \neq f(2) + f(3)$).
4. $f : \mathbb{Z}_4 \to \mathbb{Z}_8$, definida por $f(a) = 2a$ no es un morfismo de anillos, pues conserva la suma, pero no el producto (por ejemplo, $f(1 \cdot 2) \neq f(1) \cdot f(2)$).

Observación 5 *La definición de morfismo de cuerpos es la misma que la de morfismo de anillos, es decir, una aplicación entre cuerpos que conserva las operaciones. Por la Proposición 7, apartado 4, todo morfismo de cuerpos es el morfismo nulo o es inyectivo. Si* $f : K \to K'$ *es un morfismo no nulo, entonces* $f : K - \{0\} \longrightarrow K' - \{0\}$ *es un morfismo de grupos (con el producto) y, en consecuencia,* $f(1_K) = 1_{K'}$ *y* $f(x^{-1}) = (f(x))^{-1}$.