Tema 2.- Grupos: Definición, generalidades y ejemplos

2.1.- Grupos

Definiciones

Un grupo es un par $(G,*)$ donde G es un conjunto no vacío y $*: GxG \to G$es un ley de composición (operación binaria) que satisface los axiomas: *Asociatividad, existencia de elemento neutro y existencia de elemento simétrico.*

Si además verifica el axioma de *conmutatividad,* se dice que es un *grupo conmutativo o abeliano.*

Se llama *orden* del grupo $(G,*)$ al cardinal del conjunto G y se representa por $|G|$. Si $|G|$ es finito, se dice que el grupo es un *grupo finito*.

Definición

En un grupo finito $G = \{x_1, \dots, x_n\}$ *la tabla de grupo (o de Caley*) es la matriz nxn cuya entrada (i,j) es el elemento $x_i x_j$. Un grupo finito es abeliano si y solo si su tabla es simétrica.

2.2.- Generalidades

Definición

En un grupo G *el orden* de un elemento $x \in G$ es el menor entero positivo n, si existe, tal que $x^n = 1$ (o bien $nx = 0$ en notación aditiva). Si tal n no existe se dice que el orden de x es ∞.

2.3.- Ejemplos de Grupos

(I) *Los grupos diédricos*, $D_n, n \geq 3$

Sea $D_n, n \geq 3$, el conjunto de simetrías de un polígono regular de n lados, esto es, movimientos rígidos del plano (isometrías) que llevan el $n - gono$ en sí mismo.

Se tiene que $|D_n| = 2n$. Se denota r la rotación (en sentido antihorario) con centro en el origen y ángulo $2\pi/n$ radianes, y s es la reflexión en el eje que pasa por el vértice 1 y el origen.

$$D_n = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

Definición

Un conjunto de generadores de un grupo G es un subconjunto $S \subset G$ tal que todo elemento de G puede escribirse como un producto finito de elementos de S y de sus inversos. Lo denotamos por $G = \langle S \rangle$.

Si un grafo G está generado por un subconjunto S y existe un conjunto de relaciones $R_1, \dots, R_m$ (donde cada R_i es un igualdad entre los elementos de $S \cup \{1\}$) tal que cualquiera relación entre los elementos de S pueda deducirse de éstas, entonces se dice que estos generadores y relaciones constituyen *una representación* de G y lo denotaremos

$$G = \langle S : R_1, \dots, R_m \rangle$$

Ejemplos:

$$D_n = \langle r, s / \ s^2 = 1 \ \ r^n = 1 \ \ sr = r^{-1}s \rangle \quad C_n = \langle x / \ x^n = 1 \rangle$$

$$V^{abs} = \langle x, y / \ x^2 = 1 \ \ y^2 = 1 \ \ (xy)^2 = 1 \rangle = \{1, x, y, xy\} \ \ Grupo\ de\ Kleim\ abstracto$$

$$Q_2^{abs} = \langle x, y / \ x^4 = 1 \ \ y^2 = x^2 \ \ yxy^{-1} = x^{-1} \rangle = \{1, x, x^2, x^3, y, yx, yx^2, yx^3\}$$

(II) *Los grupos simétricos,* S_n

El conjunto S_n de permutaciones del conjunto $X = \{1,2, \dots, n\}$, y donde $|S_n| = n!$.

El número de ciclos de longitud m de S_n esta dado por la expresión

$$\frac{V_n^m}{m} = \frac{n!}{(n-m)!\, m}$$

El orden de un ciclo de longitud m es m. Los ciclos de orden 2 se llaman *trasposiciones*.

Se puede realizar la descomposición en ciclos disjuntos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$$

$$\sigma = (1 \quad 12 \quad 8 \quad 10 \quad 4)(2 \quad 13)(5 \quad 11 \quad 7)(6 \quad 9)$$

Para calcular σ^{-1}, se hace los números en orden inverso:

$$\sigma^{-1} = (4 \quad 10 \quad 8 \quad 12 \quad 1)(13 \quad 2)(7 \quad 11 \quad 5)(9 \quad 6)$$

Teorema

Toda permutación $\sigma \in S_n, \sigma \neq 1$, se expresa en la forma $\sigma = \gamma_1 \dots \gamma_k$ donde $\gamma_i \ i = 1, \dots, k$ son ciclos disjuntos de longitud ≥ 2 y esta descomposición es única salvo el orden de factores.

Corolario

El orden de cualquier permutación es igual al m.c.m. de las longitudes de los ciclos disjuntos en que se descomponen.

Proposición

Si $\gamma \in S_n$ es un ciclo de longitud m también lo es todo conjugado suyo, esto es, todo elemento de la forma $\tau\gamma\tau^{-1} \ \ \forall \tau \in S_n$.

Proposición

Toda permutación es un producto de trasposiciones.

$$(x_1 \ \ x_2 \dots \ x_m) = (x_1 \ \ x_m)(x_1 \ \ x_{m-1}) \dots (x_1 \ \ x_2)$$

Definición

Para cada $\sigma \in S_n$ se define *su signatura (signo)* como el valor que le adjudica la aplicación

$$\varepsilon: S_n \to \{1,-1\}/\ \varepsilon(\sigma) = \begin{cases} 1 \ \ si\ \ \sigma(\Delta) = \Delta \\ -1\ si\ \ \sigma(\Delta) = -\Delta \end{cases}$$

$$\Delta = \prod_{1\le i<j\le n} (x_i - x_j) \Longrightarrow \sigma(\Delta) = \prod_{1\le i<j\le n} \left(x_{\sigma(i)} - x_{\sigma(j)}\right)$$

Si $\varepsilon(\sigma) = 1$ se dice que σ es una permutación *par* y si $\varepsilon(\sigma) = -1$ se dice que σ es una permutación *impar*.

Proposición

$$\varepsilon(\tau\sigma) = \varepsilon(\tau)\varepsilon(\sigma)\ \ \forall \tau, \sigma \in S_n$$

Corolario

Las trasposiciones son permutaciones impares y ε es un aplicación sobreyectiva.

Corolario

Una permutación $\sigma \in S_n$ es par (respectivamente impar) si y solo si el número de ciclos de longitud par en su descomposición es par (respectivamente impar).

(III) *Los grupos alternados*, A_n

Es el formado por las permutaciones pares de S_n , y donde $|A_n| = \frac{n!}{2}$.

Proposición

Se tiene:

a.- $S_n = \langle (1 \quad 2), (2 \quad 3), \dots, (n-1 \quad n) \rangle$

b.- $S_n = \langle (1 \quad 2), (1 \quad 2 \quad \dots \quad n) \rangle$

c.- $S_n = \langle (1 \quad 2), (1 \quad 3), \dots, (1 \quad n) \rangle$

d.- $A_n = \langle (1 \quad x \quad y) \rangle = \langle (x_1 \quad x_2 \quad x_3) \rangle = \langle (1 \quad 2 \quad 3), (1 \quad 2 \quad 4), (1 \quad 3 \quad 4) \rangle \ \ n \ge 3$

(IV) *Los grupos de matrices*

Si F es un cuerpo el conjunto $M_n(F)$ de las matrices cuadradas de orden n con entradas en F es un anillo con las operaciones usuales de suma y multiplicación de matrices.

Sea $GL_n(F) = \{A \in M_n(F) \setminus A\ tiene\ inversa\}$, se llama el *grupo lineal general* de grado n sobre F. Si F es un cuerpo finito con q elementos entonces:

$$|GL_n(F)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$

Ejemplo: $F = Z_3 \Longrightarrow |GL_2(Z_3)| = (3^2 - 1)(3^2 - 3) = 48$

Sea $SL_n(F) = \{A \in GL_n(F) \setminus detA = 1\}$, se llama el *grupo lineal especial* de grado n sobre F. Si F es un cuerpo finito con q elementos entonces:

$$|SL_n(F)| = \frac{|GL_n(F)|}{q-1} = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{n-1})}{q-1}$$

Ejemplo: $F = Z_3$

$$\Longrightarrow |SL_2(Z_3)| = \frac{|GL_n(F)|}{q-1} = \frac{48}{2} = 24$$

2.4.- Homomorfismos de grupos

Dados dos grupos G y H, un homomorfismo de grupos de G en H es un aplicación $f: G \to H$ que verifica que $\forall x, y \in G, f(xy) = f(x)f(y)$. En tal caso se dice que G se dominio de f y H el codominio o rango de f.

Lema

Si $f: G \to H$ es un homomorfismo de grupos entonces:

a.- $f(1) = 1$ b.- $f(x^{-1}) = f^{-1}(x)\ \forall x \in G$

Definición

$$Imf = \{f(x) \setminus x \in G\} \quad kerf = \{x \in G \setminus f(x) = 1\}$$

Un homomorfismo de grupos se dice que es un *monomorfismo* (respectivamente *epimorfismo o isomorfismo*) si la aplicación f es inyectiva (respectivamente sobreyectiva o biyectiva).

Si $G = H$, se dice que es un *endomorfismo*, y en este caso, es un isomorfismo, se dice que es un *automorfismo*.

Proposición

Sea $f: G \to H$ es un homomorfismo de grupos entonces:

a.- f es monomorfismo $\Leftrightarrow kerf = 1$

b.- f es isomorfismo $\Leftrightarrow f$ tiene inverso ($f^{-1}: H \to G, f^{-1}f = Id_G\ ff^{-1} = Id_H$)

Proposición

$i)$ Si $f: X \to Y$ es una aplicación biyectiva entre los conjuntos X e Y se tiene que la aplicación $\varphi: Perm(X) \to Perm(Y)$ dada por $\varphi(\sigma) = f\sigma f^{-1}$ es un isomorfismo de grupos.

$ii)$ El conjunto de $Aut(G)$ de los automorfismos de un grupo G es un grupo (con la operación de composición).

$iii)$ Si $f: G \to H$ es un isomorfismo de grupos entonces $|G| = |H|$.

$iv)$ Si G y H son grupos isomorfos entonces G es abeliano si y solo si H es abeliano.

v) Si $f: G \to H$ es un isomorfismo entonces, $\forall x \in X, o(x) = o(f(x))$.

Teorema (Dyck)

Sea G un grupo finito con una presentación $G = \langle S \setminus R_1, \dots, R_k \rangle$ donde $S = \{s_1, \dots, s_m\}$. Sea H otro grupo finito y $\{r_1, \dots, r_m\} \subset H$ y supongamos que cualquier relación satisfecha en G por los s_i $i = 1, \dots, m$, es también satisfecha en H cuando s_i es sustituido por r_i $i = 1, \dots, m$. En estas condiciones se puede asegurar que existe un único homomorfismo de grupos $f: G \to H$ tal que $f(s_i) = r_i$ $i = 1, \dots, m$. Si además $\{r_1, \dots, r_m\}$ es un conjunto de generadores de H entonces f es un epimorfismo y si además $|G| = |H|$ entonces f es un isomorfismo.