1 Definición y propiedades

Definición 1.1 *Sea G un conjunto. Una operación binaria en G es una aplicación m: $G \times G \to G$.*

Definición 1.2 *Sea G un conjunto*

i) Si G tiene una operación binaria $*$ definida en G, se dice que G es un **grupoide**.

ii) Un grupoide G se llama un **semigrupo** *si $*$ cumple la propiedad asociativa: dados g_1, g_2 y g_3 en G, se tiene que $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.*

iii) Un semigrupo G se llama **monoide** *si existe un elemento e en G tal que $e * g = g * e = g$ para cualquier g en G. Dicho elemento e se denomina elemento neutro.*

iv) Un semigrupo se llama **grupo** *si para cada elemento g en G existe otro elemento g' en G tal que $g * g' = g' * g = e$. Dicho elemento se denomina elemento simétrico de g.*

Si además $*$ verifica la propiedad conmutativa, es decir,

$$g_1 * g_2 = g_2 * g_1$$

para cualesquiera $g_1, g_2 \in G$ se dice que G es un grupoide, semigrupo, monoide o grupo **abeliano** *según corresponda.*

Ejemplos i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}-0, \cdot)$, $(\mathbb{Z}_m, +)$, $U(\mathbb{Z}_m, \cdot)$ son grupos.

ii) $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$ o $(\mathbb{Q}, \cdot)$ son monoides pero no son grupos.

iii) $(\mathbb{Z}_m - 0, \cdot)$ es un grupo siempre que m sea un número primo.

Lema 1.3 (Propiedad cancelativa) *Sea (G,*) un grupo y sean a, b y c elementos de G. Entonces:*

i) $a * c = b * c$ *implica que* $a = b$.

ii) $a * b = a * c$ *implica que* $b = c$.

Lema 1.4 *Sea* $(G, *)$ *un grupo.*

i) El elemento neutro de G es único.

ii) Sea $g \in G$. *El elemento simétrico de g es único. (Lo denotaremos* g^{-1}*).*

iii) Además, $(g^{-1})^{-1} = g$.

iv) Si $g_1, g_2 \in G$, *se verifica* $(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$.

Definición 1.5 *Sea $(G, *)$ un grupo y sea G' un subconjunto de G. Si $(G', *)$ es un grupo, se dirá que G' es un subgrupo de G.*

$(\mathbb{Z}, +)$ en $(\mathbb{Q}, +)$ es un ejemplo de subgrupo.

Proposición 1.6 *Sea $(G, *)$ un grupo y G' un subconjunto de G. G' es un subgrupo de G con la operación $*$ si y sólo si para cualesquiera g_1 y g_2 en G' se tiene que $g_1 * g_2^{-1}$ es un elemento de G'.*

Denotaremos por g^n al elemento $g * g * \cdots * g$ (n veces operado) de G.

Proposición 1.7 *Sea $(G, *)$ un grupo y sea S un subconjunto de G. Entonces $H = \{g_1^{n_1} * g_2^{n_2} * \cdots * g_m^{n_m}\}$, donde los g_i y son elementos de S y los n_i son números enteros, es un subgrupo de G. Además es el menor subgrupo de G que contiene a S.*

Dado un grupo $(G, *)$ y S un subconjunto de G, el menor subgrupo de G que contiene a S se denotará por $< S >$. Debido a la forma de los elementos de $< S >$, se dice que los elementos de S generan $< S >$.

Definición 1.8 *Un grupo se dice cíclico si esta generado por un único elemento.*

Definición 1.9 *Sea $(G, *)$ un grupo y g un elemento de G. El orden de g es el número de elementos del subgrupo $< g >$.*

Definición 1.10 *Sean $(G, *)$ y $(G', *')$ dos grupos y $f : G \to G'$ una aplicación de G en G'. Se dice que f es un homomorfismo de grupos si $f(a*b) = f(a)*'f(b)$ para cualesquiera $a, b \in G$.*

En caso de que f sea una biyección se dice que f es un isomorfismo de grupos, o bien que G y G' son grupos isomorfos.

Ejemplo $f : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \times)$, $f(x) = 2^x$.

Proposición 1.11 *Sea f un homomorfismo entre dos grupos $(G, *)$ y $(G', *')$.*

1) $f(e) = e'$, donde e y e' son los elementos neutros de G y G' respectivamente.

2) $f(g^{-1}) = f(g)^{-1}$ para cualquier elemento g de G.

2 El grupo simétrico S_n

Definición 2.1 *Dado un conjunto A, el grupo S_A de las biyecciones en A se llama grupo simétrico sobre A. Cada elemento de S_A es, lo que se llama, una permutación en A. Cuando $A = \{1, 2, 3, \cdots, n\}$, S_A será denotado simplemente por S_n. S_n se denomina grupo simétrico de orden n.*

Dado entonces $A = \{1, 2, 3, \cdots, n\}$, si se considera un elemento a de S_n, éste puede ser representado en la forma:

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n-1) & \alpha(n) \end{pmatrix}$$

donde $\alpha(i)$ representa la imagen de i mediante la aplicación α.

La composición de biyecciones puede representarse en este caso de la siguiente forma. Sean α y β dos elementos de S_n. Entonces si se escribe

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n-1) & \alpha(n) \\ \beta(\alpha(1)) & \beta(\alpha(2)) & \cdots & \beta(\alpha(n-1)) & \beta(\alpha(n)) \end{pmatrix}$$

la permutación $\beta\alpha$ es

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \beta(\alpha(1)) & \beta(\alpha(2)) & \cdots & \beta(\alpha(n-1)) & \beta(\alpha(n)) \end{pmatrix}$$

3 Ciclos

Definición 3.1 *Sean $i_1, i_2, .., i_k$ k enteros distintos en $A = \{1, 2, ..., n\}$. El símbolo $(i_1 i_2 ... i_k)$ representará la permutación $\sigma \in S_n$ donde $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \sigma(i_j) = i_{j+1}$ para $j < k$, $\sigma(i_k) = i_1$, y $\sigma(s) = s$ para cualquier $s \in A$ si $s \neq i_1, i_2, ..., i_k$. Una permutación de la forma $(i_1 i_2 ... i_k)$ se llama un* **ciclo de longitud k**. *Un ciclo de longitud dos se llama una transposición.*

Ejemplo En S_8 el ciclo de orden 5 (13478).

Debido a que la composición de aplicaciones no es, en general, conmutativa se tiene que el producto de ciclos tampoco lo es.

Ejemplos:
a) (1 2 3)(1 3) = (2 3).
b) (1 2)(1 3) = (1 3 2), mientras que (1 3)(1 2) = (1 2 3).

Teorema 3.2 *Toda permutación en S_n puede escribirse como producto de ciclos disjuntos.*

Definición 3.3 *Sea α una permutación en S_n. Llamaremos orden de α al número de elementos del subgrupo generado por α. Dicho numero se denota por $o(\alpha)$.*

Lema 3.4 *Sea $\sigma = (a_1\ \sigma(a_1)\ \sigma^{k-1}(a_1))$ un ciclo. Entonces $o(\sigma) = k$.*

Teorema 3.5 *Sea α una permutación en S_n y $\alpha = \sigma_1 \cdots \sigma_n$ una descomposición como ciclos disjuntos de α. Entonces $o(\alpha)$ es el mínimo común múltiplo de los $o(\sigma_i)$ con $i = 1, \cdots, n$.*

4 Transposiciones

Corolario 4.1 *Cualquier permutación en S_n puede expresarse como producto de transposiciones.*

Teorema 4.2 *Una permutación se expresa como producto de un numero par de transposiciones (se denomina permutación par) o como producto de un numero impar de transposiciones (permutación impar), pero no de las dos formas al mismo tiempo.*

Definición 4.3 *Sea α una permutación y $\alpha = \sigma_1\sigma_2\cdots\sigma_m$ una descomposición de α como producto de transposiciones. Se define la signatura de α como $sig(\alpha) = (-1)^m$. Dicho invariante es +1 en caso de que la permutación sea par y -1 en caso de ser impar. La permutación identidad tiene signatura +1.*

Corolario 4.4 *Sea $\sigma = (a_1\ a_2\ \cdots a_k)$ un ciclo en S_n. Entonces la signatura de σ es $sig(\sigma) = (-1)^{k-1}$.*

Corolario 4.5 *Sean α_1 y α_2 permutaciones en S_n. Entonces $sig(\alpha_1\alpha_2) = sig(\alpha_1)sig(\alpha_2)$.*

5 El grupo alternado A_n

Definición 5.1 *El conjunto de las permutaciones pares de S_n se denota por A_n y se denomina grupo alternado de orden n.*

Proposición 5.2 *A_n es un grupo.*

Proposición 5.3 *$|A_n| = n!/2$.*

6 Grupo diédrico

Definición 6.1 *El grupo diédrico de orden n, D_n, se define como el grupo de simetrías de un polígono regular de n lados. D_n puede verse como un subgrupo de S_n, el subgrupo generado por dos permutaciones de S_n, α y β, tales que $\alpha^n = \beta^2 = Id$ y $\alpha\beta = \beta\alpha^{n-1}$.*

Proposición 6.2 *D_n tiene $2n$ elementos.*