Teoría de Grupos

Definiciones Básicas

Definición 5 (Grupo) *Sea* $(A, *)$ *una estructura algebraica con una ley de composición interna. Decimos que* $(A, *)$ *es un* ***grupo*** *si:*

1. $*$es asociativa.
2. $*$tiene neutro $1 \in G$.
3. toda $g \in G$ tiene inverso $g^{-1} \in G$ para $*$.

Con esta definición de grupo, es directo que el neutro es único, al igual que el inverso g^{-1} de $g \in G$.

También se tienen las siguientes propiedades:

1. $(g^{-1})^{-1} = g$.
2. $(g * h)^{-1} = h^{-1} * g^{-1}$.

Un grupo $(G, *)$, donde $*$es conmutativo, se denomina **Abeliano**.

Ejemplos: Los siguientes son algunos ejemplos de grupos

- $(\mathbb{Z}, +)$ es un grupo abeliano.
- $(\mathbb{Z}_p, +)$ es un grupo abeliano.
- Sea $A = \{\pi : \{1,2,3\} \to \{1,2,3\} \mid \pi$ es función biyectiva $\}$ y se considera la operación $*$:``composición de funciones". Este conjunto tiene 6 elementos que se pueden nombrar $\pi_0, \pi_1, \pi_2, \pi_3, \pi_4, \pi_5$. Luego la operación se puede ver en la tabla

$*$	π_0	π_1	π_2	π_3	π_4	π_5
π_0	π_0	π_1	π_2	π_3	π_4	π_5
π_1	π_1	π_0	π_4	π_5	π_2	π_3
π_2	π_2	π_3	π_0	π_1	π_5	π_4
π_3	π_3	π_2	π_5	π_4	π_0	π_1
π_4	π_4	π_5	π_1	π_0	π_3	π_2
π_5	π_5	π_4	π_3	π_2	π_1	π_0

Con esta operación $(A, *)$ es un grupo, pero no es abeliano.

Definición 6 (Morfismo de grupos) *Una función* $f : G \to H$*, entre dos grupos* $(G, *), (H, \diamond)$ *se dice* ***morfismo (u homomorfismo)*** *ssi:*

$$\forall x, y \in G \qquad f(x * y) = f(x) \diamond f(y).$$

Un morfismo inyectivo suele llamarse **monomorfismo**, uno sobreyectivo se llama **epimorfismo**, y finalmente un morfismo biyectivo se llama **isomorfismo**.

$(G, \cdot) \cong (H, *) \Leftrightarrow G$ isomorfo a H

Endomorfismo es un morfismo de un grupo en si mismo; un **automorfismo** es un isomorfismo endomorfo.

Propiedades

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

1. $f(1) = 1$.
2. Si $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

Si $f : G \to H$ es un morfismo de grupos llamaremos **Núcleo** de f a $Ker(f) = f^{-1}(1)$.

Con esto, f es monomorfismo $\Leftrightarrow Ker(f) = \{1\}$.

Ejemplos:

- La función logaritmo (en cualquier base), $log : (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$ tiene la conocida propiedad $log(a \cdot b) = log(a) + log(b)$, y como es biyectiva, es un isomorfismo entre $(\mathbb{R}_+, \cdot)$ y $(\mathbb{R}, +)$. Así $(\mathbb{R}_+, \cdot)$ y $(\mathbb{R}, +)$ son estructuras isomorfas.
- Si $\alpha \in \mathbb{R}$ es un real fijo, la función $f : (\mathbb{R}, +) \to (R, +)$ tal que $f(x) = \alpha \cdot x$ es un homomorfismo, dado que $f(x_1 + x_2) = \alpha \cdot (x_1 + x_2) = \alpha \cdot x_1 + \alpha \cdot x_2 = f(x_1) + f(x_2)$. Si además $\alpha \neq 0$, entonces f es un automorfismo.

Definición 7 (Subgrupo) *Si* $(G, *)$ *es un grupo, y* $H \subseteq G$*, diremos que* H *es un* ***subgrupo*** *de* G *si* $(H, *)$ *es también un grupo.*

Si H es un subgrupo de $(G, *)$, el neutro de $(H, *)$ es el mismo que el de $(G, *)$, y para cada $g \in H$, si $g^{-1} \in G$ es su inverso en $(G, *)$, también g^{-1} es el inverso de g en $(H, *)$ (y por lo tanto $g^{-1} \in H$).

Una caracterización de los subgrupos es la siguiente:

$H \subseteq G$ es subgrupo ssi:

1. $H \neq \emptyset$.
2. $(\forall x, y \in H) \quad x * y^{-1} \in H$.

Definición 8 *Si* $(G, *)$ *es grupo, una relación de equivalencia* $\sim$ *en G se dice compatible con* $*$ *ssi:*

$$(\forall x, x', y, y' \in G) \qquad x \sim x' \wedge y \sim y' \Rightarrow x * y \sim x' * y'.$$

Dada una relación de equivalencia $\sim$ compatible con $*$, podemos definir una l.c.i. en el conjunto cociente $G/\sim$.

$$[x] * [y] = [x * y].$$

La compatibilidad hace que la operación $*$ en $G/\sim$ esté bien definida. Es directo que en este caso $(G/\sim, *)$ resulta ser un grupo, y la sobreyección canónica

$$\begin{aligned} \nu: \ G &\to G/\sim \\ x &\to \nu(x) = [x]. \end{aligned}$$

es un epimorfismo. (Por este motivo ν también recibe el nombre de epimorfismo canónico).

Ahora, si $\sim$ es compatible con $*$, entonces

$$\begin{aligned} x \sim y &\Leftrightarrow 1 = x^{-1} * x \sim x^{-1} * y \quad \text{(compatibilidad y } \sim \text{refleja)} \\ &\Leftrightarrow x^{-1} * y \in [1]. \end{aligned}$$

Llamemos $H = [1]$ (subgrupo). Con esto se tiene la siguiente propiedad:

Si $h \in H$ y $x \in G$ es un elemento cualquiera de G, entonces $x * h * x^{-1} \in H$. En efecto:

$$\begin{aligned} h \in H &\Leftrightarrow h \sim 1. \\ &\Rightarrow x * h \sim x * 1 = x \quad \text{(compatibilidad de } \sim \text{con } *). \\ &\Rightarrow (x * h) * x^{-1} \sim x * x^{-1} = 1 \quad \text{(compatibilidad de } \sim \text{con } *). \\ &\Rightarrow x * h * x^{-1} \in H = [1] \quad \text{(asociatividad para eliminar paréntesis).} \end{aligned}$$

O sea, $(\forall x \in G)\ x * H * x^{-1} = \{x * h * x^{-1} \mid h \in H\} \subseteq H$.

Definición 9 (Subgrupo normal) *Un subgrupo H de G tal que satisface*

$$(\forall x \in G) \quad x * H * x^{-1} \subseteq H.$$

se llama ***subgrupo normal*** *de G.*

Se usará la siguiente notación para designar a los subgrupos normales de G

$H \lhd G \Leftrightarrow$ \$H\$ subgrupo normal de \$G\$.

Esto caracteriza completamente a las relaciones compatibles con $*$. En efecto, si partimos de un subgrupo normal $H \lhd G$ dado, definimos la relación $\sim_H$ en G tal que

$$x \sim_H y \Leftrightarrow x^{-1} * y \in H$$

Entonces

1. $\sim_H$ es de equivalencia en G.
2. $\sim_H$ es compatible con $*$.
3. $[1] = H$.

Notación: Si G es un grupo, y $H \lhd G$, el cociente $G/\sim_H$ se anota como G/H.
Ejemplos:

- Cualquier subgrupo de un grupo Abeliano $(A,*)$ es un subgrupo normal, gracias a la conmutatividad de la operación $*$. En efecto, sea H subgrupo de A. Entonces
$$x * H * x^{-1} = \{x * h * x^{-1} \mid h \in H\} \overset{\text{conmuta}}{=} \{(x * x^{-1}) * h \mid h \in H\} = H.$$

- El núcleo de todo morfismo de grupos $f : G \to H$ es un subgrupo normal de G; es más, todos los subgrupos normales de G son núcleos de algún morfismo. En efecto
  - Si $a \in G$ y $x \in Ker(f)$ Por lo tanto $a * x * a^{-1} \in Ker(f) \to Ker(f)$ subgrupo normal.
  - Si $K \lhd G$, tomemos $H = G/K$ y $f = \nu_K : G \to G/K$ morfismo. Luego
$$\nu_K(x) = 1 \in G/K \Leftrightarrow [x] = [1] = K \Leftrightarrow x \in K.$$
  Luego $Ker(\nu_K) = K$.

Definición 10 (Subgrupo generado por un subconjunto) *Sea G un grupo, y $A \subseteq G$ un subconjunto cualquiera. Denotemos*
$$< A > = \bigcap_{\substack{A \subseteq H \\ H \text{ subgrupo}}} H.$$
el subgrupo generado por A.
Se tiene $A \subseteq < A >$. Mas aun, $< A >$ es más pequeño (en el sentido de la inclusión) de los subgrupos de G que contiene a A. Evidentemente, si A es subgrupo de G entonces $< A > = A$.

Es también claro que

$$A \subseteq \underbrace{\{a_1^{n_1} \cdots a_k^{n_k} \mid k \geq 0,\ a_1, \cdots, a_k \in A\ ;\ n_1, \cdots, n_k \in \mathbb{Z}\}}_{\text{es subgrupo}} \subseteq < A > .$$

Por lo tanto:

$$< A >= \{a_1^{n_1} \cdots a_k^{n_k} \mid k \geq 0,\ a_1, \cdots, a_k \in A\ ;\ n_1, \cdots, n_k \in \mathbb{Z}\}.$$

Caso interesante

Si $A = \{a\}$ entonces $< A >= \{a^n \mid n \in \mathbb{Z}\}$ y se denomina **subgrupo cíclico generado por a**.

Un grupo G se dice **cíclico** si

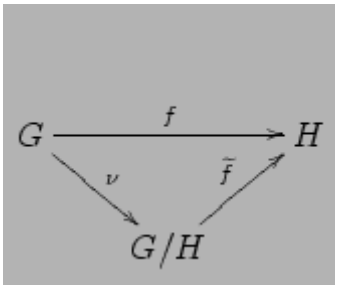
$$\exists a \in G \text{ tal que } < \{a\} >= G.$$

Así $G = \{a^n \mid n \in \mathbb{Z}\}$. Veremos que los grupos cíclicos son "pocos", y para eso nos ayudaremos del siguiente resultado.

Teorema 1 (Teorema del factor) *Si* G, H *grupos,* $f : G \to H$ *morfismo, y* $K \lhd G$ *tal que* $K \subseteq Ker(f)$. *Entonces:*

$$\exists!\ \text{morfismo } \tilde{f} : G/K \to H.$$

tal que el diagrama siguiente es conmutativo



Con ν *el epimorfismo canónico (introducido anteriormente). Es claro que* $f = \tilde{f} \circ \nu$. *Se dice que f se* ***factoriza*** *a través de G/K. Además*

f es un epimorfismo $\Leftrightarrow$ $\tilde{f}$ *es un epimorfismo.*

$\tilde{f}$ *es monomorfismo* $\Leftrightarrow$ $K = Ker(f)$.

Usando este resultado se puede demostrar la siguiente proposición

Proposición 2 *Si G es un grupo cíclico, entonces:*

- Si G es infinito $\Rightarrow G \cong (\mathbb{Z}, +)$.

- Si G es finito $\Rightarrow G \cong (\mathbb{Z}_p, +)$.

Donde $p \geq 1$ *(notemos que* $p = |G|$*).*

Figura 0.1