Resumen Grupos

Mario Calvarro Marines

Índice general

1. Generalidades sobre grupos. Fórmula de Lagrange **1**

1.1. Grupos cíclicos y diedrales 1

1.2. Fórmula de Lagrange 2

2. Subgrupos normales y homomorfismos **5**

2.1. Subgrupos normales 5

2.1.1. Grupo cociente 5

2.2. Homomorfismos de grupos 6

2.2.1. Teoremas de isomorfía 6

Generalidades sobre grupos. Fórmula de Lagrange

Grupos cíclicos y diedrales

Definición (Grupo)

Un conjunto G y la operación $G \times G \to G, (a,b) \mapsto ab$ se dicen ***grupo*** *si cumplen:*

- *Asociatividad.*
- *Elemento neutro.*
- *Elementos inversos.*

Si además es conmutativo, se dice ***abeliano****.*

Proposición

Sea G, grupo, y $g \in G \Rightarrow$

$$\{gx : x \in G\} = G = \{xg : x \in G\}$$

Definición (Subgrupo)

Se dice que $H \subset G$ es un ***subgrupo*** *de G si:*

- $1_G \in H$
- $ab^{-1} \in H,\ \forall a, b \in H$

Definición (Subgrupo generado por un subconjunto)

Sea G, grupo, y $\emptyset \neq S \subset G$. Llamamos ***subgrupo generado por*** *S a:*

$$\langle S \rangle = \bigcap_{H \in \mathcal{H}_S} H$$

donde $\mathcal{H}_S$ es la familia de los subgrupos de G que contienen a S.

Otra forma de expresarlo es:

$$\mathcal{W}(S) = \{s_1^{n_1}, \ldots, s_k^{n_k} : s_i \in S \ \&\ n_j \in \mathbb{N}\}$$

y diremos que un grupo es finitamente generado si $\exists S \subset G : \langle S \rangle = G$.

Proposición (Identidad de Bézout)

Sean $m, n \in \mathbb{Z} \setminus \{0\}$ *y* $d := \operatorname{mcd}(m, n)$. *Entonces,*

$$\exists a, b \in \mathbb{Z} : d = am + bn$$

Definición

Sea $H \leq G$

- *Sea* $a \in G$. *Llamamos* ***conjugado*** *de* H *vía a* a*:*

  $$H^a := a^{-1}Ha := \left\{a^{-1}ha : h \in H\right\}$$

  Diremos que H *y* H^a *son* ***conjugados***
- *Llamamos* ***centralizador*** *de* H *en* G *a:*

  $$C_G(H) := \{a \in G : ah = ha \ \forall h \in H\}$$

  En particular, $\mathcal{Z}(G) := C_G(G)$ *se denomina* ***centro*** *de* G.

Proposición

Sea G *un grupo cíclico (generado por un solo elemento), entonces* $H \leq G$ *es cíclico.*

Fórmula de Lagrange

Proposición

Sean $H, K \leq G$. *Entonces,*

$$\operatorname{ord}(H)\operatorname{ord}(K) = \operatorname{Card}(HK)\operatorname{ord}(H \cap K)$$

En particular, $\operatorname{Card}(HK) \leq \operatorname{ord}(H)\operatorname{ord}(K)$

Definición (Clases laterales)

Sean $H \leq G$.

- *Definimos la clase de equivalencia* $\mathcal{R}_H$ *tal que:*

  $$a\mathcal{R}_H b \Leftrightarrow ab^{-1} \in H$$

  y decimos que a *y* b *son* ***congruentes por la derecha****.*

  $$Ha := \{ha : h \in H\}$$
- *Definimos la clase de equivalencia* $\mathcal{R}^H$ *tal que:*

  $$a\mathcal{R}^H b \Leftrightarrow a^{-1}b \in H$$

  y decimos que a *y* b *son* ***congruentes por la izquierda****.*

  $$aH := \{ah : h \in H\}$$

Las clases de equivalencia definidas por estas relaciones tienen el mismo número de elementos que denominamos ***índice*** *de* H *en* G, $[G:H]$.

Corolario (Fórmula de Lagrange)

Sea G *un grupo finito.*

- $H \leq G$, *entonces:*
$$\operatorname{ord}(G) = \operatorname{ord}(H)\,[G:H]$$
- *Si* $K \leq G$ *y* $\operatorname{mcd}(\operatorname{ord}(H), \operatorname{ord}(K)) = 1$, *entonces* $H \cap K = \{1_G\}$.
- *Si el orden de* G *es un primo, entonces* G *es cíclico y está generado por cualquiera de sus elementos distintos de* 1_G.

Corolario (Pequeño teorema de Fermat)

Dados un entero primo p *y* $k \in \mathbb{Z}$ *se cumple:*

$$k^p \equiv k \operatorname{mód} p$$

Lema

Sea G *grupo y* $a, b \in G$, *elementos de orden* n, m, *entonces:*

- $\forall k \in \mathbb{Z}$, $o\left(a^k\right) = \frac{n}{\operatorname{mcd}(n,k)}$.
- *Si* $ab = ba$ *y* $\operatorname{mcd}(m,n) = 1 \Rightarrow o(ab) = mn$.

Proposición

Sea G *un grupo cíclico finito. Para cada divisor* $d > 0$ *de* $\operatorname{ord}(G)$, $\exists! H \leq G : \operatorname{ord}(H) = d$.

Proposición (Transitividad del índice)

Sean $H, K \leq G : H \subset K$ *y* $[G:H]$ *es finito. Entonces, también lo son* $[G:K]$ *y* $[K:H]$ *y*

$$[G:H] = [G:K] \cdot [K:H]$$

Subgrupos normales y homomorfismos

Subgrupos normales

Definición

Sean $H, K \leq G$, tal que $H \subset K$.

- *H es **subgrupo normal** de K si $Ha = aH, \forall a \in K \Leftrightarrow a^{-1}Ha = H$. En notación, $H \triangleleft K$.*
- *Denominamos **normalizador** de H en G, $N_G(H)$, al subgrupo de Gdefinido por:*

$$N_G(H) := \{a \in G : Ha = aH\} = \left\{a \in G : a^{-1}Ha = H\right\}$$

  Por tanto, $C_G(H) \subset N_G(H)$
- *Un grupo será **simple** si sus únicos subgrupos normales son los triviales.*

Proposición

- *Sean $H \triangleleft G$ y $K \leq G$, entonces $HK \leq G$ y $H \triangleleft HK$.*
- *Sean $H, K \triangleleft G$, entonces:*
  1. *$HK \triangleleft G$.*
  2. *$H \cap K \triangleleft G$. Si, además, $H \cap K = \{1_G\} \Rightarrow hk = kh,\ \forall k \in K, h \in H$.*
- *Sea $a \in G$ una involución, entonces $\langle a \rangle \triangleleft G \Leftrightarrow a \in \mathcal{Z}(G)$.*
- *Sean S, generador, y $H \leq G$ tales que, $s^{-1}Hs = H,\ \forall s \in S$, entonces $H \triangleleft G$.*
- *Sean $H \leq G$ y $K \triangleleft G$ finito tal que $H \subset K$, entonces $H \triangleleft G$.*

Proposición (Indice del normalizador)

Sean $H \leq G$ finito y $\Sigma := \left\{a^{-1}Ha : a \in G\right\}$. Entonces, $\mathrm{Card}(\Sigma) = [G : N_G(H)]$.

Grupo cociente

Sea $H \triangleleft G$ y utilizando la operación:

$$\begin{aligned} G/H \times G/H &\to G/H \\ (Ha, Hb) &\mapsto Hab \end{aligned}$$

definimos un **grupo cociente**.

Teorema (de Correspondencia)

Sean $H \triangleleft G$, $\Sigma_H(G) := \{L \leq G : H \subset L\}$ *y* $\Sigma(G/H) := \{L \leq G/H\}$. *Entonces,*

$$\begin{aligned} \Sigma_H(G) &\to \Sigma(G/H) \\ K &\mapsto K/H \end{aligned}$$

es una biyección.

Lema (Normalizador del cociente)

Sean $H \leq G$ *y* $K \triangleleft G : K \subset H$. *Entonces,*

$$N_G(H)/K = N_{G/K}(H/K)$$

En particular, $H \triangleleft G \Leftrightarrow H/K \triangleleft G/K$.

Homomorfismos de grupos

Definición

Dados G_1, G_2 *y una aplicación* $f : G_1 \to G_2$, *se dice que es* ***homomorfismo*** *de grupos si* $f(ab) = f(a)f(b)$.

Observación:

- $\forall H_1 \leq G$, $H_2 := f(H_1) \leq G_2$. En particular, $\operatorname{img} f := f(G_1) \leq G_2$ y si $H_1 \triangleleft G_1 \Rightarrow H_2 \triangleleft \operatorname{img} f$.
- $\forall H_2 \leq G_2$, $H_1 := f^{-1}H_2 \leq G_1$. Además, $H_2 \triangleleft G_2 \Rightarrow H_1 \leq G_1$.
  En concreto, $\ker f \triangleleft G$.
- f es inyectivo $\Leftrightarrow \ker f = \{1_G\}$.
- La composición de homomorfismos es homomorfismo.
- Llamamos **isomorfismo** a f homomorfismo biyectivo tal que f^{-1} también es homomorfismo. En tal caso, diremos que $G_1 \simeq G_2$ son isomorfos.

Ejemplo:

- Sea $f : G \to G$ isomorfismo. Lo llamaremos **automorfismo** y el conjunto $\operatorname{Aut}(G)$ con la operación $f \cdot g = g \circ f$ forma un subgrupo de Biy (G).
- Dados $H \leq G$ y $a \in N_G(H)$ las aplicaciones:

  $$\begin{aligned} f_a : H &\to H \\ x &\mapsto a^{-1}xa \end{aligned}$$

  forman el grupo $\operatorname{Int}_G(H)$, **automorfismos internos** de H, que es un subgrupo de $\operatorname{Aut}(G)$.

Teoremas de isomorfía

Teorema (Primer teorema de isomorfía)

Dado $f : G_1 \to G_2$ *homomorfismo, la aplicación:*

$$\begin{aligned} \hat{f} : G_1/\ker f &\to \operatorname{img} f \\ a \ker f &\mapsto f(a) \end{aligned}$$

es un isomorfismo.

Corolario

- *Sea* $f : G_1 \to G_2$ *homomorfismo sobreyectivo y* $H \triangleleft G$*. Entonces,* $G_1/f^{-1}(H) \simeq G_2/H$*.*
- *Sea* $H \leq G$*, entonces* $N_G(H)/C_G(H) \simeq \mathrm{Int}_G(H)$*. En particular,* $G/\mathcal{Z}(G) \simeq \mathrm{Int}(G)$*.*