Resumen Grupos

Mario Calvarro Marines

Índice general

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*

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