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:

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

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* $d := \mathrm{mcd}(m, n)$. *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,*

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

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

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:

$$k^p \equiv k \text{ mód } p$$

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, $\operatorname{Card}(\Sigma) = [G : N_G(H)]$.

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 $H \lhd G$, $\Sigma_H(G) := \{L \leq G : H \subset L\}$ *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* $K \lhd G : K \subset H$. *Entonces,*

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

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

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 $H_1 \lhd G_1 \Rightarrow H_2 \lhd \operatorname{img} f$.
- $\forall H_2 \leq G_2$, $H_1 := f^{-1} H_2 \leq G_1$. Además, $H_2 \lhd G_2 \Rightarrow H_1 \leq G_1$.
  En concreto, $\ker f \lhd G$.
- 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:

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

  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,* $G/\mathcal{Z}(G) \simeq \mathrm{Int}(G)$*.*

Grupos de permutaciones

Generalidades

Grupo simétrico

Siendo $n \in \mathbb{N}$, denotamos $I_n := \{x \in \mathbb{Z} : 1 \leq x \leq n\}$ y $\mathcal{S}_n$ al conjunto de biyecciones de I_n en si mismo, que tiene $\operatorname{Card}(\mathcal{S}_n) = n!$. Forma el llamado **grupo de permutaciones** con la composición “al revés”.

$$\begin{aligned} \sigma \cdot \tau := \sigma\tau : I_n &\to I_n \\ j &\mapsto \tau(\sigma(j)) \end{aligned}$$

Teorema (de Cayley)

Todo grupo G es isomorfo a un subgrupo de $\operatorname{Biy}(G)$. En particular, todo grupo finito es isomorfo a un subgrupo del grupo de permutaciones.

Definición (Soporte)

*Llamamos **soporte** de una permutación $\sigma \in \mathcal{S}_n$ al conjunto:*

$$\operatorname{sop}(\sigma) := \{j \in I_n : \sigma(j) \neq j\}$$

*y decimos que dos permutaciones son **disjuntas** si lo son sus soportes.*

Proposición

- *Sea $j \in \operatorname{sop}(j)$, entonces $\sigma(j) \in \operatorname{sop}(j)$.*
- *Dos permutaciones disjuntas conmutan.*

Definición (Ciclos)

*Una permutación $\sigma \in \mathcal{S}_n$ se denomina **ciclo de longitud** k si $\exists i_1, \ldots, i_k \in I_n$ tales que $\operatorname{sop}(\sigma) = \{i_1, \ldots, i_k\}$ y*

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k\ \&\sigma(i_k) = i_1$$

*Si es de longitud 2 lo denominaremos como **transposición**.*

Proposición

- *Toda permutación es composición de ciclos disjuntos y esta factorización es única salvo el orden de los factores.*

- *Si $\sigma_1, \dots, \sigma_r$ son ciclos disjuntos y* $\operatorname{long}(\sigma_i) \leq \operatorname{long}(\sigma_{r+1})$, $\forall 1 \leq i \leq r-1$, *se llama* ***estructura cíclica*** *de $\sigma := \sigma_1 \cdots \sigma_r$ a la r-tupla* $(\operatorname{long}(\sigma_1), \dots, \operatorname{long}(\sigma_r))$.

Lema

Siendo $\sigma, \tau \in \mathcal{S}_n$ disjuntas tal que $o(\sigma) = \ell$ y $o(\tau) = m$, entonces $o(\sigma\tau) = \operatorname{mcm}(\ell, m)$

Corolario

Sea $\sigma := \sigma_1 \cdots \sigma_k$ una factorización en ciclos de la permutación. Entonces,

$$o(\sigma) = \operatorname{mcm}(\operatorname{long}(\sigma_1), \dots, \operatorname{long}(\sigma_k))$$

Definición (Índice)

- *$\forall \sigma \in \mathcal{S}_n$ consideramos el endomorfismo, $f_\sigma : \mathbb{R}^n \to \mathbb{R}^n$ que cumple que $f_\sigma(e_j) = e_{\sigma^{-1}(j)}$. Entonces,*

  $$\begin{aligned} \psi : \mathcal{S}_n &\to \operatorname{Aut}(\mathbb{R}^n) \\ \sigma &\mapsto f_\sigma \end{aligned}$$

  es homomorfismo de grupos.

  La matriz de f_σ proviene de desordenar las columnas de la identidad, por tanto, $\det(f_\sigma) \in \{1, -1\}$. *Definimos, pues, el homomorfismo* ***índice:***

  $$\varepsilon := \det \circ \psi : \mathcal{S}_n \to \mathcal{U}_2$$

- *Al kernel de ε se le denota $\mathcal{A}_n$,* **n-*ésimo grupo alternado***. *Si $\sigma \in \mathcal{A}_n$ se dice* ***par*** *y en caso contrario* ***impar***.

Lema

Las transposiciones constituyen un sistema generador de $\mathcal{S}_n$.

Proposición

El ciclo $\sigma := (a_1, \dots, a_k) \in \mathcal{S}_n \in \mathcal{A}_n \Leftrightarrow k$ impar.

Proposición (Sistemas generadores de $\mathcal{S}_n$ y $\mathcal{A}_n$)

- *$\mathcal{S}_n$ es generado por $\{\alpha_i := (1, i) : 2 \leq i \leq n\}$.*
- *$\mathcal{S}_n$ es generado por $\{\tau_i := (i, i+1) : 1 \leq i \leq n-1\}$.*
- *$\mathcal{S}_n$ es generado por $(1, 2)$ y $(1, \dots, n)$.*
- *$\mathcal{A}_n$ es generado por $\{\sigma_i := (1, 2, i) : 3 \leq i \leq n\}$.*

Teorema de Abel

Teorema (De Abel)

Si $n \geq 5$, $\mathcal{A}_n$ es simple.

Corolario

Si $n \geq 5$, *entonces* $\mathcal{A}_n$ *es el único subgrupo normal propio de* $\mathcal{S}_n$.

Definición

$H \leq \mathcal{S}_n$ *será* ***transitivo*** *si* $\forall\,(i,j)$ *tal que* $1 \leq i,j \leq n$, $\exists \sigma \in H$ *tal que* $\sigma\,(i) = j$.

Proposición

Si $p \in \mathbb{Z}$ *es primo y* $H \leq \mathcal{S}_p$ *transitivo que contiene una transposición, entonces* $H = \mathcal{S}_p$.

Acción de un grupo sobre un conjunto

Ecuación de clases

Acciones, órbitas y estabilizadores

Definición

Denominamos ***acción de un grupo*** G *sobre un conjunto* $X \neq \emptyset$ *a cualquier homomorfismo:*

$$\begin{aligned} G &\to \mathrm{Biy}\,(X) \\ g &\mapsto \tilde{g} \end{aligned}$$

Esto define una relación de equivalencia tal que $x \sim y \Leftrightarrow \exists g \in G : y = \tilde{g}\,(x)$.

La clase de equivalencia definida así se denomina **G-*órbita*** *de* x *bajo la acción de* G, $O_{G,x} := \{\tilde{g}\,(x) : g \in G\}$.

Observación:

$\{O_x : x \in X\}$ particiona X y, siendo $R \subset X$ un conjunto de representantes de las clases, se cumple $X = \bigsqcup_{x \in R} O_x$. Por tanto, $\mathrm{Card}\,(X) = \sum_{x \in R} \mathrm{Card}\,(O_x)$.

Definición

Llamamos ***estabilizador*** *de* $x \in X$ *bajo la acción de* G *al subgrupo:*

$$\mathrm{Stab}_G\,(x) := \{g \in G : \tilde{g}\,(x) = x\}$$

Órbitas y estabilizadores

Proposición (Cardinal de una órbita)

Si G *actúa sobre* X *y* $x \in X$, *se cumple* $\mathrm{Card}\,(O_x) = [G : \mathrm{Stab}_G\,(x)]$.

Corolario (Fórmula de las órbitas)

Sea R *conjunto de representantes de las órbitas de* X, *finito, bajo la acción de* G. *Entonces,*

$$\mathrm{Card}\,(X) = \sum_{x \in R} [G : \mathrm{Stab}_G\,(x)]$$

Aplicaciones a los p-grupos

Definición

Llamamos **p-*grupo*** *a aquellos cuyo orden es potencia de un número primo* p.

Lema (Centro de un p-grupo)

Sea $H \neq \{1_G\} \leq G$, *p-grupo. Entonces,* $H \cap \mathcal{Z}(G) \neq \{1_G\}$. *En particular,* $\mathcal{Z}(G) \neq \{1_G\}$, *por lo que* G *no es simple salvo si* $\operatorname{ord}(G) = p$.

Lema (Criterio de abelianidad)

- *Sean* p, *nº primo,* $n \in \mathbb{N}$ *y* $G : \operatorname{ord}(G) = p^n$. *Entonces,* $\operatorname{ord}(\mathcal{Z}(G)) \neq p^{n-1}$. *En particular, si* $\operatorname{ord}(G) = p^3$, *no abeliano, entonces* $\operatorname{ord}(\mathcal{Z}(G)) = p$.
- *Todo* G *de orden* p^2, *es abeliano.*

Lema

Sean p, *nº primo,* G *finito y* $H \leq G$ *que es p-grupo. Entonces* $[G : H] \equiv [N_G(H) : H] \bmod p$.

Teorema de Cauchy

Teorema (de Cauchy)

Sea p, *nº primo, y* G *grupo de orden múltiplo de* p. *Entonces, el nº de subgrupos de* G *de orden* p *es congruente con* $1 \bmod p$. *En particular,* $\underline{\exists a \in G \text{ de orden } p}$.