Subgrupos

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

Órdenes y subgrupos

- $o(a^k) = \frac{o(a)}{mcd(o(a),k)}$
- Si $ab = ba$ y $mcd(o(a), o(b)) = 1$ entonces $o(ab) = o(a) * o(b)$
- $|H||K| = |HK||H \cap K|$
- Si $mcd(|H|, |K|) = 1$ entonces $H \cap K = \{e\}$
- $[G : K] = [G : H][H : K]$

Subgrupos normales

- $H \trianglelefteq G \Leftrightarrow gH = Hg \Leftrightarrow g^{-1}Hg = H\ \forall g \in G$
- Si $H \leq G$ y es el único con ese orden, $H \trianglelefteq G$
- Si $H \leq G$ y $[G : H] = 2$ entonces $H \trianglelefteq G$
- Si $H \trianglelefteq G$ entonces $HK \leq G$
- Si $H, K \trianglelefteq G$ entonces $HK \trianglelefteq G$
- Si $H, K \trianglelefteq G$ y $H \cap K = \{e\}$ entonces $hk = kh$

Subgrupos especiales

- Conjugado: $g^{-1}Hg \leq G$. Isomorfo a H.
- $|\{g^{-1}Hg\}| = [G : N_G(H)]$
- Centro: $\mathcal{Z}(G) = \{g \in G : gh = hg\ \forall h \in G\}$
- Centralizador ($S \subseteq G$): $C_G(S) = \{g \in G : gs = sg\ \forall s \in S\}$
- Normalizador: $N_G(H) = \{g \in G : Hg = gH\}$
  → El mayor subgrupo que tiene a H normal.
- Si $H, K \leq G$ son conjugados, sus normalizadores también.
- Si $K \trianglelefteq G$, $H \leq G$ y $K \trianglelefteq H$ entonces $N_{G/K}(H/K) = N_G(H)/K$

Homomorfismos

- Conservan neutros, inversos y subgrupos.
- f^{-1} conserva normalidad. Si sobreyectiva, también f.
- $o(f(a))$ divide a $o(a)$
- Es biyectivo y conserva normalidad {Subgrupos de G que contienen a H}$\longrightarrow${Subgrupos de G/H} tal que $K \longmapsto K/H$

Permutaciones

- $\mathcal{Z}(\mathcal{S}_n) = \{id\}$ si $n \geq 3$
- Si σ ciclo, $o(\sigma) = long(\sigma)$
- $\mathcal{S}_n$ tiene $\binom{n}{k}(k-1)!$ ciclos de longitud k
- Si $\sigma,\ \tau$ ciclos disjuntos, $o(\sigma\tau) = o(\sigma)o(\tau)$
- Si $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_k$ con σ_i ciclos disjuntos, $o(\sigma) = mcm(long(\sigma_1), \ldots, long(\sigma_k))$ y $long(\sigma_1) + \ldots + long(\sigma_k) \leq n$
- Signatura: $s(\sigma) = (-1)^t$ con $t = \#$transposiciones
- $\mathcal{A}_n = ker(s)$ (permutaciones pares)
- $\mathcal{A}_n$ no abeliano si $n \geq 4$
- $\mathcal{A}_n$ simple y es el único subgrupo normal de $\mathcal{S}_n$ si $n \geq 5$

Teoremas del isomorfismo

1. Si f homomorfismo, $G/ker(f) \cong Im(f)$
2. $\frac{G/K}{H/K} \cong G/H$
3. $\frac{H}{H \cap N} \cong \frac{HN}{N}$

Grupo diédrico: $\mathcal{D}_n$

- $o(\rho^k) = \frac{n}{mcd(n,k)}$
- $G \cong \mathcal{D}_n \Longleftrightarrow G =< a, b >$, $o(a) = n$, $o(b) = 2$, $o(ab) = 2$

Acciones

- Homomorfismo $\phi : G \longrightarrow Biy(X)$. También $\phi : G \times X \longrightarrow X$
- $Orb(x) = \{y \in X : \exists g \in G : \tilde{g}(x) = x'\} \subseteq X$
- $Stab(x) = \{g \in G : \tilde{g}(x) = x\} \leq G$
  - $\mathcal{S}_n \longrightarrow Biy(I_n)$
  - Si $H \leq G$, $(h, g) \longmapsto hg$
  - Si $H \leq G$, $(h, g) \longmapsto h^{-1}gh$

Teoremas de Sylow

- Teorema de Cauchy: Si $|G| = n$, y p primo tal que p divide a n, entonces $\exists g \in G : o(g) = p$
- G es p-grupo ($|G| = p$) $\Leftrightarrow \forall g \in G : o(g) = p^m$.
- $H \leq G$ es p-Sylow si $|G| = p^n m$ y $|H| = p^n$

1. Si $|G| = p^n m$ con $mcd(p, m) = 1$, entonces $\exists\ H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_n \leq G$ con $|H_i| = p^i$
2. Si H_1, H_2 son p-Sylow, entonces son conjugados: $\exists g \in G : g^{-1}H_2g = H_1$
3. Si $|G| = p^n m$ y s_p es el número de p-Sylow, s_p divide a m y $s_p \equiv 1 \pmod p$

Grupos abelianos finitos

- Si $\exists N_1, N_2 \trianglelefteq G$ con $N_1 \cap N_2 = \{e\}$ y $N_1N_2 = G$ entonces $G \cong N_1 \times N_2$
  → Si todos los Sylow de G son normales, G es el producto directo de ellos.
- Si G es p-grupo abeliano con un solo subgrupo cíclico de orden p, entonces G es cíclico.
- Si G es p-grupo abeliano y $C \trianglelefteq G$ maximal, entonces $\exists\ D \trianglelefteq G$ tal que $C \cap D = \{e\}$ y $CD = G$
- Caracterización de los p-grupos abelianos: $\exists!\ k_! \geq \ldots \geq k_l : G \cong \mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_l}}$
- n-torsión de G: $G[n] = \{g \in G : g^n = e\} \leq G$ (es el núcleo de $g \longmapsto g^n$; la imagen es G^n)
  → $\mathbb{Z}_{p^k}[p^s] = \langle [p^{k-s}] \rangle = \mathbb{Z}_{p^s}$

Anillos

1. $(A, +)$ es un grupo abeliano.
2. $(A, *)$ es asociativo, [conmutativo y con 1].
3. $(A, +, *)$ es distributivo.

- $0a = a0 = 0$, $(-a)b = a(-b) = -ab$, $A_1 \times A_2$ anillo.
- $\mathcal{U}(A) = \{a \in A : \exists b \in A : ab = ba = 1\}$
- A es cuerpo si $\mathcal{U}(A) = A^*$
- $Div(A) = \{a \in A^* : \exists b \in A^* : ab = 0\}$
- A es DI si $Div(A) = \emptyset$
- $\mathcal{U}(A) \cap Div(A) = \emptyset$

Subanillos e ideales

- B subanillo: $(B, +) \leq (A, +)$ y $b_1b_2 \in B$ para $b_1, b_2 \in B$
  → Si B es subanillo de A conmutativo con 1, B es conmutativo, pero no tiene por qué tener 1.
- I ideal: $(I, +) \leq (A, +)$ y $ai \in I$ para $i \in I,\ a \in A$
  → Si $I = \{0\}$ o $I = A$ entonces I es impropio.
  → A es cuerpo $\Leftrightarrow$ todos sus ideales son impropios.
  → $I + J$, $I \cap J$, $IJ = \{\sum i_k j_k\}$ son ideales.

Ideales especiales

- Ideal generado: $(S) = \{\sum s_i a_i : s_i \in S,\ a_i \in A\}$
- Ideal principal: $iA = (i) = \{ia : a \in A\}$
- Ideal primo: $\forall a, b \in A$ si $ab \in I$ entonces $a \in I$ o $b \in I$
  $\Leftrightarrow$ A/I es DI.

- Ideal maximal: $I \neq A$ y $\forall J : I \subseteq J$ entonces $J = I$ o $J = A$
  $\Leftrightarrow$ A/I es cuerpo.
  $\Rightarrow$ I primo

Homomorfismos de anillos

- f es homomorfismo si conserva $+$, $*$ y el 1.
  $\rightarrow$ Entonces conserva el 0 y $f(\mathcal{U}(A)) \subseteq \mathcal{U}(B)$
- $f^{-1}(J)$ es ideal.
- f sobreyectiva $\Rightarrow$ $f(I)$ es ideal.
- f sobreyectiva $\Leftrightarrow$ $f^{-1}(M)$ es maximal.
- f sobreyectiva $\Leftrightarrow$ $f^{-1}(P)$ es primo.
- K cuerpo $\Rightarrow$ f inyectiva.

Correspondencia: Sea el homomorfismo $\Pi(a) = [a]$.

1. Si $J \subseteq A/I$, entonces $\Pi^{-1}(J)$ es ideal de A y contiene a I.
   Si J es primo o maximal, $\Pi^{-1}(J)$ también.
2. Si $J \subseteq A$ y contiene a I, entonces J/I es ideal de A/I.
   Si J es primo o maximal, J/I también.

Cuerpo de fracciones

- Sea $A \times A^*$ y $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. Entonces $[(a,b)] = \frac{a}{b}$
- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ y $\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}$
- Si A no es DI, no existe $f : A \longrightarrow K$ un homomorfismo inyectivo con K cuerpo.

Divisibilidad y factorización

- a divide b ($a|b$) si $b = ac$
- a, b asociados si $a|b$ y $b|a$
- $a \in A \backslash \mathcal{U}(A)$ reducible si $\exists\ b, c \in A \backslash \mathcal{U}(A)$ tales que $a = bc$
  $\rightarrow$ a irreducible si no es reducible ni unidad.
- $a \in A^*$ primo si $\forall\ b, c \in A$ tales que $a|bc$ entonces $a|b$ o $a|c$
  $\Leftrightarrow$ aA primo.
  $\Rightarrow$ a irreducible.
- $mcd(a_1, \ldots, a_n) = d$
  si $d|a_i$ y $\forall d' \in A$ que cumpla lo anterior, entonces $d'|d$

$\mathbb{Z}$:	Algoritmo de la división	$\Rightarrow$	Bezout	$\Rightarrow$	T$^{\text{a}}$ fundamental de la aritmética
DI:	DE	$\Rightarrow$	DIP	$\Rightarrow$	DFU

Dominio de Factorización Única (DFU)

Si $\forall a \in A^* \backslash \mathcal{U}(A)$ $\exists a_1 \ldots a_n \in A$ irreducibles y únicos salvo asociación tales que $a = a_1 \ldots a_n$

- a irreducible $\Leftrightarrow$ a primo
- Existe el mcd
- Si a irreducible $\Leftrightarrow$ a primo y existe descomposición en irreducibles, entonces A es DFU.

Dominio de Ideales Principales (DIP)

Si $\forall I \subseteq A$ ideal, I es principal ($I = iA = (i)$)

- a irreducible $\Leftrightarrow$ a primo $\Leftrightarrow$ aA maximal

---

Dominio Euclídeo (DE)

Si $\exists\ \varphi : A^* \longrightarrow \mathbb{N}^0$ tal que

1. $\forall a, b \in A^*$ $\varphi(a) \leq \varphi(ab)$
2. $\forall a, b \in A$ con $b \neq 0$ $\exists q, r \in A$ con $r = 0$ o $\varphi(r) < \varphi(b)$ tal que $a = bq + r$

- $\varphi(1) \leq \varphi(1 * a) = \varphi(a) \implies \varphi(1) = min\{\varphi(a)\}$
- $\mathcal{U}(A) = \{a \in A^* : \varphi(a) = \varphi(1)\}$

Ecuaciones diofánticas

- $ax + ny = b \Leftrightarrow ax \equiv b \pmod{n}$
- Tiene solución $\Leftrightarrow$ $mcd(a,n)|b$
- Una solución es $x_0 = u_0 c$, con $b = c * mcd(a,n)$ y Bezout: $mcd(a,n) = au_0 + nv_0$
- La solución general es $x = x_0 + nt$, $y = y_0 - at$

Enteros de Gauss

- Si p primo impar, p reducible en $\mathbb{Z}[i]$ $\Leftrightarrow$ $p \equiv 1 \pmod{4}$ $\Leftrightarrow$ $\exists x \in \mathbb{Z}$ tal que $-1 \equiv x^2 \pmod{p}$
- $x \in \mathbb{Z}[i]$ es irreducible $\Leftrightarrow$ $||x||$ es primo o [$x = p, -p, ip, -ip$ y $p \equiv 3 \pmod{4}$ con p primo]

Polinomios

- $deg(PQ) \leq deg(P) + deg(Q)$
- $deg(P+Q) \leq max\{deg(P), deg(Q)\}$
- Si $\ell(P)\ell(Q) \neq 0$, $deg(PQ) = deg(P) + deg(Q)$

Anillo de polinomios

- A DI $\Rightarrow$ $\mathcal{U}(A[t]) = \mathcal{U}(A)$
- A DI $\Leftrightarrow$ $A[t]$ DI
- Sean $P, Q \in A[t]$ con $\ell(Q) \in \mathcal{U}(A) \Rightarrow$
  $\exists!\ C, R \in A[t] : P = CQ + R$ con $R = 0$ o $deg(R) < deg(Q)$
- Ruffini: $P(t) = C(t)(t-a) + P(a)$
- A cuerpo $\Leftrightarrow$ $A[t]$ es DE $\Leftrightarrow$ $A[t]$ es DIP

Raíces

- $ev_d(P) = P(d)$ es un homomorfismo.
- a es raíz si $P(a) = 0$
  $\Leftrightarrow$ $t - a|P$
- $mult_a(P) = max\{k : (t-a)^k | P\}$
- Si A DI, $mult_{a_1}(P) + \ldots + mult_{a_n}(P) \leq deg(P)$
- Si K cuerpo finito, $|K| = p^r$
- a es raíz simple si es raíz y $mult_a(P) = 1$
  $\Leftrightarrow$ $P'(a) \neq 0$

Teorema de Gauss

- Contenido de P: $\mathcal{C}(P) = mcd(a_n \ldots a_1)$
  $\rightarrow$ P primitivo si $\mathcal{C}(P) = 1$
  $\rightarrow$ Si $P \in \mathbb{Z}[t]$ con $deg(P) \geq 1$ irreducible $\Rightarrow$ es primitivo
- $\mathcal{C}(PQ) = \pm \mathcal{C}(P)\mathcal{C}(Q)$
- Si $P(t) \in \mathbb{Z}[t]$ es primitivo con $deg(P) \geq 1$ entonces
  P irreducible en $\mathbb{Z}[t]$ $\Leftrightarrow$ P irreducible en $\mathbb{Q}[t]$
- Teorema de Gauss: A DFU $\implies$ $A[t]$ DFU

Criterios de irreducibilidad

- Si K cuerpo, $P(t) \in K[t]$ y $2 \leq deg(P) \leq 3$ entonces
  P irreducible $\Leftrightarrow$ no tiene raíces.
- Si A DI, $P(t) \in A[t]$ con $2 \leq deg(P) \leq 3$ y P primitivo,
  P irreducible $\Leftrightarrow$ no tiene raíces.
- Si A DI, $P(t) \in A[t]$ y $a \in A$,
  $P(t)$ irreducible $\Leftrightarrow$ $P(t+a)$ irreducible.
- Si A DFU, $P(t) \in A[t]$ y $deg(P) \geq 1$, si p primo tal que $p \nmid a_n$, $p^2 \nmid a_0$ y $p \nmid a_i$ $\forall i \in [0, n)$, entonces P irreducible.
- Si p primo tal que $p \nmid a_n$, y sea $\overline{P} = \sum \overline{a_i}\ t^i$ con $\overline{a_i} \in \mathbb{Z}_p$, $\overline{P}(t)$ irreducible en $\mathbb{Z}_p \Rightarrow P(t)$ irreducible en $\mathbb{Z}$.

Celia Rubio Madrigal