Hidden Subgroup Minicourse - Groups

Gábor Ivanyos
MTA SZTAKI & TU/e

CWI Amsterdam, October 30 - November 3, 2006

Contents

Prerequisites

- def. of groups, homomorphisms, isomorphisms, image, kernel
- subgroups, cosets, Lagrange's theorem
- cyclic groups, orders of elements $\sim$ orders of cyclic subgroups
- exponent of G ($=$ lcm of orders of elements)
- The Euler-Fermat theorem

Prereqs 2.

- normal subgroups, factor groups,
- homomorphism theorem: $\phi(G) \cong G/(\ker \phi)$
- direct products, the fundamental theorem of finite abelian groups.
- permutations, signs of permutations, symmetric and alternating groups.
- Isomorphism theorems
    1. $N, K \lhd G, K \leq N \Rightarrow$G/N$\cong (G/K)/(N/K)$.
    2. $N \lhd G, H \leq G \Rightarrow HN \leq G$ and $HN/N \cong H/(H \cap N)$.
- Def. of simple groups, composition series

Basic exercises, examples

- Which is the smallest noncommutative group (by size)?
  $S_3 = D_3$
- Next?
  D_4: automorphisms of the square: rotations and reflections.
  $Q : \{\pm i, \pm j, \pm k\}$ from the quaternion algebra.
  $\sim \sigma_x, \sigma_y, \sigma_z$???
- $|G : H| = 2 \Rightarrow H \lhd G$.
  $gH = Hg$: OK, if $g \in H$. Otherwise $gH = G \setminus H = Hg$.
- $|G : H|$ prime $\not\Rightarrow H \lhd G$.
  In $S_3 = D_3$, the transposition/reflection

The dihedral group D_n

- D_n: automorphisms of the n-gon.:
  - rotations (preserve orientation of the plane)
  - (axial) reflections (reverse orientation)
- $\alpha = 2\pi/n$, basic generators for D_n:
  - r = rotation by α. $r = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & cos(\alpha) \end{pmatrix}$
  - t = reflection w.r.t. the x-axis. $t = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- all elements:
  - rotations: $r^k = \begin{pmatrix} \cos(k\alpha) & -\sin(k\alpha) \\ \sin(k\alpha) & \cos(k\alpha) \end{pmatrix}$
  - reflections: $r^k t = \begin{pmatrix} \cos(k\alpha) & \sin(k\alpha) \\ \sin(k\alpha) & -\cos(k\alpha) \end{pmatrix}$

Contents

Permutation representations - definitions

- Ω: a set. The definitions and most of the basic properties generalize to infinite Ω.
- $S_\Omega = \{\text{permutations of } \Omega\} = \{\text{bijections } \Omega \leftrightarrow \Omega\}$
    - for convenience, mult. in S_Ω: $fg = g \circ f$, thus $fg(x) = f(g(x))$. (First we execute the perm. on the right.)
    - Omit "()" from $f(x)$ (or replace with " $\cdot$") : $fx = f(x)$
    - Then $(fg)x = f(gx)$.
- $S_n = S_{\{1,\ldots,n\}}$.
- A permutation representation of G (on Ω): a homomorphism $\phi : G \rightarrow S_\Omega$
- A G-action on Ω: map $G \times \Omega$ $(g, \omega) \mapsto g\omega$, with associativity: $(g_1 g_2)\omega = g_1(g_2(\omega))$.

Permutation groups - defs 2.

- Perm reps $\leftrightarrow$ actions.
  - $\rightarrow$: $g\omega = \phi(g)\omega$
  - $\leftarrow$: $\phi(g) : g \mapsto g\omega$.
- Equivalent perm reps: $\phi_1 : G \rightarrow \Omega_1$, $\phi_2 : G \rightarrow \Omega_2$, perm reps. ϕ_1 and ϕ_2 are equivalent iff $\exists$ bijection $\mu : \Omega_1 \rightarrow \Omega_2$ such that for every $g \in G$,

$$\mu(\phi_1(g)\omega) = \phi_2(g)(\mu\omega)$$

Equivalently,

$$\phi_2(g) = \mu^{-1} \circ \phi_1(g) \circ \mu.$$

That is, $\phi_2(g)$ is $\phi_1(g)$, *conjugated by* μ.

Orbits, stabilizers, cosets

- Orbit of ω: $G\omega = \{g\omega | g \in G\}$
- collection of the orbits is a partition of Ω
- Stabilizer of ω: $G_\omega = \{g \in G | g\omega = \omega\}$
- (action of) G is transitive, if there is just one orbit. Equivalently, for every pair $\omega_1, \omega_2 \in \Omega$, there is $g \in G$ s.t. $\omega_2 = g\omega_1$.
- $|G\omega| = |G : G_\omega|$.
  - $g_1\omega = g_2\omega \Leftrightarrow g_2^{-1}g_1 \in G_\omega \Leftrightarrow g_1G_\omega = g_2G_\omega$
- By the proof above, a transitive action on Ω is equivalent with the action of G on the left cosets of G_ω (for an arbitrary $\omega \in \Omega$).

Orbits, stabilizers, cosets 2.

- A transitive action on Ω is equivalent with the action of G on the left cosets of G_ω.
- The converse (Cayley's theorem): $H \leq G$ G acts on left cosets of H by multiplication transitively. Stabilizer of H is H.
- What is the stabilizer of xH?
  - $gxH = xH \Leftrightarrow x^{-1}gxH = H \Leftrightarrow x^{-1}gx \in H \Leftrightarrow g \in xHx^{-1}$.
- Conjugation by x: $g \mapsto g^x = xgx^{-1}$ is an automorphism of G ($xg_1x^{-1}xg_2x^{-1} = xg_1g_2x^{-1}$, etc...) Automorphisms of this form are the inner automorphisms of G.

Permutation groups - exercises

- D_n permutes the vertices's and the edges of the n-gon. Are these actions equivalent?
- What is the kernel of the perm rep on the left cosets of a subgroup H?
- (Burnside's Lemma.) Let G, Ω finite. Prove that

$$\frac{1}{|G|}\sum_{g\in G}|\{\omega\in\Omega|g\omega=\omega\}| = \text{number of orbits of } G.$$

Average number of fixed points = number of orbits.

Contents

conjugation. conjugacy classes

- Conjugation by x: $g \mapsto g^x = xgx^{-1}$ is an automorphism of G.
- G act on itself by conjugation.
- Orbits: conjugacy classes of G.
- Stabilizer of g $C_G(g)$, the centralizer of g
  - $g^x = g \Leftrightarrow xgx^{-1} = g \Leftrightarrow xg = gx$
- Fixed points of x: $C_G(x)$.
- Size of the conjugacy class of g is $|G : C_G(g))|$

conjugation. conjugacy classes 2.

- $x \mapsto \cdot^x \in Aut(G) \subseteq S_G$ a permutation representation. The kernel is the center of G:

$$Z(G) = \{x \in G | xg = gx \; \forall g \in G\}.$$

- Example: conjugacy classes of D_4, Q?
- Example: conjugacy classes of D_n?
- Example: conjugacy classes of S_n?

Conjugation - applications

- A finite group G is a p-group if $|G|$ is a power of the prime p.
- If G is a finite p-group then $Z(G) \neq \{1_G\}$.
  - Each conj. class is of size $|G|$/something, a power of p.
  - The one-element conjugacy classes are form Z_G.
  - $\{1_G\}$ is such.
  - There must be others.
- Exercise. Every group of order p^2 (p prime) is commutative.
- Exercise (Cauchy's theorem). If $|G|$ is divisible by the prime p then there is an element of G of order p.

Contents

Commutators

- commutator: $[x, y] = x^{-1}y^{-1}xy$.
- $[x, y] = (yx)^{-1}xy$, also $[x, y] = x^{-1}x^{y^{-1}}$.
- $xy = yx \leftrightarrow [x, y] = 1$.
- commutator subgroup $G' = \langle [x, y] | x, y \in G \rangle$
- $\phi \in Aut(G) \Rightarrow [\phi(x), \phi(y)] = \phi([x, y])$
  in particular $[x^g, y^g] = [x, y]^g$,
- So $G' \lhd G$, more generally: if $N \lhd G$ then $N' \lhd G$.

The commutator subgroup

- commutator subgroup $G' = \langle [x,y] | x, y \in G \rangle$
- $\phi \in Aut(G) \Rightarrow [\phi(x), \phi(y)] = \phi([x,y])$
- Characteristic subgroup: $K \leq G$ is characteristic in G, if $\phi(K) = K$ for every $\phi \in Aut(G)$.
- characteristic $\Rightarrow$ normal.
- characteristic $\not\Leftarrow$ normal.
- Examples $G', Z(G)$

Commutators of subgroups

- $K \leq N \lhd G$, K characteristic in N. Then $K \lhd G$.
- $K \leq N \leq G$, K characteristic in N, N characteristic in G. Then K characteristic in G.
- So $G', G'' = (G')', \ldots$ are characteristic in G.
- if $N \lhd G$ then $N' \lhd G$.
- $[H, K] = \langle [x, y] | x \in H, y \in K \rangle$
- $N \lhd G \Leftrightarrow [N, G] \leq N$.
  - $[x, y^{-1}] = x^{-1}yx^{-1}y^{-1} = x(x^y)^{-1}$, so for $x \in N$: $x^y \in N \Leftrightarrow [x, y^{-1}] \in N$.

Commutators and abelian factors

- G' is the smallest $N \triangleleft G$ such that G/N abelian:

  $N \triangleleft G$: G/N abelian $\Leftrightarrow N \geq G'$.

  $\Rightarrow$ $x, y \in G$, $\phi : G \to G/N$ the natural map.
  $\phi([x, y]) = [\phi(x), \phi(y)] = 1_{G/N}$, i.e. $[x, y] \in N$.

  $\Leftarrow$ $[x, y] \in N \Rightarrow [xN, yN] \subseteq N$:
  $[xn, y] = n^{-1}x^{-1}y^{-1}xny \in Nx^{-1}y^{-1}xNy = [x, y]N$.

Solvable groups

- Derived series of G: $G^{(0)} = G$,
  $G^{(1)} = G' = [G, G] = G^{(i+1)} = G^{(i)'} = [G^{(i)}, G^{(i)}]$,
  descending chain of characteristic subgroups.
- Derived length of G: smallest ℓ such that $G^{(\ell+1)} = G^{(\ell)}$.
- G is solvable if $G^{(\ell)} = \{1\}$ for some ℓ.
- Exercise: G finite group is solvable if and only if there is a chain $1 = G_0 \leq G_1 \leq \ldots \leq G_r = G$ such that for every $1 \leq i \leq r$, $G_{i-1} \triangleleft G_i$ and G/G_{i-1} is a cyclic group of prime order.

Solvable groups 2.

- Exercise: $D_4' = ?$, $Q' = ?$
- Exercise $D_n' = ?$
- Exercise: Every finite p-group is solvable.
- Exercise: S_4 is solvable.
- Remark: the non-solvable (simple) group of smallest size is A_5.

Contents

Inner view of direct products

Proposition. If $N, H \lhd G$, $\langle N \cup H \rangle = G$, $N \cap H = 1$, then $G \cong N \times H$.

- $G = \langle N \cup H \rangle = NH = \{xy | x \in N, y \in H\}$
- $[N, H] \leq N$, $[N, H] \leq H$, so $N, H \leq N \cap H = \{1\}$.
- $(x_1 y_2)(x_2 y_2) = x_1 x_2 y_1 y_2$, (etc. with 1 and inverse)
- so $(x, y) \mapsto xy$ is an isomorphism $N \times H \to G$.

Semidirect products - inner view

$N \lhd G$, $H \leq G$, $\langle N \cup H \rangle = G$, $N \cap H = 1$.

- $G = \langle N \cup H \rangle = NH = \{xy | x \in N, y \in H\}$
- For $y \in H$, $N^y = N$, so

$$\sigma_y : x \mapsto x^y \in Aut(N)$$

- $(x_1 y_1)(x_2 y_2) = x_1 y_1 x_2 y_1^{-1} y_1 y_2 = x_1(\sigma_{y_1}(x_2)) y_1 y_2$
- $\sigma : y \mapsto \sigma_x$ is a homomorphism from H into $Aut(N)$.
- σ needs to be neither injective nor subjective

Semidirect products - outer view

N, H, $\sigma : y \mapsto \sigma_y$ homomorphism $H \to Aut(N)$.

- $N \rtimes H = \{(x,y) | x \in N, y \in H\}$
- $(x_1, y_1)(x_2, y_2) = (x_1\sigma_{y_1}(x_2), y_1y_2)$
- $1_{N \rtimes H} = (1, 1)$
- $(x, y)^{-1} = (((x^{y^{-1}})^{-1}, y^{-1})$
- $G = N \rtimes H$ is a group of order $|N||H|$
- $\tilde{N} = \{(x, 1)|x \in N\}$, $\tilde{H} = (1, y)|y \in H\}$
- $N \cong \tilde{N} \lhd G$, $H \cong \tilde{H} \leq G$,
- $\tilde{N} \cap \tilde{H} = \{1\}$, $G = \tilde{N}\tilde{H}$.
- $x \mapsto x^y$ gives σ_y on $\tilde{N}$.

Semidirect products - examples

- Example: dihedral group D_n.
  - $N = \{\text{rotations}\} \cong \mathbb{Z}_n$.
  - $H = \{1, t\} \cong \mathbb{Z}_2$, where t is the reflection w.r.t a fixed axis.
  - $y^{\sigma_t} = y^{-1}$.
- Exercise: The quaternion group Q is not a nontrivial semidirect product
  - Hint: list the subgroups of Q.