A Glossary of Group Theory

Phil Hazelden

2012-02-04 Sat

1 Notation

$[g,h]$ The commutator, $g^{-1}h^{-1}gh$.

$[G,G]$ The commutator subgroup, $\langle [g,h] \mid g,h \in G \rangle$.

α^g When $G \ni g$ acts on $\Omega \ni \alpha$, the image of α under g.

α^G When G acts on $\Omega \ni \alpha$, the orbit $\{\alpha^g : g \in G\}$.

$\mathrm{Aut}(G)$ The automorphism group of G.

C_g The conjugation map $x \mapsto g^{-1}xg$.

$\mathrm{C}_G(x)$ The centraliser of x in G; $\{g \in G : gx = xg\}$. This is G_x under the conjugation action.

$\mathrm{C}_G(H)$ The centraliser of H in G; $\{g \in G : h \in H \Rightarrow gh = hg\}$. This is not an orbit or stabiliser; see also $\mathrm{N}_G(H)$.

$\mathrm{Cl}_G(x)$ The conjugacy class of x in G; $\{g^{-1}xg : g \in G\}$. This is x^G under the conjugation action.

G^Ω When G acts on Ω, $G^\Omega \leq \mathrm{Sym}(\Omega)$ contains permutations of the form $\alpha \mapsto \alpha^g$, for each $g \in G$.

$G^{(i)}$ $G^{(0)} = G$, and $G^{(i)} = \left[G^{(i-1)}, G^{(i-1)}\right]$.

G_α The stabilizer of α in G, $\mathrm{Stab}_G(\alpha) = \{g \in G : \alpha^g = \alpha\}$.

$G_{\alpha,\beta}$ The stabilizer of α and β, $G_\alpha \cap G_\beta$.

G_Σ The setwise stabilizer of Σ, $\{g \in G : \alpha \in \Sigma \Rightarrow \alpha^g \in \Sigma\}$.

$G_{(\Sigma)}$ The pointwise stibilizer of Σ, $\bigcap_{\alpha \in \Sigma} G_\alpha$.

$\mathrm{Inn}(G)$ The inner automorphism group of G, $\{\mathrm{C}_g : g \in G\}$. $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

$\mathrm{N}_G(H)$ The normalizer of H in G, $\{g^{-1}Hg : g \in G\}$. This is G_H under the conjugation action.

$n^{\underline{k}}$ n to the k falling, $n(n-1)\ldots(n-k+1)$.

$\mathrm{Syl}_p(G)$ The set of Sylow p-subgroups of G.

$\mathrm{Z}(G)$ The centre of G, $\{g \in G : x \in G \Rightarrow gx = xg\}$. The kernel of the conjugation action.

2 Definitions

Block A block for G^Ω is a subset $B \subsetneq \Omega$ with $|B| > 1$ such that for every $g \in G$, either $B^g = B$ or $B^g \cap B = \varnothing$.

Characteristic subgroup $N \leq G$ is a characteristic subgroup (written $N \operatorname{char} G$) if every automorphism of G preserves N.

Conjugation action G acts on itself by $x^g = g^{-1}xg$. Also, G acts on $\{H : H \leq G\}$ by $H^g = g^{-1}Hg$.

Coset action if $H \leq G$, then G acts on $\Omega = \{Hx : x \in G\}$ by $(Hx)^g = Hxg$. Transitive, not necessarily faithful. If $H = 1$, this is the right-regular action.

Cycle type The cycle type of a permutation group is the lengths of the cycles in its cyclic decomposition.

Direct product if $G_1, \dots, G_n$ are groups then $\prod_{i=1}^n G_i = G_1 \times \dots \times G_n$ is the group $\{(g_1, \dots, g_n) : g_i \in G_i\}$ with obvious multiplication.

Faithful A group action is faithful if no two orbits are identical; for every $g \neq e$ there is α such that $\alpha^g \neq \alpha$.

Maximal $H \leq G$ is maximal if $H < G$ and there is no K with $H < K < G$.

n-transitive G^Ω is n-transitive if $|\Omega| \geq n$ and for any n-tuples α_i, β_i, there is $g : \alpha_i^g = \beta_i$. (Here the α_i are distinct and the β_i are distinct, but may have $\alpha_i = \beta_j$.)

Nilpotent A finite group is nilpotent if it is the direct product of its Sylow subgroups.

p-group For prime p, a finite group G is a p-group if $|G| = p^n$.

Perfect A group is perfect if $G = [G, G]$.

Primitive G^Ω is primitive if it is transitive and has no blocks; imprimitive if it is transitive and has blocks.

Regular normal subgroup when G^Ω is specified, a regular normal subgroup is $N \trianglelefteq G$ such that N^Ω is regular.

Right-regular action G acts on itself by $x^g = xg$. Transitive and faithful.

Semidirect product if $H \leq G$, $K \trianglelefteq G$, $HK = G$ and $H \cap K = 1$, then $G = H \ltimes K = K \rtimes H$. If φ is an action of H on K, then $H \ltimes_\varphi K = K \rtimes_\varphi H$ is the group $\{(h, k) : h \in H, k \in K\}$ with multiplication $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1^{h_2} k_2)$. If φ is the conjugation action $k^h = h^{-1}kh$, this just gives us G, but we can use this to define products of any two groups.

Series A sequence $G = G_0 \geq G_1 \geq \dots \geq G_n = 1$. May be **normal** if each $G_i \trianglelefteq G$; or **subnormal** if each $G_i \trianglelefteq G_{i-1}$; or a **composition series** if it is subnormal and each factor group G_i/G_{i+1} is simple. The **derived series** has $G_i = G^{(i)} = \left[G^{(i-1)}, G^{(i-1)}\right]$, and need not terminate at 1.

Simple A simple group has no normal subgroups except itself and 1. (1 does not count as simple, analogously to primes.)

Soluble G is soluble if it has a finite subnormal series with each factor group abelian.

Sylow p-subgroup $H \leq G$ is a Sylow p-subgroup if $|H| = p^n$ and $|G| = p^n t$, where $p \nmid t$.

Transitive G^Ω is transitive if every orbit contains all of Ω; for every pair α, β there is g such that $\alpha^g = \beta$. (This is almost 1-transitive, except that $G^\varnothing$ is considered transitive.)

3 Theorems

3.1 Miscellany

- **First isomorphism theorem** if $\varphi : G \to H$ is a homomorphism, then $K = \ker(\varphi) \trianglelefteq G$ and the map $Kg \mapsto \varphi(g)$ is an isomorphism $G/K \to \operatorname{im}(\varphi)$.
- **Second isomorphism theorem** if $H \leq G$ and $K \trianglelefteq G$ then $\frac{H}{H \cap K} \approx \frac{HK}{K}$.
- **Third isomorphism theorem** if $N \trianglelefteq K \trianglelefteq G$ and further $N \trianglelefteq G$, then $\frac{K}{N} \trianglelefteq \frac{G}{N}$ and $\frac{G/N}{K/N} \cong G/K$.
- If $N \trianglelefteq G$ then subgroups of G/N are of the form H/N, where $N \leq H \leq G$.
- **Orbit-stabilizer theorem** if G is finite, then $|G| = |\alpha^G||G_\alpha|$.
- If G^Ω is k-transitive and $|\Omega| = n$, then $|G| = n^{\underline{k}}|G_{\alpha_1,\dots,\alpha_k}|$ for any k-tuple of distinct elements.
- Any transitive action of G on a set Ω is equivalent to a coset action of G on $\{(G_\alpha)g : g \in G\}$.
- Two permutations on a set are conjugate iff they have the same cycle type.
- If $N \trianglelefteq G$ then N is a union of conjugacy classes of G (i.e. $x \in N \Rightarrow \mathrm{Cl}_G(x) \subseteq N$).
- Let P be a p-group and $N \trianglelefteq P$ nontrivial. Then $N \cap \mathrm{Z}(P) \neq 1$. In particular, p-groups have nontrivial centres.
- Let $H, K \leq G$. If either $H \trianglelefteq G$ or $K \trianglelefteq G$, then $HK \leq G$. If both $H, K \trianglelefteq G$, then $HK \trianglelefteq G$.
- If $H, K \trianglelefteq G$, $HK = G$ and $H \cap K = 1$ then $G = H \times G$.
- If $K_1, \dots K_n \trianglelefteq G$, $G = K_1 \dots K_n$ and each $K_i \cap (K_1 \dots K_{i-1} K_{i+1} \dots K_n) = 1$, then $G = \prod K_i$.

3.2 Sylow's theorem

- If $p^\beta \mid |G|$, then $|\{H \leq G : |H| = p^\beta\}| \equiv 1 \bmod p$.
- If $P \in \mathrm{Syl}_p(G)$ and Q is any p-subgroup of G, then $Q \subseteq g^{-1}Pg$ for some $g \in G$.
- **Sylow's theorem** follows from the above. Let G be a group with $p \mid |G|$.

  Existence $\mathrm{Syl}_p(G)$ is nonempty.

  Containment any p-subgroup is contained in some Sylow p-subgroup.

  Conjugacy if $P, Q \in \mathrm{Syl}_p(G)$ then $\exists g \in G$ with $g^{-1}Pg = Q$.

  Number $|\mathrm{Syl}_p(G)| \equiv 1 \bmod p$.

- **Corollaries** $p \mid |G|$, $k = |\mathrm{Syl}_p(G)|$, $P \in \mathrm{Syl}_p(G)$:
  - G has an element of order p.
  - $k = |G|/|\mathrm{N}_G(P)|$. In particular, $k \mid |G|/|P|$.
  - $k = 1$ iff $P \trianglelefteq G$.
  - If $\mathrm{N}_G(P) \leq M \leq G$, then $\mathrm{N}_G(M) = M$.
  - If $N \trianglelefteq G$ and $Q \in \mathrm{Syl}_p(N)$, then $G = \mathrm{N}_G(P)N$.

3.3 Nilpotent and soluble groups

- **Nilpotent groups** TFAE:
  - $\forall p \mid |G| : |\mathrm{Syl}_p(G)| = 1$.
  - $\forall p \mid |G| : P \in \mathrm{Syl}_p(G) \Rightarrow P \trianglelefteq G$.
  - $G = \prod\{P : P \in \mathrm{Syl}_p(G) \text{ for some } p\}$.
  - $H < G \Rightarrow H < \mathrm{N}_G(H)$.
  - All maximal subgroups of G are normal in G.
- If $G \neq 1$ is nilpotent, then
  - $Z(G) \neq 1$.
  - $H \leq G \Rightarrow H$ is nilpotent.
  - $N \trianglelefteq G \Rightarrow G/N$ is nilpotent.
- On $[G, G]$:
  - $[G, G] \leq G$.
  - $G/[G, G]$ is abelian.
  - If $N \trianglelefteq G$ and G/N abelian then $[G, G] \leq N$.
- **Characteristic subgroups**
  - $N \operatorname{char} G \Rightarrow N \trianglelefteq G$.

    - $N \operatorname{char} K \trianglelefteq G \Rightarrow N \trianglelefteq G$.
    - $N \operatorname{char} K \operatorname{char} G \Rightarrow N \operatorname{char} G$.
    - $[G, G] \operatorname{char} G$.
    - $\mathrm{Z}(G) \operatorname{char} G$.
    - $P \in \mathrm{Syl}_p(G), P \trianglelefteq G \Rightarrow P \operatorname{char} G$.

- **Soluble groups** TFAE:
    - $G^{(n)} = 1$ for some n.
    - G has a subnormal series with abelian factor groups.
    - G has a normal series with abelian factor groups.

- If $N \trianglelefteq G$, then $\left(\frac{G}{N}\right)^{(k)} = \frac{G^{(k)}N}{N}$.

- **Proving a group is soluble**
    - If G is soluble and $H \leq G$ then H is soluble.
    - If G is soluble and $N \trianglelefteq G$ then G/N is soluble.
    - If N and G/N are soluble then G is soluble.
    - If G is nilpotent, it is soluble.

- Every finite group has a composition series, which is structurally unique: if (A_i) and (B_i) are two composition series, then after permutation, the factors $A_i/A_{i+1} \cong B_i/B_{i+1}$.

- A group is soluble iff its composition factors are all cyclic groups of prime order.

3.4 Permutation groups

- If B is a block, then every B^g is a block.

- If G^Ω is transitive and B is a block, then $|B| \mid |\Omega|$.

- If G^Ω is 2-transitive, it is primitive.

- If G^Ω and H^Ω are transitive and $G_\alpha \leq H \leq G$, then $H = G$.

- Let G^Ω be transitive, $|\Omega| > 1$. Then G^Ω is primitive iff every G_α is a maximal subgroup of G.

- Let G^Ω be transitive, $N \trianglelefteq G$ and $\alpha \in \Omega$. One of the following holds:
    - $\alpha^N = \{\alpha\}$ and $N^\Omega = 1$
    - $\alpha^N = \Omega$ and N^Ω is transitive
    - α^N is a block of G^Ω.

- For $n \geq 5$, A_n has no regular normal subgroup (under the permutation action).

- For $n \geq 5$, A_n is simple and is the only nontrivial normal subgroup of S_n.

3.5 Matrix groups

Choose a field K and $n \in \mathbb{N}^+$. Let Ω be the set of 1-subspaces of K^n, $\Omega = \{\langle v\rangle : 0 \neq v \in K^n\}$. We define four matrix groups:

$\mathrm{GL}(n, K)$: invertible $n \times n$ matrices over K, acting on Ω by $\langle v\rangle^g = \langle vg\rangle$, the projective action.

$\mathrm{SL}(n, K)$ $= \{g \in \mathrm{GL}(n, K) : \det g = 1\}$.

$\mathrm{PGL}(n, K)$ $= \frac{\mathrm{GL}(n,K)}{\mathrm{Z}(\mathrm{GL}(n,K))} \cong \mathrm{GL}(n, K)^\Omega$.

$\mathrm{PSL}(n, K)$ $= \mathrm{SL}(n, K)^\Omega$.

When K is finite of order q (which is necessarily a prime power), we also denote these groups by $\mathrm{GL}(n, q)$, etc.

- $\mathrm{GL}(n, K)^\Omega$ is 2-transitive.
- $\ker(\mathrm{GL}(n, K)^\Omega) = \mathrm{Z}(\mathrm{GL}(n, K)) = \{\lambda I_n : \lambda \in K^*\}$
- $|\mathrm{GL}(n, q)| = \prod_{i=0}^{n}(q^n - q^i)$; $|\mathrm{SL}(n, q)| = |\mathrm{PGL}(n, q)| = \frac{|\mathrm{GL}(n,q)|}{q-1}$; $|\mathrm{PGL}(n, q)| = \frac{|\mathrm{SL}(n,q)|}{\gcd(n,q)}$
- $\mathrm{PSL}(n, K)$ is simple, except for $\mathrm{PSL}(2, 2)$ and $\mathrm{PSL}(2, 3)$. Proof involves:
  - $\mathrm{SL}(n, K)$ is 2-transitive on Ω.
  - $\mathrm{SL}(n, K)$ is generated by transvections. These are matrices conjugate in $\mathrm{GL}(n, K)$ to the matrix T with 1s on the diagonal and in the $(2, 1)$ position and 0s everywhere else. In fact any matrix with 1s on the diagonal and a single other nonzero element is a transvection; and if $n = 1$, we consider (1) to be a tranvection.
  - $\mathrm{SL}(n, K)$ is perfect, except $(2, 2)$ and $(2, 3)$.
  - Lemma: Let G be perfect, G^Ω primitive. Suppose for some $\alpha \in \Omega$ there is $M \trianglelefteq G_\alpha$ such that $G = \langle g^{-1}Mg : g \in G\rangle$. Then G^Ω is simple.
  - Choose α to be the first standard basis vector, and M to be matrices with 1s on the diagonal, arbitrary elements in the first column (except $(1, 1)$), and 0s everywhere else. Then the lemma applies.

3.6 The transfer homomorphism

Let $H \leq G$, $[G : H] = r$, and $\Omega = \{Hg_1, \ldots, Hg_r\}$ where $g_1 = 1$. G acts on Ω by right multiplication.

For $1 \leq i \leq r$ and $g \in G$, let i^g be such that $(Hg_i)g = Hg_{i^g}$. Then we can define r functions (not homomorphisms) $h_i : G \to H$ satisfying $g_i g = h_i(g)g_{i^g}$.

We define the transfer homomorphism $T : G \to \frac{H}{[H,H]}$ by $T(g) = [H, H] \prod_{i=1}^{r} h_i(g)$.

- T is a homomorphism.
- Let the lengths of the cycles of g^Ω be $r_1, \ldots, r_s$. Let $i_j = \sum_{m=0}^{j-1} r_m$. Then each $g_{i_j} g^{r_j} g_{i_j}^{-1} \in H$, and $T(g) = [H, H] \prod_{j=1}^{s} g_{i_j} g^{r_j} g_{i_j}^{-1}$.

- If G is finite abelian and $r \in \mathbb{Z}$ with $\gcd(r, |G|) = 1$, then the map $\varphi : G \to G : g \mapsto g^r$ is an automorphism of G.
- If $P \in \mathrm{Syl}_p(G)$ is abelian and $g, h \in P$ are conjugate in G, then they are conjugate in $\mathrm{N}_G(P)$.
- **Burnside's transfer theorem** G a finite group, $P \in \mathrm{Syl}_p(G)$, and $P \leq \mathrm{Z}(\mathrm{N}_G(P))$. Then G has a normal subgroup N with $P \cap N = 1$ and $PN = G$. In particular, G can only be simple if $G = P$.
- Corollary: no group of twice-odd order is simple (except C_2).

3.7 Classification of groups

- If $|G| = p$ then $G \cong C_p$.
- If $|G| = 2p$ where p is an odd prime, then $G \cong C_{2p}$ or $G \cong D_{2p}$.
- If $|G| = p^2$ then $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.
- If $|G| = p^n$ then $Z(G) \neq 1$ so G is not simple.
- Let G be finite simple nonabelian.
  - If G acts on Ω with $G^\Omega \neq 1$, then G^Ω is faithful, $G \leq \mathrm{Alt}(\Omega)$ and $|\Omega| \geq 5$.
  - If $H < G$, let $n = [G : H] > 1$. Then $G \leq A_n$ and $n \geq 5$.
  - If $\mathrm{Syl}_p(G) = n > 1$ for some p, then $G \leq A_n$ and $n \geq 5$.
- All finite simple groups of orders 60, 168, 360 are isomorphic. (360 nonexaminable.)
- The only finite simple nonabelian groups of order ≤ 500 are those of order 60, 168, 360.
  - Most orders can be done simply by above theorems. Orders 264, 288, 336, 420, 432 and 480 are harder.