Algebra Notes

D. Zack Garza

January 6, 2020

Contents

1 Group Theory

Definition (Centralizer):

$$C_G(H) = \left\{ g \in G \;\middle|\; ghg^{-1} = h \;\forall h \in H \right\}$$

Definition (Normalizer):

$$N_G(H) = \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\}$$

Lemma: $C_G(H) \leq N_G(H)$

Lemma: The size of the conjugacy class of H is the index of the centralizer, i.e.

$$\left| \left\{ gHg^{-1} \;\middle|\; g \in G \right\} \right| = [G : C_G(H)].$$

Lemma ("The Fundamental Theorem of Cosets"):

$$aH = bH \iff a^{-1}b \in H \text{ or } aH \bigcap bH = \emptyset$$

Definition: $[x,y] = x^{-1}y^{-1}xy$ is the **commutator**, and $[G,G] \coloneqq \left\{ [x,y] \;\middle|\; x,y \in G \right\}$ is the **commutator subgroup**.

Lemma:

$$[G,G] \leq H \text{ and } H \trianglelefteq G \implies G/H \text{ is abelian.}$$

1.1 Finitely Generated Abelian Groups

Invariant factor decomposition:

$$G \cong \mathbb{Z}^r \times \prod_{j=1}^{m} \mathbb{Z}/(n_j) \qquad \text{where } n_1 \;\Big|\; \cdots \;\Big|\; n_m.$$

Going from invariant divisors to elementary divisors:

- Take prime factorization of each factor
- Split into coprime pieces

Example:

$$\begin{aligned} &\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2^3 \cdot 5^2 \cdot 7) \\ \cong &\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2^3) \oplus \mathbb{Z}/(5^2) \oplus \mathbb{Z}/(7) \\ . \end{aligned}$$

Going from elementary divisors to invariant factors:

- Bin up by primes occurring (keeping exponents)
- Take highest power from each prime as *last* invariant factor
- Take highest power from all remaining primes as next, etc

Example: Given the invariant factor decomposition

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}, .$$

$p=2$	$p=3$	$p=5$
$2,2,2$	$3,3$	5^2

$\implies n_m = 5^2 \cdot 3 \cdot 2$

$p=2$	$p=3$	$p=5$
$2,2$	3	$\emptyset$

$\implies n_{m-1} = 3 \cdot 2$

$p=2$	$p=3$	$p=5$
2	$\emptyset$	$\emptyset$

$\implies n_{m-2} = 2$

and thus

$$G \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(3 \cdot 2) \oplus \mathbb{Z}/(5^2 \cdot 3 \cdot 2).$$

1.2 The Symmetric Group

Definitions:

- A cycle is **even** $\iff$ product of an *even* number of transpositions.
  - A cycle of even *length* is **odd**
  - A cycle of odd *length* is **even**

Definition The **alternating group** is the subgroup of **even** permutations, i.e. $A_n := \left\{ \sigma \in S_n \;\middle|\; \mathrm{sign}(\sigma) = 1 \right\}$ where $\mathrm{sign}(\sigma) = (-1)^m$ where m is the number of cycles of even length.

Corollary: Every $\sigma \in A_n$ has an even number of *odd* cycles (i.e. an even number of *even-length* cycles).

Example:

$$\begin{aligned} A_4 = &\{\mathrm{id}, \\ &(1,3)(2,4), (1,2)(3,4), (1,4)(2,3), \\ &(1,2,3), (1,3,2), \\ &(1,2,4), (1,4,2), \\ &(1,3,4), (1,4,3), \\ &(2,3,4), (2,4,3)\}. \end{aligned}$$

Lemmas:

- The transitive subgroups of S_3 are S_3, A_3
- The transitive subgroups of S_4 are $S_4, A_4, D_4, \mathbb{Z}_2^2, \mathbb{Z}_4$.
- For $n = 4, S_n$ has two normal subgroups: $A_4, \mathbb{Z}_2^2$.
- For $n \geq 5, S_n$ one normal subgroup: A_n.
- $Z(S_n) = 1$ for $n \geq 3$
- $Z(A_n) = 1$ for $n \geq 4$
- $[S_n, S_n] = A_n$
- $[A_4, A_4] \cong \mathbb{Z}_2^2$
- $[A_n, A_n] = A_n$ for $n \geq 5$
- A_n is *simple* for $n \geq 5$.

1.3 Counting Theorems

Lagrange's Theorem:

$$H \leq G \implies |H| \;\Big|\; |G|.$$

Corollary: The order of every element divides the size of G, i.e.

$$g \in G \implies o(g) \;\Big|\; o(G) \implies g^{|G|} = e.$$

> **Warning:** Rhere does **not** necessarily exist $H \leq G$ with $|H| = n$ for every $n \;\Big|\; |G|$.
> Counterexample: $|A_4| = 12$ but has no subgroup of order 6.

Cauchy's Theorem:

For every prime p dividing $|G|$. there is an element (and thus a subgroup) of order p.

> This is a partial converse to Lagrange's theorem.

Notation: For a group G acting on a set X,

- $G \cdot x = \left\{ g \curvearrowright x \;\middle|\; g \in G \right\} \subseteq X$ is the orbit
- $G_x = \left\{ g \in G \;\middle|\; g \curvearrowright x = x \right\} \subseteq G$ is the stabilizer
- $X/G \subset \mathcal{P}(X)$ is the set of orbits
- $X^g = \left\{ x \in X \;\middle|\; g \curvearrowright x = x \right\} \subseteq X$ are the fixed points

Orbit-Stabilizer:

$$|G \cdot x| = [G : G_x] = |G|/|G_x| \quad \text{if } G \text{ is finite}$$

> Mnemonic: $G/G_x \cong G \cdot x$.

1.3.1 Examples of Orbit-Stabilizer

1. Let G act on itself by conjugation.

- $G \cdot x$ is the **conjugacy class** of x
- $G_x = Z(x) \coloneqq C_G(x) = \left\{ g \;\middle|\; [g, x] = e \right\}$, the **centralizer** of x.
- G^g (the fixed points) is the **center** $Z(G)$.

> *Corollary:* The size of a conjugacy class is the index of the centralizer.
> *Corollary*: the **Class Equation**:
>
> $$|G| = |Z(G)| + \sum_{\substack{\text{One } x_i \text{ from} \\ \text{each conjugacy} \\ \text{class}}} [G : Z(x_i)]$$

1. Let G act on S, its set of *subgroups*, by conjugation.

- $G \cdot H = \left\{ gHg^{-1} \right\}$ is the **set of conjugate subgroups** of H
- $G_H = N_G(H)$ is the **normalizer** of in G of H
- S^G is the set of **normal subgroups** of G

3. For a fixed proper subgroup $H < G$, let G act on its cosets $G/H = \left\{ gH \;\middle|\; g \in G \right\}$ by left-multiplication.

- $G \cdot gH = G/H$, i.e. this is a *transitive* action.
- $G_{gH} = gHg^{-1}$ is a *conjugate subgroup* of H
- $(G/H)^G = \emptyset$

> *Application:* If G is simple, $H < G$ proper, and $[G : H] = n$, then there exists an injective map $\phi : G \hookrightarrow S_n$.
> *Proof:* This action induces ϕ; it is nontrivial since $gH = H$ for all g implies $H = G$; $\ker \phi \trianglelefteq G$ and G simple implies $\ker \phi = 1$.

Burnside's Formula:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

1.3.2 Sylow Theorems

Notation: For any p, let $\mathrm{Syl}_p(G)$ be the set of Sylow-p subgroups of G.

Write

- $|G| = p^n m$ where $(m, p) = 1$,
- S_p a Sylow-p subgroup, and
- n_p the number of Sylow-p subgroups.

Definition: A p-group is a group G such that every element is order p^k for some k. If G is a finite p-group, then $|G| = p^j$ for some j.

> **Lemma:** p-groups have nontrivial centers.

Some useful facts:

- Coprime order subgroups are disjoint, or more generally $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \bigcap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$.
- The Chinese Remainder theorem: $(p, q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

1.3.3 Sylow 1 (Cauchy for Prime Powers)

$$\forall p^n \text{ dividing } |G| \quad \text{there exists a subgroup of size } p^n.$$

> If $|G| = \prod p_i^{\alpha_i}$, then there exist subgroups of order $p_i^{\beta_i}$ for every i and every $0 \leq \beta_i \leq \alpha_i$. In particular, Sylow p-subgroups always exist.

1.3.4 Sylow 2 (Sylows are Conjugate)

All sylow-p subgroups S_p are conjugate, i.e.

$$S_p^1, S_p^2 \in \mathrm{Syl}_p(G) \implies \exists g \text{ such that } gS_p^1 g^{-1} = S_p^2.$$

Corollary: $n_p = 1 \iff S_p \trianglelefteq G$

1.3.5 Sylow 3 (Numerical Constraints)

1. $n_p \,\Big|\, m$ (in particular, $n_p \leq m$),
2. $n_p \equiv 1 \mod p$,
3. $n_p = [G : N_G(S_p)]$ where N_G is the normalizer.

Corollary: p does not divide n_p.

Lemma: Every p-subgroup of G is contained in a Sylow p-subgroup.

> *Proof:* Let $H \leq G$ be a p-subgroup. If H is not *properly* contained in any other p-subgroup, it is a Sylow p-subgroup by definition.
> Otherwise, it is contained in some p-subgroup H^1. Inductively this yields a chain $H \subsetneq H^1 \subsetneq \cdots$, and by Zorn's lemma $H := \bigcup_i H^i$ is maximal and thus a Sylow p-subgroup.

Fratini's Argument: If $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, then $HN_G(P) = G$ and $[G : H]$ divides $|N_G(P)|$.

1.4 Products

Characterizing direct products: $G \cong H \times K$ when

- $G = HK = \left\{ hk \,\middle|\, h \in H, k \in K \right\}$
- $H \bigcap K = \{e\} \subset G$
- $H, K \trianglelefteq G$

> Can relax to only $H \trianglelefteq G$ to get a semidirect product instead

Characterizing semidirect products: $G = N \rtimes_\psi H$ when

- $G = NH$
- $N \trianglelefteq G$
- $H \curvearrowright N$ by conjugation via a map

$$\begin{aligned} \psi : H &\to \mathrm{Aut}(N) \\ h &\mapsto h(\,\cdot\,)h^{-1}. \end{aligned}$$

> *Lemma:* If $\sigma \in \mathrm{Aut}(H)$, then $N \rtimes_\psi H \cong N \rtimes_{\psi \circ \sigma} H$.

Useful Facts

- $\mathrm{Aut}(\prod_{k=1}^{n} \mathbb{Z}/(p)) = \mathrm{GL}(n, \mathbb{Z}/(p))$
  - If this occurs in a semidirect product, it suffices to consider similarity classes of matrices (i.e. just use canonical forms)
- $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}^n)^\times \cong \mathbb{Z}^{\varphi(n)}$ where φ is the totient function.

1.5 Isomorphism Theorems

Lemma: If $H, K \leq G$ and $H \leq N_G(K)$ (or $K \trianglelefteq G$) then $HK \leq G$ is a subgroup.

Diamond Theorem / 2nd Isomorphism Theorem:

If $S \leq G$ and $N \trianglelefteq G$, then

$$\frac{SN}{N} \cong \frac{S}{S \bigcap N}$$

Note: for this to make sense, we also have

- $SN \leq G$,
- $S \bigcap N \trianglelefteq S$,

Cancellation / 3rd Isomorphism Theorem

If $H, K \trianglelefteq G$ with $H \trianglelefteq K$, then

$$\frac{G/H}{G/K} \cong \frac{G}{K}$$

Note: for this to make sense, we also have $G/K \trianglelefteq G/H$.

The Correspondence Theorem / 4th Isomorphism Theorem: Suppose $N \trianglelefteq G$, then there exists a correspondence:

$$\left\{ H < G \;\middle|\; N \subseteq H \right\} \iff \left\{ H \;\middle|\; H < \frac{G}{N} \right\}$$
$$\{\} \iff \{\}.$$

In words, subgroups of G containing N correspond to subgroups of the quotient group G/N. This is given by the map $H \mapsto H/N$.

> Note: $N \trianglelefteq G$ and $N \subseteq H < G \implies N \trianglelefteq H$.

1.6 Special Classes of Groups

Definition: The **"2 out of 3 property"** is satisfied by a class of groups $\mathcal{C}$ iff whenever $G \in \mathcal{C}$, then $N, G/N \in \mathcal{C}$ for any $N \trianglelefteq G$.

Definition: If $|G| = p^k$, then G is a **p-group.**

Lemmas:

- p-groups have nontrivial centers
- Every normal subgroup is contained in the center
- Normalizers grow
- Every maximal is normal
- Every maximal has index p
- p-groups are *nilpotent*
- p-groups are *solvable*

Definition: A group G is **simple** iff $H \trianglelefteq G \implies H = \{e\}, G$, i.e. it has no non-trivial proper subgroups.

> **Lemma:** If G is *not* simple, then for any $N \trianglelefteq G$, it is the case that $G \cong E$ for an extension of the form $N \to E \to G/N$. >

Definition: A group G is **solvable** iff G has a terminating normal series with abelian factors, i.e.

$$G \to G^1 \to \cdots \to \{e\} \text{ with } G^i/G^{i+1} \text{ abelian for all } i.$$

Lemmas:

- G is solvable iff G has a terminating *derived series.*
- Solvable groups satisfy the 2 out of 3 property
- Abelian $\implies$ solvable
- Every group of order less than 60 is solvable.

Definition: A group G is **nilpotent** iff G has a terminating central series, upper central series, or lower central series.

> Moral: the adjoint map is nilpotent.

Lemma: For G a finite group, TFAE:

- G is nilpotent

- Normalizers grow (i.e.$H < N_G(H)$ whenever H is proper)
- Every Sylow-p subgroup is normal
- G is the direct product of its Sylow p-subgroups
- Every maximal subgroup is normal
- G has a terminating *Lower* Central Series
- G has a terminating *Upper* Central Series

Lemmas:

- G nilpotent $\implies$ G solvable
- Nilpotent groups satisfy the 2 out of 3 property.
- G has normal subgroups of order d for *every* d dividing $|G|$
- G nilpotent $\implies$ $Z(G) \neq 0$
- Abelian $\implies$ nilpotent
- p-groups $\implies$ nilpotent

1.7 Series of Groups

Definition: A **normal series** of a group G is a sequence $G \to G^1 \to G^2 \to \cdots$ such that $G^{i+1} \trianglelefteq G_i$ for every i.

Definition A **composition series** of a group G is a finite normal series such that G^{i+1} is a *maximal proper* normal subgroup of G^i.

Theorem (Jordan-Holder): Any two composition series of a group have the same length and isomorphic factors (up to permutation).1

Definition A **derived series** of a group G is a normal series $G \to G^1 \to G^2 \to \cdots$ where $G^{i+1} = [G^i, G^i]$ is the commutator subgroup.

> The derived series terminates iff G is *solvable*.

Definition: A **central series** for a group G is a terminating normal series $G \to G^1 \to \cdots \to \{e\}$ such that each quotient is **central**, i.e. $[G, G^i] \leq G^{i-1}$ for all i.

Definition: A **lower central series** is a terminating normal series $G \to G^1 \to \cdots \to \{e\}$ such that $G^{i+1} = [G^i, G]$

> Moral: Iterate the adjoint map $[\,\cdot\,, G]$.

> G is nilpotent $\iff$ the LCS terminates.

Definition: An **upper central series** is a terminating normal series $G \to G^1 \to \cdots \to \{e\}$ such that $G^1 = Z(G)$ and G^{i+1} is defined such that $G^{i+1}/G^i = Z(G^i)$.

> Moral: Iterate taking “higher centers”.