Algebra I Midterm Review

Hui Sun

October 27, 2024

Contents

Chapter 1

Definitions

1.1 Chapter IV: Groups II

We first recall some definitions.

Definition 1.1 (stabilizer, fixed points)**.** Let G act on a set S, then for $a \in S$, the stabilizer of $Stab_G(a)$ is

$$Stab_G(a) = \{g \in G : g \cdot a = a\}$$

(we use $\cdot$ to denote the action.) And the set of fixed points of this action is

$$Z = \{a \in S : g \cdot a = a, \text{ for all } g \in G\}$$

Proposition 1.1. Let S be a finite set, and let G act on S, then

$$|S| = |Z| + \sum_{a \in A} [G : Stab_G(a)]$$

where A has exactly one element from each nontrivial orbit of the action.

Definition 1.2 (p-group)**.** A p-group is a finite group whose order is a power of a prime integer p.

Corollary 1.1. Let G be a p-group acting on a finite set S, and let Z be the fixed point of the action, then

$$|Z| \equiv |S| \mod p$$

($[G : Stab_G(a)]$ divides $|G|$.)

Next we focus on the group action being conjugation.

Definition 1.3 (center)**.** The center is as follows

$$Z(G) = \{g \in G : ga = ag, \forall a \in G\}$$

In other words, the center consists of elemenets that commute with every other element in the group.

Lemma 1.1. Let G be a finite group, and assume $G/Z(G)$ is cyclic, then G is commutative.

Definition 1.4 (centralizer)**.** The centralizer $Z_G(a)$ for $a \in G$ is the stabilizer under conjugation, i.e.,

$$Z_G(a) = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\}$$

is the set of elements in G that commute with the given a.

We note that the center $Z(G) = \bigcap_{a \in G} Z_G(a)$.

Definition 1.5 (conjugacy class)**.** The conjugacy class of $a \in G$ is the orbit $[a]$ under the conjugation action. And $a, b \in G$ are conjugate if they belong to the same conjugacy class.

Proposition 1.2 (class formula)**.** Let G be a finite group, then

$$|G| = |Z(G)| = \sum_{a \in A} [G : Z_G(a)]$$

where A is a set containing one representative for each nontrivial conjugacy class in G.

Corollary 1.2. Let G be a nontrivial p group, then G has a nontrivial center.

Next we talk about conjugation of subsets and subgroups.

Definition 1.6 (normalizer, centralizer)**.** Let $A \subset G$ be a subset, then $N_G(A)$ is the normalizer of a subset A is $Stab_G(A)$ under conjugation, i.e.,

$$N_G(A) = \{g \in G : gAg^{-1} = A\}$$

The centralizer of A, $Z_G(A)$ is

$$Z_G(A) = \{g \in G : gag^{-1} = a, \text{ for all } a \in A\}$$

i.e., $Z_G(A) = \bigcap_{a \in A} Z_G(a)$. We note that $Z_G(A) \subset N_G(A)$.

We interpret $N_G(H)$ as the largest subgroup of G in which H is normal.

The definition implies that if H is a normal subgroup of G, then $N_G(H) = G$.

Lemma 1.2. Let $H \subset G$ be a subgroup, then if finite, then the number of subgroups conjugate to H is equal to the index $[G : N_G(H)]$ of the normalizer H in G.

Proposition 1.3. If $[G : H]$ is finite, then the number of subgroups conjugate to H is finite and divides $[G : H]$.

Next we begin Sylow theorems.

Proposition 1.4 (Cauchy's theorem)**.** Let G be a finite group, and let p be a prime divisor of $|G|$, then G contains an element of order p.

Corollary 1.3. Let G be a finite grou, and let p be a prime divisor of $|G|$, and let N be the number of cyclic subgroups of G of order p, then $N \equiv 1 \mod p$.

Definition 1.7 (simple group)**.** A group is simple if it is nontrivial and is only normal subgroups are $\{e\}$ and G itself.

Definition 1.8 (p-Sylow subgroup)**.** Let p be a prime integer, A p-Sylow subgroup of a finite group G is a subgroup of order p^r, where $|G| = p^r m$ and $\gcd(p, m) = 1$.

Theorem 1.1 (Sylow I)**.** Every finite group contains a p-Sylow subgroup, for all primes p.

The next proposition is stronger and implies Sylow I.

Proposition 1.5. If p^k divides the order of G, then G has a subgroup of order p^k.

The second Sylow theorem states that every maximal p-group in $|G|$ is a p-Sylow subgroup. It is as large as is allowed by Lagrange's.

Theorem 1.2 (Sylow II)**.** Let G be a finite group, let P be a p-Sylow subgroup, and $H \subset G$ be a p-subgroup, then H is contained in some conjugate of P: there exists $g \in G$ such that

$$H \subset gPg^{-1}$$

Proposition 1.6. Let H be a p-subgroup of a finite group G, assume that H is not a p-Sylow subgroup, then there exists a p-subgroup H' of G containing H, such that

$$[H' : H] = p$$

and H is normal in H'.

Here comes the last Sylow theorem.

Theorem 1.3 (Sylow III)**.** Let p be prime, and let G be a finite group of order $|G| = p^r m$, assume p does not divide m, then the number of p-Sylow subgroups of G divides m and is congruent to 1 modulo p.

Next we list some applications of Sylow theorems.

Proposition 1.7. Let G be a group of order mp^r, where p is a prime integer and $1 < m < p$. Then G is not simple.

Corollary 1.4. Assume $p < q$ are prime integers, and $q \not\equiv 1 \mod p$, let G be a group of order pq, then G is cycic.

Corollary 1.5. Let q be an odd prime, and let G be a noncommutative group of order q, then $G \cong D_{2q}$, the dihedral group.

Next we begin composition series and solvability.

Definition 1.9 (series). A series of subgroups G_i of a group G is a decreasing sequence of subgroups starting from G:

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \dots$$

where each $\supsetneq$ is strict inclusion.

The series is normal if G_{i+1} is normal in G_i for all i. The maximal length of a normal series is denoted as $l(G)$.

We note that $l(G) = 1$ if and only if G is simple.

Definition 1.10 (composition series). A composition series for G is a normal series

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \dots$$

such that the successive quotients G_i/G_{i+1} are simple.

Theorem 1.4 (Jordan-Holder). Let G be a group, and let

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{e\}$$

and

$$G = G'_0 \supsetneq G'_1 \supsetneq \cdots \supsetneq G'_n = \{e\}$$

be two composition series for G. Then $m = n$ and the lists of quotients groups $H_i = G_i/G_{i+1}$, $H'_i = G'_i/G'_{i+1}$ agree (up to isomorphism) after a permutation of the indices.

Proposition 1.8. Let G be a group, and let N be a normal subgroup of G. Then G has a composition series if and only if both N and G/N have composition series. Further, if this is the case, then

$$l(G) = l(N) + l(G/N)$$

and the composition factors of G consist of the collection of composition factors from N and G/N.

Definition 1.11 (refinement). A series is a refinement of another series if all terms of the first appear in the second.

Proposition 1.9. Any two normal series of a finite group ending with $\{e\}$ admit equivalent refinements.

(The idea is to first refine it to composition series then apply Jordan-Holder).

Definition 1.12 (commutator subgroup). Let G be a group, the commutator subgroup of G is the subgroup **generated** by all elements

$$[g, h] = ghg^{-1}h^{-1}$$

where $g, h \in G$. We denote the commutator subgroup as $[G, G]$.

Lemma 1.3. Let $\varphi : G \to H$ be a homomorphism, then

$$\varphi[g, h] = [\varphi(g), \varphi(h)]$$

Proposition 1.10. Let $[G, G]$ be commutator subgroup of G, then

1. $[G, G]$ is normal in G.
2. The quotient $G/[G, G]$ is commutative.
3. If $\alpha : G \to A$ is a homomorphism to some commutative group A, then
$$[G, G] \subset \ker \alpha$$
4. the natural projection $G \to G/[G, G]$ is universal in the category of homomorphisms $\alpha : G \to A$ where A is some commutative group.

One can get taking the commutator:

Definition 1.13 (derived series)**.** Let a derived series of G be as follows:
$$G \supset [G, G] \supset [[G, G], [G, G]] \supset \dots$$

Definition 1.14 (solvable)**.** A group is solvable if its derived series terminates with the identity.

Proposition 1.11. For a finite group G, then the following are equivalent:

1. G is solvable.
2. All composition factors of G are cycic.
3. G admits a cyclic series ending in $\{e\}$.
4. G admits an abelian series ending in $\{e\}$.

Corollary 1.6. All p-groups are solvable.

Corollary 1.7. Let N be a normal subgroup of a group G, then G is solvable if and only if both $N, G/N$ are solvable.

Next we talk about symmetric group.

Definition 1.15 (cycle)**.** A nontrivial cycli is an element of S_n with exactly one nontrivial orbit. For distinct $a_1, \dots, a_r$ in $\{1, \dots, n\}$, the notation
$$(a_1 a_2 \dots a_n)$$
denote the cycle in S_n with nontrivial orbit $\{a_1, \dots, a_r\}$, acting as
$$a_1 \mapsto a_2 \mapsto a_2 \mapsto \dots a_r \mapsto a_1$$
In this case, r is the lenght of the cycle. A cycle of length r is called an r-cycle.

Lemma 1.4. Disjoint cycles commute.

Lemma 1.5. For every $\sigma \in S_n$, where $\sigma \neq e$, can be written as a product of disjoint nontrivial cycles, in a unique way up to permutations of the factors.

Definition 1.16 (type). The type of $\sigma \in S_n$ is the parittion of n given by the size of the orbits of the action of $\langle \sigma \rangle$ on $\{1, \ldots, n\}$.

For example, $\sigma = (18632)(47)(5)$ has type $[5, 2, 1]$.

Lemma 1.6. Let $\tau \in S_n$, and let $(a_1 \ldots a_r)$ be a cycle, then

$$\tau(a_1 \ldots a_r)\tau^{-1} = (\tau^{-1}a_1 \ldots \tau^{-1}(a_n))$$

Proposition 1.12. Two elements of S_n are conjugate in S_n if and only if they have the same type.

Corollary 1.8. The number of conjugacy classes in S_n equals the number of parititons of n.

Next we talk about alternating groups.

Definition 1.17 (sign). The sign of a permutation $\sigma \in S_n$, denoted as $(-1)^\sigma$, is determined by the action of σ on Δ_n, where

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

which is in $\mathbb{Z}[x_1, \ldots, x_n]$, and

$$\Delta_n \sigma = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

and

$$\Delta_n \sigma = (-1)^\sigma \Delta_n$$

Lemma 1.7. Transpositions generate S_n.

Lemma 1.8. Let $\sigma = \tau_1 \ldots \tau_r$ be a product of transpositions, then σ is even when r is even, and odd when r is odd.

Definition 1.18 (alternating group). The alternating group on $\{1, \ldots, n\}$, denoted A_n, consists of even permutations $\sigma \in S_n$.

We note that A_n is a normal subgroup of S_n, and $[S_n : A_n] = 2$.

Next we talk about conjugacy class of A_n, solvability of S_n, etc.

Lemma 1.9. Let $n \geq 2$, and $\sigma \in A_n$, then

$$[\sigma]_{A_n} = [\sigma]_{S_n}$$

or the size of $[\sigma]_{A_n}$ is half hte size of $[\sigma]_{S_n}$, according to whether the centralizer $Z_{S_n}(\sigma)$ is not or is contained in A_n.

Proposition 1.13. Let $\sigma \in A_n$, where $n \geq 2$, then the conjugacy class of σ in S_n splits into two conjugacy classes in A_n precisely if the type of σ consists of distinct odd numbers.

Corollary 1.9. The alternating group A_5 is a simple noncommutative group of order 60.

Lemma 1.10. The alternating group A_n is generated by 3-cycles.

Proposition 1.14. Let $n \geq 5$, if a normal subgroup of A_n contains a 3-cycle, then it contains all 3-cycles.

Theorem 1.5. The alternating group A_n is simple for all $n \geq 5$.

Corollary 1.10. For $n \geq 5$, the group S_n is not solvable.

Next we talk about products of groups.

Lemma 1.11. Let N, H be normal subgroups of a group G, then

$$[N, H] \subset N \cap H$$

Corollary 1.11. Let N, H be normal subgroups of a group G, assume $N \cap H = \{e\}$, then N, H commute, i.e., for all $n \in N, h \in H$, we have

$$nh = hn$$

Proposition 1.15. Let N, H be normal subgroups, and $N \cap H = \{e\}$, then

$$NH \cong N \times H$$

Next we talk about groups in exact sequences.

Definition 1.19 (extension). Let N, H be groups, a group G is an extension of H by N if there is an exact sequence of groups:

$$1 \to N \to G \to H \to 1$$

Definition 1.20 (split). An exact sequence of groups is said to split if H may be identified with a subgroup of G, so that

$$N \cap H = \{e\}$$

Lemma 1.12. Let N be a normal subgroup of a group G, and let H be a subgroup of G such that $G = NH$ and $N \cap H = \{e\}$. Then G is a split extension of H by N.

Next we define internal and semidirect products.

Definition 1.21. Let N, H be any two groups and an arbitrary homomorphism

$$\theta : H \to Aut(N), h \mapsto \theta_h$$

define an operation $\bullet_\theta$ on the set $N \times H$ as follows: for $n_1, n_2 \in N, h_1, h_2 \in H$, we have

$$(n_1, h_1) \bullet_\theta (n_2, h_2) = (n_1\theta_{h_1}(n_2), h_1h_2)$$

Lemma 1.13. The resulting structure $(N \times H, \bullet_\theta)$ is a group, with the identity element (e_N, e_H).

Definition 1.22. The group $(N \times H, \bullet_\theta)$ is a semidirect product of N, H and is denoted by $N \rtimes_\theta H$.

Proposition 1.16. Let N, H be groups, and let $\theta : H \to Aut(N)$ be a homomorphism, let $G = N \rtimes_\theta H$ be the corresponding semidirect product. Then

1. G contains isomorphic copies of N and H.
2. The natrual projection $G \to H$ is a surjective homomorphism, with kernel N, thus N is normal in G, and the sequence
$$1 \to N \to N \rtimes_\theta H \to H \to 1$$
is split exact.
3. $N \cap H = \{e_G\}$.
4. $G = NH$.
5. The homomorphism θ is realized by conjugation in G: that is, for $h \in H$ and $n \in N$, we have
$$\theta_h(n) = hnh^{-1}$$
in G.

Proposition 1.17. Let N, H be subgroups of a group G, with N normal in G. Assume that $N \cap H = \{e\}$, and $G = NH$, let $\gamma : H \to Aut(N)$ be defined by conjugation: for $h \in H, n \in N$, we have
$$\gamma_h(n) = hnh^{-1}$$
then
$$G \cong N \rtimes_\gamma H$$

We now talk about finite abelian groups.

Lemma 1.14. Let G be commutative, and let H, K be subgroups such that $|H|, |K|$ are relatively prime, then
$$H + K \cong H \oplus K$$

Corollary 1.12. Every finite abelian group is the direct sum of its nontrivial Sylow subgroups.

Lemma 1.15. Let G be a commutative p-group, and let $g \in G$ be an element of maximal order, then the exact sequence
$$0 \to \langle g \rangle \to G \to G/\langle g \rangle \to 0$$
splits.

Lemma 1.16. Let p be a prime integer and $r \geq 1$, let G be a noncyclic abelian group of order p^{r+1}, and let $g \in G$ be an element of order p^r. Then there exists an element $h \in G$, where $h \notin \langle g \rangle$, such that
$$|h| = p$$

Corollary 1.13. Let G be a finite abelian groups, then G is a direct sum of cyclic p-groups.

Theorem 1.6. Let G be a finite nontrivial commutative group, then

1. There exist prime integers $p_1, \dots, p_r$ and positive integers n_{ij} such that $|G| = \prod_{i,j} p_i^{n_{i,j}}$ and
$$G \cong \bigoplus_{i,j} \frac{\mathbb{Z}}{p_i^{n_{i,j}}\mathbb{Z}}$$
2. There exist positive integers $1 < d_1 | \dots | d_s$ such that $|G| = d_1 \dots d_s$ and
$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{d_s\mathbb{Z}}$$

Lemma 1.17. Let G be a finite abelian group, and assume that for every integer $n > 0$, the number of elements $g \in G$ such that $ng = 0$ is at most n. Then G is cyclic.

Theorem 1.7. Let F be a field, and let G be a finite subgroup of the multiplicative group $(F^*, \cdot)$, then G is cyclic.