Algebraic Theory I

Thomas Fleming

October 22, 2021

Contents

Lecture 24: Summary of Group Theory

Mon 18 Oct 2021 18:06

1 Summary of Group Theory

This is a study guide for the midterm and not an actual lecture.

1.1 Basic Group Theory

Theorem 1.1 (Isomorphism Theorems)**.** The isomorphism theorems go roughly as follows:

- Kernel's of surjective homomorphisms are normal subgroups.
- Quotients behave like division: $\frac{G}{H} = \frac{\frac{G}{K}}{\frac{H}{K}}$ (if $K \leq H$).
- Quotients "cancel" into simpler quotients: $\frac{HK}{K} = \frac{H}{H \cap K}$.
- Quotients perserve group structure: Bijecetion between $H \trianglelefteq G$ and $\frac{H}{K} \trianglelefteq \frac{G}{K}$ if $\ker(\varphi) \trianglelefteq H$.

Definition 1.1. We denote the following sets

$$G_x = \{g \in G : x^g = x\}$$
$$G_X = \{g \in G : x^g = x \forall x \in X\}$$
$$N_G(X) = \{y \in G : yXy^{-1} = X\}$$
$$Z_G(X) = \{y \in G : yxy^{-1} = x \forall\ x \in X\}$$
$$[X, Y] = \{xyx^{-1}y^{-1} : x \in X, y \in Y\}$$
$$\mathscr{O}_X = \{x^g : x \in X, g \in G\}.$$

Definition 1.2 (Group Action)**.** A group G acts on Ω by permuting its elements. Formally $\alpha : G \to \mathrm{Perm}(\Omega)$ such that each g permutes Ω. A special group action is the conjugation map $x \mapsto yxy^{-1}$.

Remark. We need only check $(x^g)^h = x^{hg}$ and $x^1 = 1$.

Definition 1.3. A group action is faithful if it has trivial kernel.

Theorem 1.2. $G_{x^g} = gG_xg^{-1}$.

Proof. Allude to definitions and take a change of variables to the conjugation. □

Theorem 1.3. $x^g = x^h$ if and only if x, y are in a common left G_x-coset.

Proof. Show $g \in hG_x$ by definitions. □

Theorem 1.4 (Orbit-Stabilizer)**.** $|\mathscr{O}_x| = |G : G_x|$.
$|\Omega| = |Z_G(G)| + \sum_{x \in C'} |G : Z_G(x)|$.

Proof. Take the map $f : \{gG_x : g \in G\} \to \Omega,\ x \mapsto f(gG_x) = x^g$ and show its a bijection. For the second equation let the orbit be the whole set and peel of the first term of the summation. □

1.2 P-groups

Definition 1.4. H and K are conjugate if $K = gHg^{-1}$ for some g. Note that the number of subgroups conjugate to H is $|G : N_G(H)|$ by appealing to definitions.

Theorem 1.5. A subgroup of index 2 is normal.

Proof. Let G act on all conjugate subgroups by conjugation. It is trivial that $N_G(H) = H$ or G. G is proof and if it is H we see there are two conjugate subgroups $\Omega = \{H, K\}$ so there is a homomorphism into S_2 and its kernel is H. $\square$

Remark. A subgroup of index of the smallest prime divisor of G is normal by the same argument.

Definition 1.5. A group is a p-group if the order of every element is p^n. A subgroup is a sylow p-group if its order is the highest prime power of p in $|G|$.

Theorem 1.6 (Cauchy's Theorem)**.** If $p \mid |G|$ then there is a $\operatorname{ord}(g) = p$ (hence a subgroup of order p).

Proof. There are two cases, the abelian and nonabelian.

- For the abelian case we proceed as follows:
- Let $H = \langle x \rangle$ and note that if $p \mid H$, then $\operatorname{ord}\left(x^{|H|/p}\right) = p$, so such an element exists.
- If $p \nmid |H|$, then appeal to the quotient group so $p \mid |G/H|$ and define a homomorphism to the quotient where the IH guaranteed an element of order p which we can pullback.
- For the nonabelian case we cite the class equation. If $p \mid |Z(G)|$, then appeal to the abelian case. Else, we find atleast one $p \nmid |G : Z_G(x)|$ by appealing to the class equation mod p. Then, we see $p \mid |Z_G(x)|$. If $Z_G(x)$ is smaller than G we apply IH else we see if a point centralizer is G this implies that element is in $Z(G)$, a contradiction.

$\square$

Theorem 1.7. A p group acting on a finite set has a number of fixed points congruent to $|\Omega|$ mod p.

Proof. Seperate out all orbits of index ≥ 2 and note that $|G : G_x| = p^m$, and the congruency follows. $\square$

Theorem 1.8. A sylow p-group has $H \leq N_G(P) \Rightarrow H \leq P$.

Proof. Appeal to the 3rd isomorphism theorem to see $|HP| / |P| = |H| / |H \cap P|$. Then, we sandwich $|HP|$ between $|P|$ to induce the result. $\square$

Theorem 1.9 (Sylow's Theorem).

- $n_p \geq 1$.
- A p-group is contained in a sylow p-group.
- p-groups are conjugate.
- $n_p \equiv 1 \mod p$
- $n_p = |G : N_G(P)|$ hence $n_p \mid \frac{|G|}{n^p}$

Proof.

- 1 is already shown
- Let Ω be the set of subgroups conjugate to P and G act by conjugation. G acts transitively, hence $|\Omega| = |G : G_P|$ Then, $p \nmid |G : N_G(P)|$. THen, restricting the action to H yields by an earlier lemma the number of fixed points a multiple of p. Hence, there is some fixed point P' which is conjugate to P and $H \leq P'$.
- We find a P' conjugate to P and we see $P' \leq P$ but $|P| = |P'|$, so equality holds and we see the claim holds.
- As all $p$groups are conjuagte applying orbit stabilizer yields $n_p = |\Omega| = |G : G_P| = N_G(P)$ hence $n_p \equiv |\Omega| \mod p$. Letting P' be another P group which is fixed we see $P' = P$ and $P \subseteq N_G(P')$ and $P' = P$ is the only fixed point so $n_p \equiv 1 \mod p$.

$\square$

Theorem 1.10. A group of order p^2 is abelian.

Theorem 1.11. A nontrivial p-group admits a nontrivial $Z(G)$.

Proof. Appeal to the class equation to see $p \mid |Z(G)|$. As the center is nontrivial wee it has order p or p^2. If $|Z(G)| = p$ hence cylic hence $G = Z(G) \cup G/Z(G)$. Then, we see generators $x, Z(G)$ which commute, so G is abelian. $\square$

Theorem 1.12. If $|G| = pq$ $p < q$ and $p \nmid q - 1$, then G is abelian.

Proof. We see $n_p = 1 = n_q$ by sylow's theorem, Hence every $g \in G$ fixes P, Q by conjugation. Then, we see $pq || |PQ|$, so $|PQ| = G$ THen appealing to the size of the subgroups and normality yields $xy = yx' = x'y' = xy \Rightarrow xy = yx$. $\square$

1.3 Semidirect products

Definition 1.6. $(x, y)(a, b) = (xa^y, b)$

Remark. $(x, y)^{-1} = \left(\left(x^{-1}\right)^{h^{-1}}, h^{-1}\right)$

Theorem 1.13. If $H \trianglelefteq N \rtimes_{\alpha} H$, then $\alpha = 1$

Proof. Examine $(x, 1)(1, h)\left(x^{-1}, 1\right)$ and we find $\left(x^{-1}\right)^{h} = x^{-1}$ □

Theorem 1.14. $NH \simeq N \rtimes_{\alpha} H$ if $\alpha : h \mapsto hxh^{-1}$.

Proof. Appeal to 2nd isomorphism theorem and we see $\frac{NH}{N} \simeq H$. So, we see there are $|H|$ N-cosets in NH. So every Nh is distinct. So, $\alpha : xh \mapsto (x, h)$ is a bijective homomorphism. So they are isomorphic. □

1.4 Simple Groups

Definition 1.7 (Simple Groups)**.** G is simple if it has no nontrivial proper normal subgroups.

Remark. Methods for Determining if a group is simple

- Counting elements of p-groups of power 1.
- Permutation representations.
- Small index subgroups.
- Playing p-groups off each other.

Remark. Counting elements of p-groups of order 1 consists of finding sylow p-groups of order p^1 and then it is clear all elements of the sylow p-groups must be distinct (except identity). Adding these up for all p yields a contradiction.

Remark. For small index subgroups we know a subgroup of index k implies $G \simeq H \leq S_k$. Hence, $|G| \mid |S_k|$. Then, we know if k is the smallest integer such that $|G| \mid k!$, then k is also the minimal index over all proper subgroups. From here we can induce a contradiction by appealing to sylows theorem.

Remark. For Permutation Representations we appeal to one of the following facts. If G has an element of order of k , then so does S_k and if P is a sylow p-group of G, then $|N_G(P)| \mid |N_{S_k}(P)|$. Then, we see the number of p-groups in S_k is $\frac{\prod_{i=k-p+1}^{k} i}{p(p-1)}$. Hence $|N_{S_k}(p)| = p(p-1)$, so $|N_G(P)| \mid p(p-1)$.

Remark. For playing p-groups off of each other. Take a p-group in a p-group, for example $P \leq Q$ and force it to be normal. Then, it is eithere a P-group in G or its contained in one, P^* (which is contained in $N_G(P)$). Hence, we find $\langle N_G(Q), P^* \rangle \leq N_G(P)$, so $|N_G(Q)||P^*| \mid |N_G(P)|$. We can induce a contradiction from here.

1.5 Nilpotent Groups

Definition 1.8. The upper central series is $Z_1(G) = Z(G)$, and $Z_n(G)/Z_{n-1}(G) = Z(G/Z_n(G))$. If this is G eventually, then G is nilpotent.
Equivalently the lower central series is $G^1 = [G, G]$, $G^n = \{G, G^{n-1}\}$. If this is trivial eventually, then G is nilpotent.

Theorem 1.15. Every finite p-group is nilpotent.

Proof. We know the center of a p-grop is nontrivial. From here we show $Z_1 < Z_2$ and induce up to the size of the group. □

Definition 1.9. A subgroup H is characteristic if every automorphism has $\alpha(H) \leq H$.

Remark. $K \trianglelefteq H$ and H characteristic is G yields $K \trianglelefteq G$.

Theorem 1.16. TFAE

- P is the unique sylow p-group in G.
- $P \trianglelefteq G$
- P characteristic in G.
- A subgroup generated by elements of order p^i is a p-group.

Proof.
- $1 \Leftrightarrow 2$ is already shown and $1 \Rightarrow 3$ follows as $\alpha(P)$ is also a sylwo p-group.
- $1 \Rightarrow 4$ If X is such a group $\langle x \rangle \subseteq P$ for all x so $X \subseteq p$ is a p-group.
- $4 \Rightarrow 1$ if they were not unique we have that such a group X would be $P \subseteq \langle P \cup P' \rangle \subseteq X \subseteq P$ so contradiction.

□

Remark. If H, K are groups then $Z(H \times K) = Z(H) \times Z(K)$

Proof. Appeal to definitions. □

Theorem 1.17. For a homomorphism with $\ker(\alpha) = K \leq H$, then $N_G(H) = f^{-1}(N_{G'}(\varphi(H)))$.

Proof. Appeal to homomorphism properties in both directions with $x \in N_G(H)$ xHx^{-1} □

Theorem 1.18. TFAE

- G is nilpotent
- Proper subgroups are proper in their normalizers
- All p-groups are normal
- G is the direct product of its sylow p-groups.

Proof.
- 2 $\Rightarrow$ 3 G must be abelian with a P not normal. Then as P is characteristic in $N_G(P)$, we see its normal in $N_G(N_G(P))$ so by definition the normalizers are equal. Hence we have a non normal P-group implies there is a subgroup not in its normalizer contradiction.

□

Theorem 1.19. If G has $n \mid |G|$ with at most n x , $x^n = 1$, then G is cyclic.

Proof. First, we see there are at most $|P| = p^\alpha$ elements with $x^{p^\alpha} = 1$, so P must be distinct. So, all P-groups are normal G is the product of the P-groups. Then, we can show each P_i group is cyclic and the product of their generators is a generator of G as the primes are distinct. □

Theorem 1.20 (Frattini Argument)**.** If $H \trianglelefteq G$ and $P \leq H$ is a sylow group of H , then $G = HN_G(P)$.

Proof. $HN_G(P) \leq G$ by an earlier lemma so letting G act by conjugation yields $P^g \leq H$ so P^g is a sylow p-group which is conjugate to P, so there is a $P^h = P^g$ and we find $h^{-1}g \in N_G(P)$, so $g \in hN_G(P)$. Appealing to third isomorphismtheorem yields $|G : H| \mid |N_G(P)|$. □

Theorem 1.21. G is nilpotent iff every maximal subgroup is normal.

Proof. $\Rightarrow$ If M is maximal then $M = N_G(M)$ or M is normal. If $M = N_G(M)$ this is contradiction as nilpotent groups do not admit proper subgroups equal to their normalizer. $\Leftarrow$ We need only show all sylow groups are normal. Take a maximal subgroup containing $N_G(P)$. Applying frattini argument yields $G = N_G(P)M$, so $G \subseteq MM = M < G$ contradiction. □

1.6 Solvable Groups

Definition 1.10. A group is solvable if it admite a normal chain $H_0 \trianglelefteq H_1 \ldots \trianglelefteq H_n = G$ with the quotient of consecutive H_i being abelian.
An equivalent characterization is the iterated commutator $G^{(1)} = [G, G]$ and $G^{(n)} = \left[G^{(n-1)}, G^{(n-1)}\right]$. If this is trivial at some point then G is solvable.

Proof. $\Rightarrow$ We show each $G^{(i)} \leq H_i$. Induce $G^{(i)} \leq H_{n-i}$ on i and the base case is trivial. For the i case note $G^{(i)} \leq \left[H_{n-(i-1)}, H_{n-(i-1)}\right]$ and we get $G^{(n)} \leq H_{n-n} = \{1\}$.
$\Leftarrow$. Let $H_i = G^{(n-i)}$ and induce on i to show the quotient H_i/H_{i-1} is abelian as it is the quotient of a commutator.. $\square$

Theorem 1.22. A subgroup of a solvable group is solvable.

Proof. Induce to show $H^{(n)} \leq G^{(n)}$. $\square$

Theorem 1.23. Homomorphisms preserve solvability.

Proof. Induce on $G^{(i)}$ to show $\varphi\left(G^{(i)}\right) = \varphi\left(G\right)^{(i)}$ $\square$

Theorem 1.24. Let G and $H \trianglelefteq G$ then G solvable iff H and G/H are solvable.

Proof. $\Rightarrow$ Already shown. $\Leftarrow$. Take normal chains of H and G/H and append then to each other. $\square$

1.7 Free Groups

Definition 1.11. X is an alphabet, then $F\left(X\right)$ is the free group on X.

Theorem 1.25 (Universal Mapping Property)**.** $F\left(X\right)$ is a group F with an injection $\sigma : X \overset{F}{\hookrightarrow}$ so that for any $\alpha : X \to G$ there is a $\beta : F \to G$ such that $\beta\left(\sigma\right) = \alpha$.

Theorem 1.26. Use universal mapping property to induce bijective homomorphisms from $F_1 \to F_2$ which is an extension of the assymed bijection $\alpha : X_1 \to X_2$.

Theorem 1.27. For $\alpha : F \to H$ and $\beta : G \to H$, we find a $\gamma : F \to G$ so that $\beta\gamma = \alpha$.

Proof. Let $\beta(g_x) = \alpha(x)$ for some g_x , then we find a homomorphism $x \mapsto g_x$. $\square$

Definition 1.12 (Group Presentations)**.** A group presentation is a set X and a set of relators Y such that $\bigcap_{H \trianglelefteq G, H \geq Y} H = N$ yields a group $F(X)/N$ following the relations.

Remark. $\{\prod_{i=1}^{\ell}\left(g_i x_i g_i^{-1}\right) : g_i \in G, g\times \in X \cup X^{-1}\}$

Theorem 1.28. If $G = \langle X : R\rangle$ and $H = \langle X : R'\rangle$ with all relations in R being relations in R' , then $\alpha(G) = H$ for some α homomorphism.

Proof. $N \leq N'$ so appealing to isomorphism theorems yields $F(X)/N' = G/(N'/N)$. $\square$

Theorem 1.29. Every word is equivalent to a uniqe reduced word.

Proof. For each letter define a map multiplying elements by m on the left. It is a permutation on the set of redued words hence each letter corresponds to a symmetry of R via a homormophism. Then for any two reduced words which are equivalent we find their representation in the symmetry group is the same, hence the words are the same. $\square$

Definition 1.13. $V_X(w) =$ the sum of total powers of a letter in a word.

Definition 1.14. $\text{Rank}(F(X)) = |X|$.

Theorem 1.30. If $F(X) \simeq F(Y)$, then $|X| = |Y|$

Proof. Take a subgroup generated by squares and remark that it is characteristic hence normal. Then, we see $G/H \simeq \varphi(G)/\varphi(F(X)) \simeq G'/H'$. Then as every elements square is 1 in G/H , so it is an abelian 2-group. Then, we see all products of cosets are unique by multiplying any two and noting the multiplicity of elements versus the multiplicity of their generators.
Hence, we find $G/H = \bigoplus_{x \in X} \langle x\rangle = (\mathbb{Z}/2\mathbb{Z})^{|X|}$. This is a vector space over $\mathbb{F}_2$ with elements corresponding to the power 1 or 0 of some $\overline{x} \in X$. Then, we find the dimensions of G/H and G'/H' are equal and as the dimensions are simply $|X|$, $|X'|$ this completes the proof. $\square$

Theorem 1.31. Subgroups of free groups are free. A subgroup of finite index, m, has $\text{Rank}(H) = \text{Rank}(F)\, m + 1 - m$.

Lecture 25: Review of Test and Intro to Ring Theory

Fri 22 Oct 2021 11:31

Proof of question 6. Let $C_{105} \rtimes_{\alpha} C_5$ and define $\alpha : C_5 \to \text{Aut}\,(C_{105})$. Recall, we need only show α is the trivial homomorphism. Recall $\text{Aut}\,(C_{105}) = C_2 \times C_4 \times C_6$. Hence, $|\text{Aut}\,(C_{105})| = 2 \cdot 4 \cdot 6$ and as $5 \nmid 2 \cdot 4 \cdot 6$, we see every element must map to 1. $\square$

2 Intro to Ring Theory

Definition 2.1 (Ring)**.** A **ring** R is a set equipped with two closed operations $+$ and $\times$ obeying the following properties

1. $(R, +)$ forms an abelian group with additive identity, 0 .
2. There is a multiplicative identity, 1 .
3. $0 \neq 1$. (This would guarantee the ring is trivial)
4. The multiplicative operation is associative : $(xy)\,z = x\,(yz)$ for all $x, y, z \in R$.
5. The distributive properties hold: $x\,(y + z) = xy + xz$ and $(x + y)\,z = xz + yz$ for all $x, y, z \in R$.

A ring for which the multiplication operation is also commutative: $xy = yx$, will be called a **commutative ring**.
In general not every element $x \in R$ has a multiplicative inverse. We define the special class of elements with inverses the **units** of R and we denote x^{-1} to denote the unique inverse of a unit x.
A (not necessarily commutative) ring in which every nonzero element is a unit is a **division ring**. A commutative ring for which every nonzero element is a unit is a **field**.

Remark. Technically, a ring need not have a multiplicative identity, but almost all of them will be equipped with one. Sometimes we denote a ring without identity to be a rng (no i).

Example. $\diamond$