Algebraic Theory I

Thomas Fleming

October 19, 2021

Contents

Lecture 24: Summary of Group Theory

Mon 18 Oct 2021 18:06

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

Theorem 0.1 (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 0.1. We denote the following sets

$$\begin{aligned}
G_x &= \{g \in G : x^g = x\} \\
G_X &= \{g \in G : x^g = x \forall x \in X\} \\
N_G(X) &= \{y \in G : yXy^{-1} = X\} \\
Z_G(X) &= \{y \in G : yxy^{-1} = x \forall\ x \in X\} \\
[X, Y] &= \{xyx^{-1}y^{-1} : x \in X, y \in Y\}
\end{aligned}$$

$\mathscr{O}_X = \{x^g : x \in X, g \in G\}$.

Definition 0.2 (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 0.3. A group action is faithful if it has trivial kernel.

Theorem 0.2. $G_{x^g} = gG_xg^{-1}$.

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

Theorem 0.3. $x^g = x^h$ if and only if x, y are in a common left G_x-coset.

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

Theorem 0.4 (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. □

Definition 0.4. 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 0.5. 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. □

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

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 0.6 (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 $\text{ord}\left(x^{|H|/p}\right) = p$, 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.

□

Theorem 0.7. 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. □

Theorem 0.8. 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. □

Theorem 0.9 (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 $n_p \equiv 1 \mod p$.

□

Theorem 0.10. A group of order p^2 is abelian.

Theorem 0.11. 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. □

Theorem 0.12. 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 $xy = yx' = x'y' = xy \Rightarrow xy = yx$. □

Definition 0.5. $(x, y)(a, b) = (xa^y, b)$

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

Theorem 0.13. 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 0.14. $NH \simeq N \rtimes_\alpha H$ if $\alpha : h \mapsto hxh^{-1}$.

Lecture 23: Free Groups (6)

Mon 18 Oct 2021 11:26

Recall, we defined the rank of a free group to be the size of its underlying alphabet. In order to ensure this was well defined, we needed to prove the following claim

Proposition 0.1. If $F(X) \simeq F(Y)$ via the isomoprhism φ, then $|X| = |Y|$.

Proof. Denote $G = F(X)$ and $G' = F(Y)$ and let $H = \left\langle g^2 : g \in F(X) \right\rangle$. We know this to be a characteristic subgroup by the homework problem. Hence, we have $H \trianglelefteq F(X)$. Consider G/H and note that $\varphi(H) = H' = \{h^2 : h \in F(Y)\}$.

Since, $\varphi(H) = \{\varphi(g^2) = \varphi(g)^2 : g \in F(X)\} = \{h^2 : h \in \varphi(F(X)) = F(Y)\}$. Hence, $G/H \simeq \varphi(G)/\varphi(H) \simeq G'/H'$ as φ is an isomorphism. We show that $G/H \simeq \underbrace{\mathbb{Z}/2\mathbb{Z} + \ldots + \mathbb{Z}/2\mathbb{Z}}_{|X| \text{ times}} \simeq (\mathbb{Z}/2\mathbb{Z})^{|X|}$.

First, note $xyxy = (xy)^2 = 1$ in G/H for all $x, y \in G/H$ by definition. Hence, $xyx^{-1}y^{-1} = xyxy$ as $x^2 = y^2 = 1$ for every $x, y \in G/H$. Hence, $xyx^{-1} = y$, so G/H is an abelian 2-group. Now, note that $\langle xH : x \in X\rangle = G/H$ and denote $xH = \overline{x}$ for each $x \in G$. Then $G/H = \{\overline{x} : x \in X\}$. Note that an element $g \in G/H$ has

$$\overline{x_1 x_2} \ldots \overline{x_\ell}$$

with all $\overline{x_1}, \ldots, \overline{x_\ell}$ being distinct.
Suppose $\overline{x_1} \ldots \overline{x_\ell} = \overline{y_1} \ldots \overline{y_s}$. We claim that $\ell = s$ and there is a permutation such that $x_i = y_i$ for all i. Suppose the contrary, so WLOG $x_1 \notin \{y_1, \ldots, y_\ell\}$. Hence, $w = \overline{x_1} \ldots \overline{x_\ell y_s} \ldots \overline{y_1} = 1$, so $w \in H$. Furthermore, we find $V_{x_1}(w) = 1$. But, for any generator $g^2 \in H$, we have $V_{x_1}(g^2) = 2n$ for some $n \geq 0$. So, we must have $V_{x_1}(w) = \sum_{i=1}^{m} V_{x_1}(g_i^2) = 2\hat{n}$ for generators g_i and some $\hat{n} \geq 0$. $\lightning$.
Hence there is a unique representation in G/H.
This shows that

$$\begin{aligned} G/H &= \langle \overline{x} : x \in X \rangle \\ &= \bigoplus_{x \in X} \langle x \rangle \end{aligned}$$

with each $\langle \overline{x} \rangle \in \mathbb{Z}/2\mathbb{Z}$ as $\operatorname{ord}(\overline{x}) = 2$. Hence,

$$G/H = \sum_{i=1}^{|X|} \mathbb{Z}/2\mathbb{Z}.$$

We know this to be a vector space over a 2 element field, $\mathbb{F}_2$, consisting of elements $(\varepsilon_x)_{x \in X} \mapsto \prod_{x \in X} \overline{x}^{\varepsilon_x}$ with almost all (finitely many) $\varepsilon_x = 0$ and $\dim_{\mathbb{F}_2}(G/H) = |X|$ as $\overline{X}$ is a basis for G/H. As $G/H \simeq G'/H'$, we see $\dim_{\mathbb{F}_2}(G'/H') = |X|$. But by the same argument, we see $\dim_{\mathbb{F}_2}(G'/H') = |Y|$ as well. Hence, $|X| = |Y|$. $\square$

Remark. If $F \simeq F(X)$ is free and $H \leq F$, then H is free. Similairly, if $|F : H| = m < \infty$ then $\operatorname{Rank}(H) = \operatorname{Rank}(F) \cdot m + (1 - m)$ for some $m \geq 0$.

Midterm

The test Wednesday will be proofs of ~ 4 (choose 2 out of 4) theorems, propositions, lemmas we proved in class. There will be a second part consisting of short answers consisting of applying theorems, lemmas, ... from class to prove simple or concrete results.