Algebra III: Groups

MATH 341

Steven Xia

March 1, 2023

Contents

1 Assorted Introductions

Author's Remark

This section is weird because most of the material was already covered either in MATH 340 or MATH 440. There is missing material, and I am simply too lazy to add it.

Theorem 1.1 (Internal Characterization). *For $G_1, G_2 \subseteq G$ groups, $G \cong G_1 \times G_2$ if and only if all the following apply:*

(i) $G = \{g_1 g_2 : g_1 \in G_1, g_2 \in G_2\}$,

(ii) $G_1 \cap G_2 = \{e_G\}$, *and*

(iii) $g_1 g_2 = g_2 g_1$ *for all* $g_1 \in G_1$ *and* $g_2 \in G_2$.

Proof. Tedious rule checking. $\square$

Theorem 1.2 (Cayley). *Every finite group of order n is isomorphic to some subgroup of S_n.*

Proof. Let G be a finite group of order n. Define $\phi : G \to S_n$ as $\phi(\mathrm{g}) = \sigma_g$ where $\sigma_g(h) = gh$, an isomorphism. $\square$

Theorem 1.3 (Lagrange). *Let $H \subseteq G$ be groups (not necessarily finite). Then, $|G| = [G : H]|H|$ (with cardinality if infinite).*

Proof. We prove only for the finite case, by seeing that cosets partition the group, and that all cosets are of the same size. $\square$

Theorem 1.4 (Cauchy). *Let G be a finite group of order n. If a prime p divides n, there exists an element of order p.*

Proof. Define $X = \{(x_1, \dots, x_p) \in G^p : x_1 \cdots x_p = e\}$ and see that x_p is determined entirely by the choices of $x_1, \dots, x_{p-1}$. Since $x_1, \dots, x_{p-1}$ can be chosen arbitrarily, $|X| = n^{p-1}$.

Let $\mathbb{Z}_p$ act on X by cyclic permutation of the p-tuple. Since stabilizers are subgroups, the orbit-stabilizer theorem says that all orbits of X are size either 1 or p. We note an orbit of some $(x_1, \dots, x_p) \in X$ is size 1 if and only if $x_1 = \cdots = x_p$, id est, x_1 is of order p or $x_1 = e$. Finally, since $|X|$ is a multiple of p, the class equation says there must be at least p elements of with an orbit of size 1, hence $p - 1$ elements of order p. $\square$

Theorem 1.5. *Let $H \subseteq G$ be a normal subgroup. Then, the quotient set G/H has a group structure.*

Proof. Tedious rule checking. $\square$

Theorem 1.6. *A group $H \subseteq G$ is normal if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.*

Proof. The "only if" is trivial, so we prove the "if" direction by showing $gHg^{-1} \supseteq H$. We see $gHg^{-1} \subseteq H \implies g^{-1}Hg \subseteq H$. For some $ghg^{-1} \in H$, we have $ghg^{-1} = h' \iff h = g^{-1}h'g$ for some $h' \in H$. But then $g^{-1}h'g \in g^{-1}Hg$ so $h = gh'g \in H$. $\square$

Theorem 1.7. *Subgroups of index 2 are normal.*

Proof. Let $H \subseteq G$ be a subgroup of index 2. Then, the left cosets of H are H, gH and the right cosets of H are H, Hg, so $gH = Hg$. $\square$

Theorem 1.8 (First Isomorphism). *Let $\phi : G \to H$ be a surjective homomorphism. Then, $H \cong G/\ker(\phi)$.*

Proof. Tedious rule checking. $\square$

Corollary 1.8.1. *Let $\phi : G \to H$ be a homomorphism. Cosets of $\ker(\phi)$ contain all values mapping to some element in the codomain.*

Remark 1.1. Normal subgroups of a group are exactly all possible kernels of homomorphisms from that group.

2 Alternating Groups

Definition 2.1. A **transposition** in a symmetric group is a cycle with support size 2.

Remark 2.1. Every permutation can be written (not uniquely) as a product of transpositions.

Theorem 2.1. *For some permutation σ, any writing of σ as a product of transpositions has the same parity of the number of factors.*

Remark 2.2. The parity of a permutation σ is the number of transpositions in a 2-cycle factorization of σ.

Definition 2.2. The **alternating group** on n elements, A_n, is the set of even permutations.

Definition 2.3. The **cycle structure** of a permutation σ is the list of cycle lengths in σ sorted in non-increasing order.

Theorem 2.2 (Conjugation). *Every conjugate of a permutation has the same cycle structure.*

Theorem 2.3. *Every pair of permutations of the same cycle structure is conjugates in S_n.*

Definition 2.4. A group is **simple** if the only normal subgroups are the trivial group or itself.

Theorem 2.4. *The group A_n is normal if and only if $n \neq 4$.*

3 Sylow Theorems

Definition 3.1. For prime p, a p-**group** is one which only contains elements of order a power of p.

Theorem 3.1. *A finite group is a p-group if and only if it is of order a power of p.*

Theorem 3.2. *Let G be an abelian group with $|G| = p^n m$ where* $\gcd(p, m) = 1$. *Defining P as all elements of order a power of p and M as all other elements, we see $G \cong P \times M$.*