GROUPS

ADAM KELLY (AK2316@CAM.AC.UK)

1. Basic Results

Theorem 1.1 (Lagrange)**.** *Let G be a finite group, and let $H \leq G$. Then $|G| = |H||G : H|$, where $|G : H|$ is the* index *of H in G, the number of left cosets.*

Theorem 1.2 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism. Then $G/\ker\phi \cong \operatorname{img}\phi$.*

Theorem 1.3 (Second Isomorphism Theorem)**.** *Let $H \leq G$ and $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$ and $H/(H \cap N) \cong HN/N$.*

Theorem 1.4 (Third Isomorphism Theorem)**.** *Let $N \leq M \leq G$ such that $N \trianglelefteq G$ and $M \trianglelefteq G$. Then $M/N \trianglelefteq G/N$ and $(G/N)/(M/N) \cong G/M$.*

Theorem 1.5 (Correspondence Theorem)**.** *Let $N \trianglelefteq G$. Then the subgroups of G/N are in bijective correspondence with subgroups of G containing N.*

2. Simple Groups

Definition 2.1. A group is *simple* if $\{e\}$ and G are its only normal subgroups.

Lemma 2.2. *The only simple abelian group if C_p for a prime p.*

Lemma 2.3. *If G is a finite group, then G has a* composition series

$$1 \cong G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

where each quotient G_{i+1}/G_i is simple.

Proof Sketch. Induct on $|G|$. Let G_{n-1} be a normal subgroup of largest possible order not equal to $|G|$. Then G/G_{n-1} exists, and it's simple by the correspondence theorem. □

3. Simplicity of the Alternating Group

Lemma 3.1. *A_n is generated by 3-cycles.*

Lemma 3.2. *If $n \geq 5$, all 3-cycles are conjugate in A_n.*

Theorem 3.3. *A_n is simple for $n \geq 5$.*

Proof Sketch. Let N be normal and nontrivial, and let $\sigma \in N$. We then consider $\sigma^{-1}\delta^{-1}\sigma\delta$ for a given δ.

- *Case 1.* σ contains a cycle of length $r \geq 4$.

  Write $\sigma = (1\ 2\ \cdots\ r)\tau$, and let $\delta = (1\ 2\ 3)$. Then we get $(2\ 3\ r) \in N$.

Date: June 7, 2022.

- *Case 2.* σ contains two 3-cycles.

  Again write $\sigma = (1\ 2\ 3)(4\ 5\ 6)\tau$. Then let $\delta = (1\ 2\ 4)$, and we get $(1\ 2\ 4\ 3\ 6)$, which is the first case.

- *Case 3.* σ contains two 2-cycles.

  Write $\sigma = (1\ 2)(3\ 4)\tau$. We then repeatedly perform our process for δ in $\{(1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 3),\ (2\ 3\ 5)\}$ (in order), operating on our result. We then get $(2\ 5\ 3)$.

In each case we get a 3 cycle, and in the last case, σ contains a 3 cycle but then (by considering powers of σ) we get a 3-cycle as required. $\square$

4. p-Groups

Definition 4.1. A finite group G is a p-group if $|G| = p^n$ where p is a prime.

Theorem 4.2. *If G is a p-group then $Z(G)$ is non-trivial.*

Proof. For $g \in G$, we have $|\mathrm{ccl}_G(g)| \cdot |C_G(g)| = |G| = p^n$. So each conjugacy class has size that is a power of p. Since G is a union of it's conjugacy classes,

$$\begin{aligned} |G| &\equiv \#(\text{ conj. classes of size } 1) \pmod{p} \\ \implies 0 &\equiv |Z(G)| \pmod{p}. \end{aligned}$$

In particular, $|Z(g)| > 1$. $\square$

Theorem 4.3. *Let G be a p-group of order p^n. Then G has a subgroup of order p^r for all $0 \leq r \leq n$.*

Proof. We have a composition series $1 \equiv G_0 \lhd \cdots G_m = G$ with G_i/G_{i-1} simple. Each of these is a p-group and is thus isomorphic to C_p. $\square$