Group Theory

Kenji Nakagawa

January 7, 2021

Introduction

This is just a list of important results in elementary group theory. By no means comprehensive, and many theorems lack proof sketches. As an added note, if the proof is trivial, then it's omitted, but in the case that it takes significant effort (or I simply forgot), it's prefaced by an asterisk.

1 Theorems

Proposition 1

If N and M are normal subgroups of G, then NM is also normal in G.

Corollary 2

If M is a normal subgroup of G/N, then M extends to the normal subgroup NM of G.

Theorem 3

(*) For odd primes p, $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \cong \mathbb{Z}_{p^k - p^{k-1}}$ and $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-2}}$.

Proposition 4

$[G : C(a)] = |\operatorname{cl}(a)|$.

Theorem 5

(*) (Class equation) Let g_i denote representatives of conjugacy classes outside of the center. Then, $|G| = |Z(G)| + \sum [G : C(g_i)]$.

Corollary 6

Any p-group has nontrivial center.

Proof. From the class equation, we have that $|G|$ and each of the $[G : C(g_i)]$ is a multiple of p, and since $e \in Z(G)$, we have that $|Z(G)|$ is a nontrivial multiple of p. □

Theorem 7

(*) (N/C Theorem) For any subgroup H, $N(H)/C(H)$ is isomorphic to some subgroup of $\operatorname{Aut} H$.

Theorem 8

(*) The Sylow theorems state that if $|G| = p^k \cdot m$ where $p \nmid m$, there exists a Sylow $p-$subgroup of G of order p^n. The number of such subgroups, n_p satisfies $n_p \cong 1 \bmod p$ and $n_p = |G : N(H)| \mid |G|$ where H is any $p-$subgroup.

Corollary 9

If $n_p = 1$, then the unique Sylow $p-$ subgroup is in fact normal.

Theorem 10

(*) If $G/Z(G) \cong \mathbb{Z}_n$, then G is in fact abelian.

Theorem 11

(*) There does not exist any simple group whose order is twice an odd number.

Theorem 12

(*) (Embedding Theorem) If H is a subgroup of G, then the cosets of H induce a group action $\varphi : G \to S_{[G:H]}$. If G is simple, then $|G|$ divides $|A_{[G:H]}| = \frac{[G:H]!}{2}$.

Theorem 13

(*) (Index Theorem) Let H be any subgroup of the simple group G. Then, $|G|$ divides $[G : H]!$

Corollary 14

If G is simple, then $|G|$ divides $n_p!$.

Proof. Let H be any Sylow $p-$subgroup, then apply the index theorem to $N(H)$. □

Proposition 15

Let p be the smallest prime dividing $|G|$, then if there exists a subgroup H of index p, then G is not simple.

Proof. □