PARTIAL CONVERSES OF LAGRANGE'S THEOREM

TYLER ZHU

ABSTRACT. In this paper, we will discuss some variants of the converse to Lagrange's Theorem, namely that if m divides the order of a group G then G has a subgroup of order m, and see many fascinatingly related results.

1. Overview

In 1771, Joseph-Louis Lagrange stated a theorem about symmetric groups of polynomials in his *Réflexions sur la résolution algébrique des équations*, but did not prove it. In 1801, Carl Friedrich Gauss proved Lagrange's theorem for $\mathbb{Z}_p^\times$, the multiplicative group modulo p, and in 1844, Augustin-Louis Cauchy proved the theorem for the symmetric group S_n. It was not until 1861 that Camille Jordan finally proved Lagrange's theorem for permutation groups, which by Cayley's Theorem proves it for all groups. With the modern machinery of cosets, the proof of the theorem is but a simple application of this concept.

Theorem 1 (Lagrange's Theorem)**.** *Let G be a group, and H be a subgroup of G. Then, the order of H divides the order of G, or $|H| \mid |G|$.*

Proof. By considering the cosets formed by H, one notes that these cosets partition G into equal cosets of size $|H|$, from which the theorem follows. □

It is natural to ask if the converse of this theorem is true. We will cover topics in roughly the following order:

(1) Subgroups and Generators, specifically the center of a group and the commutator subgroup.
(2) Normal subgroups, Quotient Groups, and the Isomorphism Theorems.
(3) Ascending Central Series and Nilpotent Groups
(4) Derived series and Subnormal Series.

It is suggested that one proceeds in this order when reading this paper, as later sections will rely heavily on material, or at least ideas, presented in earlier sections. One should at least skim the sections that are review and then proceed to later sections.

2. Notation

We define much of the notation used in this paper here for your reference. Some of the notation is not developed until later sections, so do not worry if you don't understand them right now.

Let G be a group. Then we denote H a subgroup of G by $H \leqslant G$. If H is also a normal subgroup of G, then we write $H \lhd G$, and denote the quotient group of G modded out by H as G/H.

Date: September 18, 2017.

3. Subgroups and Generators

4. Quotient Groups and the Isomorphism Theorems

This is a most important theorem, and will be used later on in developing ascending central series.

Theorem 2 (Theorem I.5.11 in [1]). *If $f : G \to H$ is an onto homomorphism of groups, then the assignment $K \mapsto f(K)$ defines a one-to-one correspondence between the set $S_f(G)$ of all subgroups K of G which contain* $\ker f$ *and the set $S(H)$ of all subgroups of H. Under this correspondence normal subgroups correspond to normal subgroups.*

Exercise 4.1 (Exercise I.5.16 in [1])**:** Prove that if $f : G \to H$ is a homomorphism, H is abelian, and N is a subgroup of G containing $\ker f$, then N is normal in G.

5. Nilpotent Groups

5.1. **Ascending Central Series.** In this section, we will finally be able to see what an ascending central series is, as well as the definition of a nilpotent group.

Suppose we have a group G. Then the center of the group, $Z(G) = \{z \in G | gzg^{-1} = z \forall g \in G\}$, is a normal subgroup of G. [1] Thus, if we let $Z_1 = Z(G)$, then

$$Z_1 = Z(G) \lhd G.$$

This means we can mod out by Z_1 to obtain the quotient group G/Z_1, which induces the canonical projection $\varphi_1 : G \to G/Z_1$ that sends $g \mapsto gZ_1$. However, since G/Z_1 is a group, its center, which we will denote $W_2 = Z(G/Z_1)$, is also a normal subgroup (of G/Z_1). Hence, we have that $W_2 \lhd G/Z_1$.

Now, since φ_1 is an onto[2] homomorphism, we can apply Theorem 2 to φ_1. Since W_2 is a subgroup of G/Z_1, it has some pre-image, or more formally a pullback, under the assignment $K \mapsto \varphi_1(K)$ where $K \leq G$. Let us pullback W_2 under φ_1 to a subgroup $Z_2 \leqslant G$. Theorem 2 also tells us that $\ker \varphi_1 \subseteq Z_2$, and that $Z_2 \lhd G$. However, $\ker \varphi_1$ is precisely just Z_1! Hence, we have that $Z_1 \leqslant Z_2 \lhd G$. Combining this with the fact that $Z_1 \lhd G$, we get that

$$Z_1 \lhd Z_2 \lhd G$$

because $Z_1 \lhd G$ implies that that the elements of Z_1 should be normal in any subgroup of G.

We can repeat this process again and again to get something that looks like this:

$$\{e\} \lhd Z_1 \lhd Z_2 \lhd Z_3 \lhd \cdots \lhd G.$$

This is called the **ascending central series** of the group G. If $Z_n = G$ for some n, then G is said to be **nilpotent**. How could this not happen? This does not happen when at some point, the Z_i end up being equal to each other, but not necessarily equal to G! There are examples of this later on.

Nilpotent groups turn out to have a ton of nice properties. One example is a complete converse to Lagrange's theorem.

Lemma 3. *If G is a finite nilpotent group and m divides $|G|$, then G has a subgroup of order m.*

[1] Straightforward to show, as we did in Section 2

[2] In other words, all of G maps into G/Z_1, so that every $z \in G/Z_1$ has a preimage.

Proof. See [1] page 101. First prove that a finite group is nilpotent if and only if it is a direct product of its Sylow subgroups. The lemma follows by breaking up m into its prime powers and applying the First Sylow Theorem. □

5.2. **Examples.**

Example 5.1: Let us consider the group $\mathbb{Z}_7$ under addition. The center, $Z_1 = Z(\mathbb{Z}_7)$, is the set of elements of $\mathbb{Z}_7$ that commute with everything in the group. Since $\mathbb{Z}_7$ is abelian however, everything commutes with everything else. Hence, $Z_1 = Z(\mathbb{Z}_7) = \mathbb{Z}_7$, and thus $\mathbb{Z}_7$ is nilpotent.

Example 5.2: The previous example actually hints that if G is *any* abelian group, then G is nilpotent. This is true, for the center $Z_1 = Z(G)$ will be all of G because G is abelian, and hence $Z_1 = G$, which is precisely the definition of nilpotent. This also means that it is only interesting to study nonabelian groups for nilpotence, so all of the following examples will be of nonabelian groups.

Example 5.3: Let us consider the Discrete Heisenberg Group

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{Z} \right\},$$

named after the German physicist Werner Heisenberg. There is a similar group called the Continuous Heisenberg Group, where $a, b, c \in \mathbb{R}$, which has applications in one-dimensional quantum mechanical systems.

Example 5.4: Now we will present an example of a nonabelian group that is not nilpotent. Consider the alternating group A_5. Recall that A_5 is simple, which means that it has no proper normal subgroups. Hence, the only normal subgroups of A_5 are $\{e\}$ and A_5 itself. Now consider $Z(A_5) = Z_1$. The center of always abelian, so Z_1 must be abelian and normal in A_5. However, A_5 is nonabelian, so therefore $Z_1 = \{e\}$. This means that the ascending central series for A_5 is

$$\{e\} \lhd \{e\} \lhd \cdots \lhd \{e\} \lhd A_5,$$

where $\{e\} = Z_1 = Z_2 = \cdots$. Hence, A_5 is not nilpotent.

Example 5.5: The only special property of A_5 was that it was simple and nonabelian. Therefore, one can argue similarly as we did for A_5 that any group G that is simple and nonabelian cannot be nilpotent. Groups with these properties of small order are quite rare in fact. There are (up to isomorphism) only two nonabelian simple groups of order less than 200, namely A_5 and a subgroup of S_7 of order 168 (see [1] pg. 111).

6. Other Series

6.1. **Derived Series.**

Derived Series are to the commutator subgroup as what ascending central series are to the center of a group.

6.2. **Subnormal Series.**

Subnormal Series are essentially a generalization of what we have previously with the derived series and ascending central series.

References

[1] Thomas Hungerford, *Algebra*. Springer-Verlag New York, 1974.