The Sylow Theorems

A Partial Converse to Lagrange's Theorem

Jasmine Tom

University of California, Santa Cruz

Directed Reading Program, Spring 2022

June 1, 2022

Elementary Group Theory

Definition

- A binary structure $(G, *)$ is called a **group** if it satisfies the following axioms:
  - $x * (y * z) = (x * y) * z$, for all $x, y, z \in G$,i.e., $*$ is associative.
  - There exists an identity element denoted by 1_G such that $g * 1_G = g = 1_G * g$.
  - For every element $g \in G$, there exists an element $g^{-1} \in G$, called the inverse of g, such that $g * g^{-1} = 1_G = g^{-1} * g$.
- A group G is called an **abelian** group if $x * y = y * x$, for all $x, y \in G$, i.e., $*$ is commutative. Otherwise, we call G nonabelian.
- The number of elements in G is called the **order** of G, and it is denoted by $|G|$.
- A group is called a **finite group** if its order is finite.

Elementary Group Theory

Definition

- A subset H of G is a **subgroup** of G if it has the following properties:
  - $1_H \in G$
  - $x * y \in H$, for any $x, y \in H$, i.e., H is closed under the binary operation of G.
  - For all $h \in H$ also h^{-1} lies in H.
- Let G be a group and let $g \in G$. Then

$$\{g^n | n \in \mathbb{Z}\}$$

is a subgroup of G. It is called the **subgroup generated** by g and is denoted by $\langle g \rangle$.

Lagrange's Theorem

Theorem.
If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

Sylow's Theorem

Definition.

Let G be a group and let p be a prime.

- A group of order p^k for some $k \geq 0$ is called a **p-group**.
- If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a **Sylow p-subgroup** of G.
- The set of Sylow p-subgroups of G is denoted by $Syl_p(G)$ and the number of Sylow p-subgroups in G is denoted by n_p.

Sylow's Theorem

Theorem.
Let G be a group of order $p^{\alpha}m$, where p is a prime not dividing m.

- Sylow p-subgroups of G exist,i.e., $Syl_p(G) \neq \varnothing$.
- If P, Q are Sylow p-subgroups of G, then there exists $g \in G$ such that $Q = gPg_{-1}$, i.e., P and Q are G-conjugate.
- $n_p \equiv 1 \pmod{p}$.

Applications of Sylow's Theorem

Definition.

- A subgroup N of a group G is called **normal** if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$.
- A nontrivial group G is called **simple** if the only normal subgroups of G are 1 and G.

Applications of Sylow's Theorem

Theorem

There is a list consisting of 18 (infinite) families of simple groups and 26 simple groups not belonging to these families (the *sporadic* simple groups) such that every finite simple group is isomorphic to one of the groups in this list.

References

D. Dummit, R. Foote (2004)
Abstract Algebra. Third Edition. John Wiley & Sons, Inc., 2004.

Thank you for listening!

Any questions?

Special thanks to John McHugh & DRP Organizers :)