Subgroups, Lagrange's Theorem and its applications

Tim Hsiung

January 25, 2026

Outline

- Subgroups
- How to construct subgroups
- Cyclic groups and order of elements
- Lagrange's Theorem
- Use Lagrange's theorem to prove Fermat's Little Theorem

This slide will cover some of Dummit Foote Chapter 2, and section 3.2.

Basic definitions and properties of subgroups

Definition 0.1 (Subgroups): A subset H of G is a subgroup of G if it is itself a group under the operation of G.

More precisely,

- H is non-empty.
- (Closed under the binary operation) For all $a, b \in H$, we have $ab \in H$.
- (Closed under the inversion) For all $a \in H$, we have $a^{-1} \in H$.

Example: The trivial subgroup $\{e\}$ is a subgroup of any group G.

Example: Any group G is a subgroup of itself.

Example (Center): The center $Z(G) := \{g \in G \mid gx = xg \text{ for all } x \in G\}$ of a group G is a subgroup of G.

Theorem 0.1 (The subgroup criterion): Let G be a group and $H \subseteq G$, then H is a subgroup of G if and only if

- H is non-empty.
- $ab^{-1} \in H$ for all $a, b \in H$.

Proof: The $(\Rightarrow)$ direction is trivial.

For the $(\Leftarrow)$ direction, we need to verify that H is closed under the inversion.

Let $a \in H$. Then $e = aa^{-1} \in H$ by the assumption. Therefore, $a^{-1} = ea^{-1} \in H$ by the closure of H under the binary operation.

Therefore, H is a subgroup of G. $\square$

Theorem 0.2: Furthermore, if H is finite, then it is sufficient to check that H is non-empty and closed under the binary operation.

Proof: Let $a \in H$. We now verify that $a^{-1} \in H$.

Consider the set $\{a^n \mid n \in \mathbb{N}\} \subseteq H$.

Hint: this is a finite set. $\square$

Theorem 0.3: Let $\{H_\alpha\}_{\alpha \in A}$ be a collection of subgroups of G. Then

$$\bigcap_{\alpha \in A} H_\alpha$$

is a subgroup of G.

Proof: Use the subgroup criterion. $\square$

The above theorem shows that the intersection of subgroups is also a subgroup.

How about the union of subgroups? How about the product of subgroups?

Exercise: Show that $H \cup K \leq G$ if and only if $H \subseteq K$ or $K \subseteq H$.

Exercise: Let $HK := \{hk \mid h \in H, k \in K\}$. Show that $HK \leq G$ if and only if $HK = KH$.

Generated subgroups

Definition 0.2 (Subgroup generated by a subset): Let $S \subseteq G$. The subgroup "generated" by S is the smallest subgroup of G that contains S. We denote it by $\langle S \rangle$.

More precisely,

$$\langle S \rangle := \bigcap_{H \leq G, S \subseteq H} H$$

This is similar to the concept of "span" in linear algebra.

Theorem 0.4 (Another definition of the subgroup generated by a subset):

Let $S \subseteq G$. Then $\langle S \rangle$ is the set of all finite products of elements of S and their inverses. More precisely, let $\overline{S} = \{s_1 s_2 ... s_n \mid n \in \mathbb{N}, s_i \in S \text{ or } s_i \in S^{-1}\}$, then $\langle S \rangle = \overline{S}$.

If you are still familiar with linear algebra, recall that the span of a set of vectors is also the set of all linear combinations of the vectors in the set. The concepts are similar.

Proof: First, use the subgroup criterion to show that $\overline{S} \leq G$.

Then verify that $\langle S \rangle = \overline{S}$:

- $\langle S \rangle \leq \overline{S}$: because $\overline{S}$ is a subgroup containing S.
- $\overline{S} \leq \langle S \rangle$: observe that each element of $\overline{S}$ is a finite product of elements of S and their inverses.

$\square$

Exercise: Find the generated subgroup of the following sets:

- $S = \{3\}$ in $\mathbb{Z}$
- $S = \{r\}$ in D_8
- $S = \{r^2\}$ in D_8
- $S = \{s\}$ in D_8
- $S = \{sr\}$ in D_8
- $S = \{s, r^2\}$ in D_8
- $S = \{j\} \in Q_8$
- $S = \{-1\} \in Q_8$

Definition 0.3 (Cyclic groups): A group G is cyclic if there exists $g \in G$ such that $G = \langle g \rangle$. The element g is called a generator of G.

Definition 0.4 (Cyclic subgroups): A subgroup H of G is cyclic if there exists $g \in G$ such that $H = \langle g \rangle$.

Example: $\mathbb{Z} = \langle 1 \rangle$ is cyclic. The subgroup $\langle r \rangle$ of D_8 is cyclic. The subgroup $\langle j \rangle$ of Q_8 is cyclic.

Exercise: Is $\mathbb{Q}$ cyclic? Why or why not?

Order of elements and groups

Definition 0.5 (Order of an element): The order of an element $g \in G$ is the smallest positive integer n such that $g^n = e$. We denote it by $|g|$. If no such n exists, we say that g has infinite order or $|g| = \infty$.

Exercise: Find the order of the elements in the following groups:

- $1 \in \mathbb{Z}$
- $r, r^2, r^3, s, sr \in D_8$

Exercise: Let $g \in G$. Show that $|g| = |g^{-1}|$.

Exercise: Let G be a group such that $|g| = 2$ for all $g \in G$. Show that G is abelian.

Exercise: Let $G := \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{N}\} \subseteq \mathbb{C}^\times$. Show that G is a group under multiplication. Show that every element of G has finite order, but G is infinite.

Definition 0.6 (Order of a group): The order of a group G is the number of elements in G. We denote it by $|G|$.

Theorem 0.5: Let $g \in G$. Then $|g| = |\langle g \rangle|$.

Exercise: Find the order of the generated subgroups in the previous exercise.

Lagrange's Theorem

Theorem 0.6 (Lagrange's Theorem): Let G be finite and $H \leq G$. Then $|H|$ divides $|G|$.

Lagrange's Theorem is a very important theorem in group theory. It tells us that the order of a subgroup divides the order of the group.

Exercise: Verify Lagrange's Theorem with the groups D_8, Q_8.

Exercise: Let G be a group of prime order, then the only subgroups of G are $\{e\}$ and G itself. Furthermore, G must be cyclic.

To prove this theorem, we will need the concept of **cosets**.

Cosets

Definition 0.7 (Cosets): Let $H \leq G$, then we denote G/H "the set of (left) cosets"

$$G/H := \{gH \mid g \in G\}$$

where $gH := \{gh \mid h \in H\}$.

Exercise: Find the cosets of the subgroups $\langle r \rangle, \langle s \rangle$ in D_8.

Note: cosets are generally not subgroups!

Theorem 0.7: Let $H \leq G$ and $a, b \in G$. Then either $aH = bH$ or $aH \cap bH = \emptyset$.

Proof: Suppose $aH \cap bH \neq \emptyset$. Then there exists $h_1, h_2 \in H$ such that $ah_1 = bh_2$. Then $a = bh_2h_1^{-1}$. Therefore, $aH = (bh_2h_1^{-1})H = bH$. $\square$

Theorem 0.8: All the cosets of H in G have the same size.

Proof: Let $a \in G$ and consider the map $\varphi_a : H \to aH$ defined by $\varphi_a(h) = ah$. This map is bijective (you can verify 1-1 by cancellation law). Therefore, the size of H is the same as the size of aH. Use this to show that all the cosets of H in G have the same size. □

Definition 0.8 (Index of a subgroup): The index of a subgroup H in G (not necessarily finite) is the number of cosets of H in G. We denote it by $[G : H]$.

Corollary 0.8.1:

- G/H forms a partition of G.
- (Lagrange's Theorem) $|G/H| = \frac{|G|}{|H|} = [G : H]$.

Exercise: Let $H \leq G$. Find the index of H in G for the following groups:

1. $H = 5\mathbb{Z}, G = \mathbb{Z}$
2. $H = \mathbb{Z}, G = \mathbb{R}$
3. $H = 5\mathbb{Z}, G = \mathbb{R}$
4. $H = \mathbb{Z}, G = \mathbb{Q}$
5. $H = \mathbb{Q}, G = \mathbb{R}$

Fermat's Little Theorem

We know that Fermat's Little Theorem is important in cryptography. We will now prove it using Lagrange's Theorem.

Theorem 0.9: Let p be a prime and $a \in \mathbb{Z}$. Then $a^{p-1} \equiv 1 (\operatorname{mod} p)$.

You probably already know how to prove this theorem by letting $a = b + 1$ and then using the binomial theorem. We will now prove it using Lagrange's Theorem.

Theorem 0.10: Let $a \in G$. Then $|a| \mid |G|$.

Corollary 0.10.1: Let $a \in G$. Then $a^{|G|} = e$.

Proof of Fermat's Little Theorem: Consider the group $(\mathbb{Z}/p\mathbb{Z})^{\times} := \{1, ..., p - 1\}$. The group operation is multiplication modulo p. The order of this group is $p - 1$. $\square$

Exercise: Recall that $\varphi(n)$ is the Euler's totient function, which is the number of integers less than n that are coprime to n.

Consider the group $(\mathbb{Z}/n\mathbb{Z})^\times := \{a = 1, ..., n-1 \mid \gcd(a, n) = 1\}$. Show that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. Deduce that $m^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$ for all m coprime to n.