§3.2 Subgroups

Shaoyun Yi

MATH 546/701I

University of South Carolina

Spring 2022

Review

- Group $(G, *)$
  - i) **Closure** $\leftrightsquigarrow *$
  - ii) **Associativity** $\leftrightsquigarrow$ ( )
  - iii) **Identity**: Uniqueness by **Associativity**
  - iv) **Inverses**: Uniqueness by **Associativity**

  eg. $(\mathbf{R}^\times, \cdot)$, $(\mathrm{Sym}(S), \circ)$, $(M_n(\mathbf{R}), +_{\text{matrix}})$, $(\mathrm{GL}_n(\mathbf{R}), \cdot_{\text{matrix}})$

- Cancellation law

- Abelian group: eg. $(\mathbf{Z}_n, +_{[\ ]})$, $(\mathbf{Z}_n^\times, \cdot_{[\ ]})$

- Finite group (order) v.s. Infinite group

- Equivalence relation: *Reflexive/Symmetric/Transitive law*

  eg. Conjugacy: $x \sim y$ if $y = axa^{-1}$

Subgroup

Let G be a group, and let H be a subset of G. Then H is called a **subgroup** of G if H is itself a group, under the operation induced by G.

- Two special subgroups of any group G: 1) G; 2) *Trivial subgroup* $\{e\}$
- $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$: each group is a subgroup of the next under $+$
- $\{\pm 1\} \subseteq \mathbf{Q}^\times \subseteq \mathbf{R}^\times \subseteq \mathbf{C}^\times$: each group is a subgroup of the next under $\cdot$

$\mathbf{R}^+ := \{x \in \mathbf{R} | x > 0\}$ is a subgroup of $\mathbf{R}^\times$ under multiplication.

i) **closure:** ✓ ii) **associativity:** ✓ iii) **identity:** 1 iv) **inverses:** its inverse

$n\mathbf{Z} := \{x \in \mathbf{Z} : x = nk \text{ for } k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ under addition.

i) **closure:** ✓ ii) **associativity:** ✓ iii) **identity:** 0 iv) **inverses:** its negative

The **special linear group** over $\mathbf{R}$: $\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) | \det(A) = 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ under matrix multiplication.

i) $\det(AB) = \det(A)\det(B)$ ii) ✓ iii) I_n iv) A^{-1}, since $\det(A^{-1}) = 1$.

Two Simpler ways

Let G be a group with identity element e, and let H be a subset of G.

W1: H is a subgroup of G if and only if the following conditions hold:

i) $ab \in H$ for all $a, b \in H$; ii) $e \in H$; iii) $a^{-1} \in H$ for all $a \in H$.

That is, there is no worry about **associativity**.

Proof: ($\Rightarrow$): i) ✓ ii) Let e' be an identity element for H. To show $e' = e$.

$$e'e' = e' \quad \text{and} \quad e'e = e' \qquad \Rightarrow e'e' = e'e \qquad \Rightarrow e' = e$$

iii) If $a \in H$, then a must have an inverse $b \in H$. To show $b = a^{-1}$.

$$\text{In } G\text{, we have } ab = e = aa^{-1}. \qquad \Rightarrow b = a^{-1}$$

($\Leftarrow$): **associativity:** For $a, b, c \in H$, $(ab)c = a(bc)$ in G, so also in H. □

W2: H is a subgroup of G iff H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$

Proof: ($\Rightarrow$): Nonempty: By ii); $ab^{-1} \in H$: By i) and iii).

($\Leftarrow$): Let $a \in H$. ii) $e = aa^{-1} \in H$; iii) $a^{-1} = ea^{-1} \in H$; i) $ab \in H$ [Why?]

Example

Let H be the set of all **diagonal** matrices in the group $G = \mathrm{GL}_n(\mathbf{R})$.

Way 1: H is a subgroup of G if and only if the following conditions hold:

i) $ab \in H$ for all $a, b \in H$; ii) $I_n \in H$; iii) $a^{-1} \in H$ for all $a \in H$.

The diagonal entries of any element in H must all be nonzero. [Why?]

i) The product of two diagonal matrices is still a diagonal matrix.

ii) The identity matrix I_n is obviously a diagonal matrix.

iii) The inverse of $a \in H$ exists, and it is again a diagonal matrix.

Way 2: H is a subgroup of $G \Leftrightarrow H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$.

Nonempty: $I_n \in H$; The second condition: Easy to check.

Finite Subgroup

Let G be a group, and let H be a **finite**, nonempty subset of G. Then H is a subgroup of G if and only if $ab \in H$ for all $a, b \in H$.

Proof: $(\Rightarrow)$ ✓ $(\Leftarrow)$ By **Way 2** $\rightsquigarrow$ to show $b^{-1} \in H$ for all $b \in H$. Consider

$$\{b, b^2, b^3, \ldots\} \overset{!}{\subset} H.$$

Since $|H|$ is finite, they cannot all be distinct. There exists some repetition:

$$b^n = b^m \quad \text{for some } n > m > 0. \qquad \Rightarrow b^{n-m} = e$$

Hence $b^{-1} = b^{n-m-1} \in H$. □

Example 1 (Subgroups of S_3)

- Two Special Subgroups: S_3; $\{(1)\}$;
- Order Two: $\{(1), (12)\}$; $\{(1), (13)\}$; $\{(1), (23)\}$;
- Order Three: $\{(1), (123), (132)\}$

Cyclic Subgroup

Let G be a group, and let a be any element of G. The set

$$\langle a \rangle := \{x \in G : x = a^n \text{ for some } n \in \mathbf{Z}\}$$

is called the **cyclic subgroup generated by** a.

G is called a **cyclic group** if there exists an element $a \in G$ s.t. $G = \langle a \rangle$. In this case, a is called a **generator** of G.

Let G be a group, and let $a \in G$.

1) The set $\langle a \rangle$ is a subgroup of G.
2) If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.
   That is, $\langle a \rangle$ is the smallest subgroup that contains a.

1) i) $a^m a^n = a^{m+n} \in \langle a \rangle$; ii) $e = a^0 \in \langle a \rangle$; iii) $(a^n)^{-1} = a^{-n} \in \langle a \rangle$.

2) $a \in K \Rightarrow a^n \in K$ for all $n \in \mathbf{Z}_{>0}$; $e = a^0 \in K$; $a^{-n} = (a^n)^{-1} \in K$.

If the operation is denoted additively rather than multiplicatively: $a^n \rightsquigarrow na$

$(\mathbf{Z}, +)$ is cyclic. In fact, $\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

$\mathbf{Z} = \langle a \rangle = \{na \colon n \in \mathbf{Z}\} \quad \Rightarrow a = \pm 1$

$(\mathbf{Z}_n, +_{[\ ]}) = \langle [1] \rangle$ is cyclic. And all possible generators are $\{a \colon (a, n) = 1\}$.

$\mathbf{Z}_n = \langle [a] \rangle \Leftrightarrow [1]$ is a multiple of $[a] \Leftrightarrow [a]$ is a unit $\Leftrightarrow [a] \in \mathbf{Z}_n^{\times} \Leftrightarrow (a, n) = 1$

$(\mathbf{Z}_n^{\times}, \cdot_{[\ ]})$ is not always cyclic.

- $\mathbf{Z}_5^{\times} = \{[1], [2], [3], [4]\} = \langle [2] \rangle = \langle [3] \rangle$ is cyclic. But [4] is not a generator
- $\mathbf{Z}_8^{\times} = \{[1], [3], [5], [7]\}$ is not cyclic because $[a]^2 = [1]$ for all $[a] \in \mathbf{Z}_8^{\times}$.

Every proper subgroup of S_3 is cyclic, but S_3 is not cyclic.

Trivial Subgroup: $\{(1)\} = \langle (1) \rangle$;

Order Two: $\{(1), (12)\} = \langle (12) \rangle; \{(1), (13)\} = \langle (13) \rangle; \{(1), (23)\} = \langle (23) \rangle$;

Order Three: $\{(1), (123), (132)\} = \langle (123) \rangle = \langle (132) \rangle$;

S_3 is not cyclic since no cyclic subgroup is equal to all of S_3.

Order of an Element $a \in G$

We say a has **finite order** if there exists a positive integer n s.t. $a^n = e$.
The smallest such positive integer is called the **order** of a, denoted by $o(a)$
If $a^n \neq e$ for any positive integer n, then a is said to have **infinite order**.

Every element of a finite group must have finite order. [Why?]

i) If a has infinite order, then $a^k \neq a^m$ for all integers $k \neq m$.
ii) If a has finite order $o(a)$ and $k \in \mathbf{Z}$, then $a^k = e \Leftrightarrow o(a)|k$.
iii) If $o(a) = n$, then $a^k = a^m \Leftrightarrow k \equiv m \pmod{n}$. We have $|\langle a \rangle| \overset{!}{=} o(a)$.

i) Assume $a^k = a^m$ for $k \geq m$. $\Rightarrow a^{k-m} = e$ $\Rightarrow k - m = 0$

ii) $(\Leftarrow)$: ✓ $(\Rightarrow)$: Let $o(a) = n$. Write $k = nq + r$, where $0 \leq r < n$. Thus,

$$a^r = \cdots = e \overset{!}{\Rightarrow} r = 0 \quad \Rightarrow n|k$$

iii) $a^k = a^m \Leftrightarrow a^{k-m} = e \overset{\text{ii)}}{\Leftrightarrow} n|(k-m)$. **Claim:** $\langle a \rangle \overset{!}{=} \{e, a, \ldots a^{n-1}\} := S$

$S \subset \langle a \rangle$ by definition of $\langle a \rangle$; S is a subgroup of G & $a \in S$, so $\langle a \rangle \overset{!}{\subset} S$.

Examples

In the multiplicative group $\mathbf{C}^\times$, consider the powers of i:

$$\langle i \rangle = \{1,\ i,\ -1,\ -i\},$$

which is a cyclic subgroup of $\mathbf{C}^\times$ of order 4.

Furthermore, let $z = e^{2\pi i/n}$. We can see that

$$\langle z \rangle = \{z^k \mid k \in \mathbf{Z}\} \text{ is the set of complex } n\text{th roots of unity,}$$

which is a cyclic subgroup of $\mathbf{C}^\times$ of order n. Note that $i = e^{2\pi i/4}$.

The situation is quite different if we consider $\langle 2i \rangle$, which is infinite:

$$\langle 2i \rangle = \left\{\ldots,\ \frac{1}{8}i,\ -\frac{1}{4},\ -\frac{1}{2}i,\ 1,\ 2i,\ -4,\ -8i,\ \ldots\right\}.$$

Lagrange's Theorem

If H is a subgroup of the finite group G, then $|H|$ is a divisor of $|G|$.

Proof: Let $|G| = n$ and $|H| = m$. To show $m \mid n$. For $a, b \in G$, we define

$$a \sim b \quad \text{if } ab^{-1} \in H.$$

Then $\sim$ is an equivalence relation. (*reflexive* ✓ *symmetric* ✓ *transitive* ✓)
Let $[a] := \{b \in G : a \sim b\}$ denote the equivalence class of a. Consider

$$\rho_a : H \to [a], \quad \rho_a(h) = ha \quad \text{for all } h \in H.$$

Claim: The function ρ_a a one-to-one correspondence between H and $[a]$.

i) Well-defined: $\rho_a(h) = ha \in [a]$ since $a(ha)^{-1} = h^{-1} \in H$.

ii) one-to-one: If $\rho_a(h_1) = \rho_a(h_2)$, then $h_1 a = h_2 a$. $\Rightarrow h_1 = h_2$

iii) onto: If $b \in [a]$, then $ab^{-1} = h \in H$. $\Rightarrow b = h^{-1}a = \rho_a(h^{-1})$

It follows that each equivalence class $[a]$ has $m = |H|$ elements.

Since the equivalence classes partition G, each element of G belongs to precisely one of the equivalence classes. Thus

$$|G| = n = mt,$$

where t is the number of distinct equivalence classes. Hence $m \mid n$. □

The converse of Lagrange's theorem is false. (See an example in §3.6.)

$[a] := \{b \in G : ab^{-1} \in H\} = \{b \in G : b = ha \text{ for some } h \in H\} = Ha$

Note: $Ha = [a] \overset{!}{=} [b] = Hb$ for any $b \in [a]$.

Example 2 (Consider $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$)

1) $H = \langle (123) \rangle = \langle (132) \rangle = \{(1), (123), (132)\}$: **Two** equivalent classes

   i) H forms the first equivalence class: $H = H(1) = H(123) = H(132)$

   ii) Any other equivalence class must be **disjoint** from the first one and have the **same number of elements**, so the only possibility is

$$H(12) = \{(12), (13), (23)\} = H(13) = H(23).$$

2) $K = \langle (12) \rangle = \{(1), (12)\}$: **Three** equivalent classes

   i) K forms the first equivalence class: $K = K(1) = K(12)$

   ii) $K(13) = \{(13), (132)\} = K(132)$

   iii) $K(23) = \{(23), (123)\} = K(123)$

Two Corollaries

Corollary 3

Let G be a finite group of order n. For any $a \in G$, $o(a)|n$. In particular, $a^n = e$.

Proof: $\langle a \rangle$ is a subgroup and $|\langle a \rangle| = o(a)$. Thus $o(a)|n$ by Lagrange's thm

Euler's Theorem: $a^{\varphi(n)} \equiv 1 \pmod{n}$ if $(a, n) = 1$.

Proof: $G = \mathbf{Z}_n^\times$ with $|G| = \varphi(n)$: For any $[a] \in G$, we have $[a]^{\varphi(n)} = [1]$.

Corollary 4

Any group G of prime order is cyclic.

Proof: Let $|G| = p$, where p is a prime number. Let $a \in G, a \neq e$. Then

$o(a) = |\langle a \rangle| \neq 1$, and so $|\langle a \rangle|$ must be p. [Why?]

This implies that $\langle a \rangle = G$, and hence G is cyclic. □