§3.2 Subgroups

Shaoyun Yi

MATH 546/701I

University of South Carolina

Summer 2021

Review

- Group $(G, *)$ $\begin{cases} \text{i)} & \text{Closure} \leftrightsquigarrow * \\ \text{ii)} & \text{Associativity} \leftrightsquigarrow \cancel{(\ )} \\ \text{iii)} & \text{Identity: Uniqueness by Associativity} \\ \text{iv)} & \text{Inverses: Uniqueness by Associativity} \end{cases}$

  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. $(\mathbf{Z}, +)$, $(\mathbf{Z}_n, +_{[\ ]})$, $(\mathbf{Z}_n^\times, \cdot_{[\ ]})$

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

- Conjugacy: $x \sim y$ if $y = axa^{-1} \rightsquigarrow$ Equivalence relation

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: G & the *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.

$n\mathbf{Z} := \{x \in \mathbf{Z} : x = nk \text{ for } k \in \mathbf{Z}\}$ 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 $\det(A^{-1}) = 1$.

Simpler ways

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

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

$$e'e' = e' \text{ [Why?] and } e'e = e' \text{ [Why?]} \quad \Rightarrow e'e' = e'e \quad \Rightarrow e' = e$$

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

In G, we have $ab = e = aa^{-1}$. Hence $b = a^{-1}$.

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

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

Proof: $(\Rightarrow)$: Nonempty: $e \in H$; If $a, b \in H$, then $b^{-1} \in H$ and $ab^{-1} \in H$.

$(\Leftarrow)$: Since H is nonempty, there is at least $a \in H$. Then ii) $e = aa^{-1} \in H$. Also iii) $a^{-1} = ea^{-1} \in H$. Finally, i) $ab = a(b^{-1})^{-1} \in H$ for $a, b \in H$. □

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 $a \in H$.

Note that the diagonal entries of any element in H must all be nonzero.

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: $I_n \in H$; It is easy to see that the second condition also holds.

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 previous result $\rightsquigarrow$ to show $b^{-1} \in H$ for all $b \in H$. Given $b \in H$, consider the set

$$\{b, b^2, b^3, \ldots\},$$

which is a subset of H. Since H is a finite set, they cannot all be distinct. There exists some repetition: $b^n = b^m$ for some $n > m > 0$. $\rightsquigarrow$ $b^{n-m} = e$. Either $b = e$ $(n - m = 1)$ or $bb^{n-m-1} = e$ $(n - m > 1)$ implies $b^{-1} \in H$. $\square$

Example: Subgroups of S_3

- S_3 & $\{(1)\}$
- $\{(1), (12)\}$, $\{(1), (13)\}$, $\{(1), (23)\}$
- $\{(1), (123), (132)\}$

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.

The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$. 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 $\langle a \rangle \subseteq K$.

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

2) For any subgroup K containing a, it must contain a^n for all $n \in \mathbf{Z}_{>0}$. It also contains $e = a^0$ and $a^{-n} = (a^n)^{-1}$. Hence $\langle a \rangle \subseteq K$. □

When the operation is denoted additively rather than multiplicatively, we should consider multiples (eg. na) rather than powers (eg. a^n).

Examples

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

Proof: $\mathbf{Z} = \langle a \rangle = \{na : n \in \mathbf{Z}\} \Rightarrow a = \pm 1$. $\square$

$(\mathbf{Z}_n, +_{[\,]}) = \langle [1] \rangle$ is cyclic. In fact, we can determine all possible generators

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

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

- $\mathbf{Z}_5^\times = \langle [2] \rangle = \langle [3] \rangle$ is cyclic. However, $[4]$ 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.

Recall that subgroups of S_3 are

- $\{(1)\} = \langle (1) \rangle$
- $\{(1), (12)\} = \langle (12) \rangle$, $\{(1), (13)\} = \langle (13) \rangle$, $\{(1), (23)\} = \langle (23) \rangle$
- $\{(1), (123), (132)\} = \langle (123) \rangle = \langle (132) \rangle$
- 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 $|\langle a \rangle| = o(a)$.

Proof: i) Assume $a^k = a^m$ for $k \geq m$. Then $a^{k-m} = e$. Thus, $k - m = 0$.
ii) $(\Leftarrow)$: ✓ $(\Rightarrow)$: Let $o(a) = n$. Write $k = nq + r$, where $0 \leq r < n$. Thus,

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = e \cdot e^{-q} = e. \quad \Rightarrow r = 0 \quad \Rightarrow n|k.$$

iii) $a^k = a^m \Leftrightarrow a^{k-m} = e \overset{\text{ii)}}{\Leftrightarrow} n|(k-m)$. To show $\langle a \rangle = \{e, a, \ldots a^{n-1}\} := S$
$S \subset \langle a \rangle$ by definition of $\langle a \rangle$; S is a subgroup of G & $a \in S$, so $\langle a \rangle \subset S$ □

Examples

The intersection of any collection of subgroups is again a subgroup. (HW)

Given any subset S of a group G, the intersection of all subgroups of G that contain S is in fact the **smallest subgroup that contains** S.

By the previous slide, $\langle a \rangle$ is the smallest subgroup containing $S = \{a\}$.

Examples

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

$\langle i \rangle = \{1,\ i,\ -1,\ -i\}$, which is a cyclic subgroup of $\mathbf{C}^\times$ of order 4.

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

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

Let $z = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. We can show that $\langle z \rangle = \{z^k \mid k \in \mathbf{Z}\}$ is the set of complex nth roots of unity, which is a cyclic subgroup of $\mathbf{C}^\times$ of order n.

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 $[a] := \{b \in G | a \sim b \text{ i.e., } ab^{-1} \in H\}$ denote the equivalence class of a.

Consider the function $\rho_a : H \to [a]$ defined by $\rho_a(h) = ha$ for all $h \in H$.

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

i) If $h \in H$, then $\rho_a(h) = ha \in [a]$ since $a(ha)^{-1} = h^{-1} \in H$.

ii) one-to-one: For $h, k \in H$, if $\rho_a(h) = \rho_a(k)$, then $ha = ka$. $\Rightarrow h = k$.

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 $m \mid n$. □

Example

Recall that the equivalent class $[a]$ of $a \in G$ defined as

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

$[a] = Hb$ for any $b \in [a]$. ($b = ha \Leftrightarrow h^{-1}b = a$: $Ha \subset Hb$ ✓; $Hb \subset Ha$ ✓)

For example, consider $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$.

1) $H = \langle(123)\rangle = \langle(132)\rangle = \{(1), (123), (132)\}$: Two equivalent classes
   - H forms the first equivalence class: $H = H(1) = H(123) = H(132)$
   - Any other equivalence class must be **disjoint** from the first one and have the **same number of elements**, so the only possibility is

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

   Therefore, these two equivalent classes are $H, H(12)$.
2) $K = \langle(12)\rangle = \{(1), (12)\}$: Three equivalent classes
   - K forms the first equivalence class: $K = K(1) = K(12)$
   - $K(13) = \{(13), (132)\} = K(132)$
   - $K(23) = \{(23), (123)\} = K(123)$

   Therefore, these three equivalent classes are $K, K(13), K(23)$.

Two Corollaries

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

Corollary 1

Let G be a finite group of order n. For any $a \in G$, $o(a) \mid n$. And so $a^n = e$.

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 2

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

$$|\langle a \rangle| \neq 1, \text{ and so } |\langle a \rangle| \text{ must be } p. \text{ [Why?]}$$

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

Examples

Let H be any subgroup of G and $a \in G$. Then aHa^{-1} is a subgroup of G.

Proof: Note that $aHa^{-1} := \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$.

Closure: Let $g_i = ah_ia^{-1}, i = \{1, 2\}$. Then $g_1g_2 = a(h_1h_2)a^{-1} \in aHa^{-1}$.

Identity: $e = aea^{-1} \in aHa^{-1}$.

Inverses: $g = aha^{-1} \in aHa^{-1} \rightsquigarrow g^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$. □

2nd proof: Nonempty e; $g_1g_2^{-1} = ah_1a^{-1}(ah_2a^{-1})^{-1} = ah_1h_2^{-1}a^{-1}$ □

Let G be an abelian group, and let n be a fixed positive integer. Define

$$N := \{g \in G : g = a^n \text{ for some } a \in G\}.$$

Then N is a subgroup of G.

Proof: To show N is nonempty and $g_1g_2^{-1} \in N$, for all $g_1, g_2 \in N$.

- The identity element $e \in N$ since $e = e^n$.
- Let $g_1 = a_1^n$ and $g_2 = a_2^n$ for some $a_1, a_2 \in G$. Then

$$g_1g_2^{-1} = a_1^n(a_2^n)^{-1} = a_1^na_2^{-n} = a_1^n(a_2^{-1})^n \overset{!}{=} (a_1a_2^{-1})^n \in N.$$ □