§3.3 Constructing Examples

Shaoyun Yi

MATH 546/701I

University of South Carolina

Summer 2021

Review

- Subgroup H: $\begin{cases} \text{Closure} \\ \text{Identity} \\ \text{Inverses} \end{cases}$ (*no worry about* associativity)
  - Alternative way: H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$
  - If H is finite, then H is nonempty and $ab \in H$ for all $a, b \in H$
  - e.g.: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.
- Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
  e.g.: $\langle i \rangle \subseteq \mathbf{C}^\times$ & $\langle 2i \rangle \subseteq \mathbf{C}^\times$; $\langle (123) \rangle \subseteq S_3$ & $\langle (12) \rangle \subseteq S_3$.
- G is cyclic if $G = \langle a \rangle$.
  e.g.: $\mathbf{Z}$, $\mathbf{Z}_n$, $\mathbf{Z}_5^\times$. not e.g.: $\mathbf{Z}_8^\times$, S_3.
- $o(a) = |\langle a \rangle|$. If $o(a) = n$ is finite, then $a^k = e \Leftrightarrow n|k$.
- **Lagrange's Theorem:** If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \mid n$.
  - $o(a)|n$ for any $a \in G$. $\rightsquigarrow a^n = e$ $\dashrightarrow$ Euler's theorem
  - Any group of prime order is cyclic (and so abelian).
    $\rightsquigarrow$ Any group of order 2, 3, or 5 must be cyclic.

$|G| = 4$

For $a \in G$ with $a \neq e$, then either $o(a) = 2$ or $o(a) = 4$.

i) If $o(a) = 4$, then $G = \langle a \rangle = \{e, a, a^2, a^3\}$.

ii) If there is no element of order 4, then $o(a) = 2$ for all $a \neq e$.

Each element must occur **exactly once** in each row and column.

i)	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

ii)	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Both cases are abelian. $\rightsquigarrow$ The group of order 4 is always abelian.

$|G| = 6$

We have seen two basic examples of groups of order 6:

- $\mathbf{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ is cyclic. (generator $[a], (a, 6) = 1$)
- $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ is nonabelian.

$\rightsquigarrow$ The order of the **smallest** nonabelian group is 6.

Let $e = (1), a = (123)$ and $b = (12)$. $\rightsquigarrow a^2 = (132),\ a^3 = e;\ b^2 = e$.
Each element of S_3 in the form $a^i b^j$ uniquely, for $i = 0, 1, 2$ and $j = 0, 1$:

$$(1) = e,\ (123) = a,\ (132) = a^2,\ (12) = b,\ (13) = ab,\ (23) = a^2 b.$$

Q: What is ba? **A:** $ba = a^2 b$ (Double check: $(12)(123) = (23)$)

$$\boxed{S_3 = \{e, a, a^2, b, ab, a^2 b\}, \quad \text{where } a^3 = e,\ b^2 = e,\ ba = a^2 b.}$$

Q: What is ba^2? **A:** $ba^2 = (ba)a = (a^2 b)a = a^2(ba) = a^2(a^2 b) = ab$

Multiplication Table for S_3

$$S_3 = \{e, a, a^2, b, ab, a^2b\}, \quad \text{where } a^3 = e,\ b^2 = e,\ ba = a^2b.$$

We also calculated $ba^2 = (ba)a = (a^2b)a = a^2(ba) = a^2(a^2b) = ab$.

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Product of two Subgroups

Recall that *the intersection of subgroups of a group is again a subgroup*.

For $H, K \subset G$, $H \cap K$ is the largest subgroup contained in both H and K.

Q: What is the smallest subgroup containing both H and K?

Let G be a group, and let S and T be subsets of G. Then

$$ST = \{x \in G : x = st \text{ for some } s \in S, t \in T\}.$$

If H and K are subgroups of G, then we call HK the **product** of H and K.

A: The **product** HK if it is a subgroup. But, it is not always a subgroup.

If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.

Proof: Closure: For $g_1 = h_1k_1$ and $g_2 = h_2k_2$, $\rightsquigarrow g_1g_2 = (h_1k_1)(h_2k_2)$ $= h_1(h_2h_2^{-1})k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2 \in HK$ ✓ Identity: $e = e \cdot e \in HK$
Inverses: For $g = hk, g^{-1} = (h^{-1}h)k^{-1}h^{-1} = h^{-1}((h^{-1})^{-1}k^{-1}h^{-1}) \in HK$

If G is abelian, then the product of any two subgroups is again a subgroup.

If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.

For $H, K \subset G$, $H \cap K$ is the largest subgroup contained in both H and K.

- For any element $t \in H \cap K$, if $hk \in HK$, then we can write

$$hk = (ht)(t^{-1}k) \in HK.$$

$\rightsquigarrow$ Every element in HK can be written in at least $|H \cap K|$ different ways.

- On the other hand, if $hk = h'k' \in HK$, then $h'^{-1}h = k'k^{-1} \in H \cap K$. Set

$$t := h'^{-1}h = k'k^{-1} \in H \cap K.$$

$\rightsquigarrow h' = ht^{-1}$ and $k' = tk$ $\quad \rightsquigarrow h'k' = (ht^{-1})(tk)$ for some $t \in H \cap K$.

$\rightsquigarrow$ Every element in HK can be written in at most $|H \cap K|$ different ways.

$\rightsquigarrow$ Every element in HK can be written in exactly $|H \cap K|$ different ways:

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Examples: $|HK| = |H||K|/|H \cap K|$ for $|G| < \infty$

Let $G = \mathbf{Z}_{15}^{\times}$ and $H = \{[1], [11]\}$. Note G is abelian and $|G| = \varphi(15) = 8$.

- $K = \{[1], [4]\}$: $|HK| = 4$. Computing all possible products in HK gives

$$[1][1] = [1], \qquad [1][4] = [4], \qquad [11][1] = [11], \qquad [11][4] = [14].$$

$\rightsquigarrow$ $HK = \{[1], [4], [11], [14]\}$ is a subgroup of order 4.

- $L = \langle [7] \rangle = \{[1], [4], [7], [13]\}$: $|HK| = 8 = |G|$. List all products in HK:

$$HL = \{[1], [2], [4], [7], [8], [11], [13], [14]\} = \mathbf{Z}_{15}^{\times}.$$

If the operation is additive, then we write $H + K$ (the **sum** of H and K).

$$a\mathbf{Z} + b\mathbf{Z} = (a, b)\mathbf{Z}$$

Let $h \in H = a\mathbf{Z}$ and $k \in K = b\mathbf{Z}$. Let $(a, b) = d$. To show $H + K = d\mathbf{Z}$.

- $H + K \subseteq d\mathbf{Z}$: $h + k$ is a linear combination of a and b. $\rightsquigarrow$ $(a, b) | (h + k)$
- $d\mathbf{Z} \subseteq H + K$: d is the smallest positive linear combination of a and b.

$\rightsquigarrow$ $d \in H + K$. It implies that $d\mathbf{Z} \subseteq H + K$ since $d\mathbf{Z} = \langle d \rangle$. □

Direct Product of two Groups

The set of all ordered pairs (x_1, x_2) such that $x_1 \in G_1$ and $x_2 \in G_2$ is called the **direct product** of G_1 and G_2, denoted by $G_1 \times G_2$. That is,

$$G_1 \times G_2 = \{(x_1, x_2) \colon x_1 \in G_1 \text{ and } x_2 \in G_2\}.$$

If G_1, G_2 are finite groups, then $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

Let $(G_1, *, e_1)$ and $(G_2, \cdot, e_2)$ be groups.

i) The direct product $G_1 \times G_2$ is a group under the operation defined for all $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ by $(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \cdot b_2)$.

ii) If $a_1 \in G_1$ and $a_2 \in G_2$ have orders n and m, respectively, then the element (a_1, a_2) has order $k = [n, m]$ in $G_1 \times G_2$.

Proof: i) Closure: ✓Associativity: For $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$

$$(a_1, a_2)((b_1, b_2)(c_1, c_2)) = \ldots = ((a_1, a_2)(b_1, b_2))(c_1, c_2).$$

Identity: (e_1, e_2) ✓ Inverses: $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$ ✓

ii) $(a_1, a_2)^{[n,m]} = (e_1, e_2) \rightsquigarrow k \mid [n, m]$. If $(a_1, a_2)^k = (a_1^k, a_2^k) = (e_1, e_2)$, then $n \mid k$ and $m \mid k$. $\rightsquigarrow [n, m] \mid k$. Thus, $k = [n, m]$. □

Example: Klein four-group $\mathbf{Z}_2 \times \mathbf{Z}_2$

The addition table for $\mathbf{Z}_2 \times \mathbf{Z}_2 = \{([0],[0]),([1],[0]),([0],[1]),([1],[1])\}$:

	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([0],[0])$	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([1],[0])$	$([1],[0])$	$([0],[0])$	$([1],[1])$	$([0],[1])$
$([0],[1])$	$([0],[1])$	$([1],[1])$	$([0],[0])$	$([1],[0])$
$([1],[1])$	$([1],[1])$	$([0],[1])$	$([1],[0])$	$([0],[0])$

The pattern in this table is the same as the table below.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This group has order 4 and each element except the identity has order 2.

More Examples

$\mathbf{Z} \times \mathbf{Z}$ is not cyclic.

Proof by contradiction: Suppose $\mathbf{Z} \times \mathbf{Z} = \langle (m, n) \rangle = \{k(m, n) \colon k \in \mathbf{Z}\}$.
However, $\langle (m, n) \rangle$ cannot contain both of $(1, 0)$ and $(0, 1)$. (Check it!) □

Natural subgroups: $\langle (1, 0) \rangle$ and $\langle (0, 1) \rangle$. The "diagonal" subgroup $\langle (1, 1) \rangle$.

$\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic and $\mathbf{Z}_2 \times \mathbf{Z}_4$ is not cyclic.

Proof: $([1], [1])$ has order $[2, 3] = 6 = |\mathbf{Z}_2 \times \mathbf{Z}_3|$. $\rightsquigarrow$ $\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic.

$|\mathbf{Z}_2 \times \mathbf{Z}_4| = 8$: In the first component the possible orders are 1 and 2.
In the second component the possible orders are $1, 2, 4$.

$\rightsquigarrow$ The largest possible least common multiple we can have is $4 < 8$.

$\rightsquigarrow$ So there is no element of order 8 and the group is not cyclic. □

$\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic if and only if $\gcd(n, m) = 1$.

$\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic if and only if $\gcd(n, m) = 1$.

Proof: $(\Rightarrow)$: Assume $(a, b) \in \mathbf{Z}_n \times \mathbf{Z}_m$ has order $k = |\mathbf{Z}_n \times \mathbf{Z}_m| = nm$. Since $o(a)|n, o(b)|m$ and $k = [o(a), o(b)]$. $\rightsquigarrow o(a) = n, o(b) = m$. If not,

$$nm = k = [o(a), o(b)] = \frac{o(a) \cdot o(b)}{\gcd(o(a), o(b))} \leq o(a) \cdot o(b) < nm.$$

$\rightsquigarrow nm = k = [n, m]$. Hence $\gcd(n, m) = 1$ since $nm = [n, m] \cdot \gcd(n, m)$.

$(\Leftarrow)$: Assume $(n, m) = 1$, consider the cyclic subgroup $\langle([1]_n, [1]_m)\rangle$. Then

$$o([1]_n) = n \quad \text{and} \quad o([1]_m) = m.$$

It follows that

$$o(([1]_n, [1]_m)) = [o([1]_n), o([1]_m)] = [n, m] = \frac{nm}{\gcd(n, m)} = nm.$$

Thus $\mathbf{Z}_n \times \mathbf{Z}_m = \langle([1]_n, [1]_m)\rangle$, namely, is cyclic. $\square$

Example from Matrices

$$|\mathrm{GL}_2(\mathbf{Z}_p)| = (p^2 - 1) \cdot (p^2 - p), \quad \text{where } p \text{ is a prime number.}$$

Proof: 1st row: There are $p^2 - 1$ choices since $(0,0)$ cannot be a choice.
2nd row: There are $p^2 - p$ choices. (scalars of 1st row cannot be choices)

$|\mathrm{GL}_2(\mathbf{Z}_2)| = 6$: These 6 elements and their orders are as follows.

	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}1&1\\1&0\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&0\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\end{bmatrix}$	$\begin{bmatrix}1&0\\1&1\end{bmatrix}$
order	1	3	3	2	2	2

We simply use 0 and 1 to denote the congruence classes $[0]_2$ and $[1]_2$.

The group $\mathrm{GL}_2(\mathbf{Z}_2)$ is nonabelian. e.g. $\begin{bmatrix}0&1\\1&1\end{bmatrix}\begin{bmatrix}0&1\\1&0\end{bmatrix} \neq \begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}0&1\\1&1\end{bmatrix}$.

S_3 is also nonabelian with order 6. In fact, they are "the same" group! (see §3.4)

Subgroup Generated by a Nonempty S of the Group G

A finite product of elements of S and their inverses is called a **word** in S. The set of all words in S is denoted by $\langle S \rangle$.

For example, for $a, b, c \in S$, then $a^{-1}a^{-1}bab^{-1}acb^{-1}cbc^{-1}c^{-1} \in \langle S \rangle$.

$\langle S \rangle$ is a subgroup of G, and is equal to the intersection of all subgroups of G that contain S. That is, $\langle S \rangle$ is the smallest subgroup that contains S.

Proof: Closure: If x, y are two words in S, then xy is again a word in S. ✓
Identity: $e = aa^{-1} \in \langle S \rangle$. Here $a \in S$ always exists since S is nonempty. ✓
Inverses: $x^{-1} \in \langle S \rangle$: reverses the order & changes the sign of exponent. ✓
If $S \subseteq H$, where H is a subgroup of G, then it contains all words in S. So $\langle S \rangle \subseteq H \rightsquigarrow \langle S \rangle$ is the intersection of all subgroups of G that contain S. $\square$

$S = \{a\}$: In this case, $\langle S \rangle = \langle a \rangle$ is a cyclic subgroup. Simple!
$S = \{a, b\}$: In a nonabelian group G, it becomes much more complicated to describe $\langle S \rangle$.

Definition of a Field

Let F be a set with two binary operations $+$ and $\cdot$ with respective identity elements 0 and 1, where $0 \neq 1$. Then F is called a **field** if

1) the set of all elements of F is an abelian group under $+$;
2) the set of all nonzero elements of F is an abelian group under $\cdot$;
3) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in F$.

3) distributive laws give a connection between addition & multiplication

For any element $a \in F$, we have $a \cdot 0 = 0$ and $0 \cdot a = 0$.

$0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \rightsquigarrow 0 = a \cdot 0$. Similarly, $0 \cdot a = 0$.

For example, $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, when p is a prime number. But $\mathbf{Z}$ is not a field.

Let F be a field. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

i) Closure ✓ ii) Associativity ✓ iii) Identity: I_n iv) Inverses: $A^{-1} \in \mathrm{GL}_n(F)$