香港中文大學(深圳)
The Chinese University of Hong Kong, Shenzhen

Lecture 1
Groups

Grant Rao

This note is based on Ping-Shun Chan's note from CUHK.

Preliminaries

- $\mathbb{Z}$ = the set of all integers
- $\mathbb{Z}^+ = \{a \in \mathbb{Z} | a > 0\}$
- $\mathbb{Z}^- = \{a \in \mathbb{Z} | a < 0\}$
- $\mathbb{N} = \{a \in \mathbb{Z} | a \geq 0\}$
- $\mathbb{R}$ = the set of all real numbers
- $\mathbb{Q} = \left\{\frac{a}{b} \middle| a, b \in \mathbb{Z}, b \neq 0\right\}$
- $\mathbb{C}$ = the set of all complex numbers

Well Ordering Principle. Let $S \subseteq \mathbb{N}$. Then there exists a smallest element $x \in S$.

Division Theorem. Let $a \in \mathbb{Z}, b \in \mathbb{Z}^+$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.

1 Groups

Definition 1.1. A **group** G is a set equipped with a binary operation

$$* : G \times G \longrightarrow G$$

(called "**group operation**" or "**product**" or "**multiplication**") such that:

- the group operation is **associative**, i.e.,

$$(a * b) * c = a * (b * c) \qquad \forall a, b, c \in G$$

- there *exists* an **identity** $e \in G$ such that

$$a * e = e * a = a \qquad \forall a \in G$$

- for each $a \in G$, there *exists* an **inverse** $a^{-1} \in G$ such that

$$a^{-1} * a = a * a^{-1} = e$$

Remark 1.2. $a * b$ is usually written as $a \cdot b$ or ab.

Definition 1.3. The group operation of G is **commutative** if

$$ab = ba \qquad \forall a, b \in G$$

A group with a commutative operation is **abelian**; and otherwise **non-abelian**.

Definition 1.4. The **size** of a set S, denoted by $|S|$, is the number of elements in S. For a group G, the **order** of G is $|G|$, and G is **finite** (**infinite**) when $|G|$ is finite (infinite).

Remark 1.5. If a set G is equipped with an associative binary operation "$*$" (*not necessarily having identities or inverses*), then G is a **semigroup**. Moverover, if "$*$" is commutative, then G is an **abelian semigroup**.

If a semigroup G also has an identity (*not necessarily having inverses*), we call G a **monoid**.

Similar to groups, we can define the **order** of semigroups and monoids based on the number of their elements.

As an elementary course in abstract algebra, we shall not discuss the properties of these algebraic structures. Interested students may browse more details in Wikipedia.

Example 1.6. Which of following are groups?

1. $(\mathbb{Q}, +)$: the set of all rational numbers with the usual addition "+". ✓
2. $(\mathbb{Q}, \cdot)$: the set of all rational numbers with the usual multiplication "$\cdot$". ×
   (**Note:** $a^{-1} = 1/a \quad \Rightarrow \quad a \neq 0$)
   So we should instead have $(\mathbb{Q}^{\#}, \cdot)$ as a group where $\mathbb{Q}^{\#} := \mathbb{Q} \setminus \{0\}$.
3. $(U_m, \cdot)$ where $U_m = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}\}$ and $\zeta_m := e^{2\pi i/m}$**??**
4. The set of bijections of $\mathbb{R}$ with composition operation**??**
5. The set of permutations of a Rubik's cube with the rotation operations. ✓

Example 1.7. $\mathsf{GL}(2,\mathbb{R}) = \{A \in \mathbf{M}_2(\mathbb{R}) | \mathsf{det}(A) \neq 0\}$ is a group with the matrix multiplication as its operation. The identity is

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and the inverse is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Note that $\mathsf{GL}(2,\mathbb{R})$ is not abelian as there exist $A, B \in \mathsf{GL}(2,\mathbb{R})$ such that $AB \neq BA$. And $\mathsf{GL}(2,\mathbb{R})$ is infinite.
In general, if $n \in \mathbb{Z}^+$, then

$$\mathsf{GL}(n,\mathbb{R}) = \{A \in \mathbf{M}_n(\mathbb{R}) | \mathsf{det}(A) \neq 0\}.$$

is the **general linear group** under the matrix multiplication.
Similarly, one can verify that

$$\mathsf{SL}(n,\mathbb{R}) = \{A \in \mathbf{M}_n(\mathbb{R}) | \mathsf{det}(A) = 1\}$$

is the **special linear group** under the matrix multiplication. (**exercise**)

Example 1.8. Let $n \in \mathbb{Z}^+$. Set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

Define a binary operation "$+_n$" on $\mathbb{Z}_n$ by

$$a +_n b = \begin{cases} a+b & \text{if } a+b < n; \\ a+b-n & \text{if } a+b \geq n. \end{cases}$$

Then $(\mathbb{Z}_n, +_n)$ is a finite abelian group. (**exercise**)

Remark 1.9. Abusing the notation, we usually write "$+$" in lieu of "$+_n$".

Proposition 1.10. The product of the elements $g_1, g_2, \ldots, g_n$ in a group G is independent from adding parentheses.

Proof. The statement apparently holds when $n = 1$. Assume the statement holds

for $n \leq k$. Consider the case when $n = k + 1$. For each $m \in \{1, 2, \ldots, k\}$, we have

$$\begin{aligned}
&(g_1 g_2 \cdots g_m)(g_{m+1} \cdots g_{k+1}) \\
=&(g_1 \cdot (g_2 \cdots g_m))(g_{m+1} \cdots g_{k+1}) \\
=&g_1 \cdot ((g_2 \cdots g_m)(g_{m+1} \cdots g_{k+1})) \\
=&g_1 \cdot (g_2 \cdots g_{k+1})
\end{aligned}$$

□

Remark 1.11. Proposition 1.10 shows that given a sequence of elements multiplied together, we do not have to specify the order of the operations that performed, as the final result is always the same.

Moreover, for abelian groups, the product is unique regardless of the ordering.

Proposition 1.12. Each group G has a unique identity element.

Proof. Let $e, e' \in G$ be both identities. Then

$$e = e \cdot e' = e'.$$

□

Proposition 1.13. Let G be a group. Then g^{-1} is unique for any $g \in G$.

Proof. Take $g \in G$. Let h_1, h_2 be both inverses of g. By the definition of inverse

$$h_1 = h_1 \cdot e = h_1(gh_2) = (h_1 g)h_2 = e \cdot h_2 = h_2.$$

□

Remark 1.14. Based on Proposition 1.10–1.13, it makes sense to say *the* identity of a group G, and *the* inverse of an element $g \in G$. For $g \in G, n \in \mathbb{N}$, we may define

$$g^n := \underbrace{g \cdot g \cdots g}_{n \text{ times}} \qquad g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}} \qquad g^0 := e$$

Proposition 1.15. Let G be a group.

(i) $(g^{-1})^{-1} = g, \qquad \forall g \in G.$

(ii) $(ab)^{-1} = b^{-1}a^{-1}, \qquad \forall a, b \in G.$

(iii) $g^m \cdot g^n = g^{m+n}, \qquad \forall g \in G, m, n \in \mathbb{Z}.$

Proof. **Exercise.** □

In fact, we can define groups with a weaker condition.

Definition 1.16. A **group** G is a semigroup with a binary operation such that

- there *exists* a **left identity** $e \in G$ such that
$$ea = a \qquad \forall a \in G$$
- for each $a \in G$, there *exists* a **left inverse** $a^{-1} \in G$ such that
$$a^{-1}a = e$$

Proposition 1.17. Definition 1.1 and Definition 1.16 are equivalent.

Proof. It suffices to show that left identities, left inverses are identities and inverses.

① Let $a \in G$ be with a left inverse a^{-1}. Then
$$(a^{-1})^{-1}a^{-1}a = ((a^{-1})^{-1}(a^{-1}))a = ea = a$$
$$\Rightarrow \; aa^{-1} = ((a^{-1})^{-1}a^{-1}a)a^{-1} = (a^{-1})^{-1}(a^{-1}a)a^{-1} = (a^{-1})^{-1}ea^{-1} = (a^{-1})^{-1}a^{-1} = e.$$
So a left inverse is always an inverse.

② Let $e \in G$ be a left identity. Then

$$ae = a(a^{-1}a) = (aa^{-1})a = ea = a$$

So a left identity is always an identity. □

Remark 1.18. Similary, we can define a group by an associative binary operation along with right identities and right inverses. (**exercise**) However, we cannot define a group by left identities and right inverses or by right identities and left inverses.

Exercise 1.19. Let G be a set of size at least 2 equipped with a binary operation "$*$" such that

$$a * b = b \qquad \forall a, b \in G$$

Then "$*$" is associative, and G has left identities and right inverses for every element in G. But G is not a group by definition.

If a group is *finite*, then its operation can be described by its **Cayley table** (or **multiplication table**).

Example 1.20. For a group $G = \{e, a\}$ with the operation "$*$", its Cayley table is as follows.

$*$	e	a
e	e	a
a	a	e

Example 1.21. For the group $(\mathbb{Z}_6, +)$, its Cayley table is as follows.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Observe that the Cayley table records all the results of the operation, so given a set G with finite elements, we can also define a group on G by a Cayley table. However, not all Cayley tables define a group.

Exercise 1.22. Provided with the Cayley table for $G = \{\blacklozenge, \bigstar, \spadesuit, \clubsuit\}$ as follows, does $(G, \cdot)$ form a group?

$\cdot$	$\blacklozenge$	$\bigstar$	$\spadesuit$	$\clubsuit$
$\blacklozenge$	$\bigstar$	$\blacklozenge$	$\clubsuit$	$\spadesuit$
$\bigstar$	$\clubsuit$	$\bigstar$	$\spadesuit$	$\blacklozenge$
$\spadesuit$	$\blacklozenge$	$\spadesuit$	$\bigstar$	$\clubsuit$
$\clubsuit$	$\spadesuit$	$\clubsuit$	$\blacklozenge$	$\bigstar$

Exercise 1.23. For the set $G = \{e, a, b\}$, prove that the following Cayley table defines a group $(G, *)$.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Remark 1.24. Given a Cayley table, although it is usually messy to check whether it defines a group, there are a few necessary conditions we can examine:

1. Does it have a row and a column that is identical to the list of the elements?
2. For each row and column, the elements must be all distinct. (Why?)