X-Program Handout

Stephanie Yao

October 2023

Contents

§1 Lecture 1.0 - Introduction to Group Theory

§1.1 Basic Axioms of Group

Definition 1.1 (Group)**.** A group is a pair $(G, *)$, where $*$ is a binary operation on G, satisfying the following:

- Associativity: For each $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.
- Identity: There exists some element $e \in G$ such that, for all $g \in G, e * g = g * e = g$.
- Inverses: For each element $g \in G$, there exists some $h \in G$ satisfying $g * h = h * g = e$. Often, we write this h as g^{-1}.

Remind of basic axioms for (integer's) addition we learned in primary school, something familiar is missing – commutativity.

Definition 1.2 (Commutativity)**.** For each $a, b \in G$ of the group $(G, *)$, we have $a * b = b * a$.

Commutativity is **not** assumed as a group axiom. Groups that also satisfy the commutativity axiom are known as **abelian** groups.

Definition 1.3 (Abelian Group)**.** A group that satisfies the commutativity axioms is abelian, otherwise, it is non-abelian.

Proposition 1.4

The identity element of a group $(G, *)$ is *unique*. That is, if e_1 and e_2 are elements of G such that, for all $g \in G$,

$$e_1 * g = g * e_1 = g * e_2 = e_2 * g = g,$$

then in fact $e_1 = e_2$.

Proposition 1.5

Every element $g \in G$ has a *unique* inverse. That is, if h and h' are elements of G such that

$$g * h = h * g = g * h' = h' * g = e,$$

then in fact $h = h'$.

Example 1.6 (Examples of groups)

- $(\mathbb{Z}, +)$ is a group. In fact, it is an abelian group.
- $(\mathbb{Z}_m, +)$ is a group for all $m \in \mathbb{Z}$. It is also abelian.
- $(\mathbb{Z}, \cdot)$ is not a group. (Failure of inverses.)
- $(\mathbb{Z}, -)$ is not a group. (Failure of associativity.)
- $(\mathbb{Z}^+, +)$ is not a group. (Failure of inverses.)
- $(\mathbb{Z}^+, \cdot)$ is not a group. (Failure of inverses.)
- $(\mathbb{R}, +)$ is an abelian group.
- $(\mathbb{R}^+, \cdot)$ is an abelian group.

§1.2 Cyclic Group

Definition 1.7 (Cyclic Group)**.** We say that $(G, *)$ is a **cyclic group** if there exists an element g such that, for each $a \in G$, there exists some $n \in \mathbb{Z}$ such that

$$a = g^n$$

Definition 1.8 (Generator)**.** We refer to such g in the cyclic group as a **generator**. Sometimes we write $G =< g >$.

For example, $(\mathbb{Z}^+, +)$ is a cyclic group with generator $g = 1$.

Example 1.9 (A Slightly More Interesting Example)

Take the even positive numbers $2\mathbb{Z}$, defined by

$$2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$$

Then we have that $2\mathbb{Z}$ is, with the usual addition $+$, a group as well.

- Associativity is trivial, since addition is associative on all of $\mathbb{Z}$.
- The element 0 satisfies the identity axiom, and since $0 = 2 \cdot 0$, indeed $0 \in 2\mathbb{Z}$.
- If $m \in 2\mathbb{Z}$, then $m = 2n$ for some $n \in \mathbb{Z}$. Then we have $-m = 2 \cdot (-n)$, so $-m \in 2\mathbb{Z}$ as well.

Question 1.10. Did we miss anything?

We should check that $+$ is a binary operation on $2\mathbb{Z}$, not just on $\mathbb{Z}$. That is to say, we need to make sure that if $m, k \in 2\mathbb{Z}$, $m + k \in 2\mathbb{Z}$ as well.

Not only is $2\mathbb{Z}$ a group, it is a cyclic group generated by 2.

Remark 1.11. Notational caveats and remarks:

- If the group $(G, *)$ is abelian, then instead of g^n, we often write ng and for the inverse, we will also write $-g$ instead of g^{-1}.
- Not infrequently, the binary operation is suppressed in the notation; instead of $g * h$ we simply write gh.
- Often when the operation $*$ is known, the group $(G, *)$ is simply denoted by G.

§1.3 Subgroup

Example 1.9 shows that $2\mathbb{Z}$ is a group contained within $\mathbb{Z}$. There is a formal definition for this kind of group pairs.

Definition 1.12 (Subgroup)**.** Let $(G, *)$ be a group, and $H \subseteq G$. We say that $(H, *|_H)$ is a subgroup of G if the following hold:

- Closure: $*|_H$, the restriction of $*$ to H, is in fact a binary operation on H. That is, for any $h, k \in H$, we have $h * k \in H$ as well.
- Associativity
- Identity: there exists an identity element in H.
- Inverses: for each $h \in H$, we have that $h^{-1} \in H$. We often write this as $H \leq G$.

Definition 1.13 (Proper Subgroup)**.** If $(H, *|_H)$ is a subgroup of $(G, *)$ and H is not the entire set G, then we say that H is a proper subgroup of G.

Example 1.14

As shown, $(2\mathbb{Z}, +)$ is therefore a proper subgroup of $(\mathbb{Z}, +)$.

Example 1.15

For every group G, $\{e\}$ which is the set of identity elements of G is always a subgroup of G. It is often referred to as the **trivial subgroup**.

§1.4 Group Homomorphism and Isomorphism

Definition 1.16 (Homomorphism)**.** Let A_1 and A_2 be two abelian groups, and let $\varphi : A_1 \to A_2$ be a function sending elements of A_1 to those of A_2. We say that φ is a **group homomorphism** from A_1 to A_2 if, for all $a, b \in A_1$,

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

Remark 1.17 (Difference on Notations)**.** Actually, we can define group homomorphisms in general for groups G_1, G_2, even if the groups are not necessarily abelian. The definition is basically the same (note that the order matters):

$$\varphi(ab) = \varphi(a)\varphi(b)$$

Example 1.18

Define a function $\varphi : \mathbb{Z} \to \mathbb{Z}$ by

$$\varphi(n) = 2n.$$

Verify φ is a group homomorphism.

Proof. This is trivial. For every two elements a, b in $\mathbb{Z}$, we have

$$\begin{aligned} LHS &= \varphi(a+b) \\ &= 2(a+b) \\ &= 2a + 2b \\ &= \varphi(a) + \varphi(b) \\ &= RHS \end{aligned}$$

□

Definition 1.19 (kernel)**.** Let $\varphi : A \to B$ be a homomorphism of abelian groups. We define the **kernel** $\ker \varphi$ as the collection of elements of A sent by φ to the identity of B. That is,

$$\ker \varphi = \{a \in A : \varphi(a) = e_B\}$$

Proposition 1.20

Let $\varphi : A \to B$ be a group homomorphism. Then $\ker \varphi$ is a subgroup of A.

From the definition of kernel, we can deduce some trivial properties.

- $\varphi(e_A) = e_B$
- $\varphi(a^{-1}) = \varphi(a)^{-1}$

Proposition 1.21

$\varphi(e_A) = e_B$.

Proof. Applying the identity of A and B on a and $\varphi(a)$, we have

$$\varphi(a) = \varphi(e_A \cdot a) = e_B \cdot \varphi(a)$$

and according to the homomorphism, $\varphi(e_A \cdot a) = \varphi(e_A) \cdot \varphi(a)$, therefore,

$$\varphi(e_A) = e_B$$

□

Proposition 1.22

$\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof. This proof is left as an exercise for reader. ■

We also define the image of φ.

Definition 1.23. The **image** of φ is defined by

$$\operatorname{im} \varphi = \{\varphi(a) : a \in A\}$$

Some people use $\varphi(A)$ as well for image.

Proposition 1.24

Let $\varphi : A \to B$ be a group homomorphism. Then $\operatorname{im}\varphi$ is a subgroup of B.

Remark 1.25 (A Good Way to Understand kernel and Image)**.** You definitely know the definition of function (or more appropriately) already, we can think that φ is a function that links group A to B, where kernel means the zeros (x for $f(x) = 0$) and image means the range.

Definition 1.26 (Injective)**.** We say that φ is **injective** or **one-to-one** if, for any $a_1, a_2 \in A$, $\varphi(a_1) = \varphi(a_2)$ if and only if $a_1 = a_2$.

Definition 1.27 (Surjective)**.** We say that φ is **surjective** or **onto** if, for any $b \in B$, there exists $a \in A$ such that $\varphi(a) = b$. In other words, $\operatorname{im}\varphi = B$.

Proposition 1.28

The following statements are equivalent:

- φ is injective;
- $\ker\varphi = \{e_A\}$

This is an interesting proposition, let's prove it!

Proof. Let's first prove if $\varphi : A \to B$ is injective, then $\ker\varphi = \{e_A\}$.

Suppose the homomorphism $\varphi : A \to B$ is injective. Then since φ is a group homomorphism, according to Proposition 1.21, we have $\varphi(e_A) = e_B$. If we say $a \in A$ and $a \in \ker\varphi$, then we have $\varphi(a) = e_B = \varphi(e_A)$. Since $\varphi : A \to B$ is injective, we must have $a = e_A$.

Therefore, φ is injective $\implies \ker\varphi = \{e_A\}$.

Then prove if $\ker\varphi = \{e_A\}, \varphi$ is injective.

We suppose that there exist a_1 and a_2 in group A such that

$$\varphi(a_1) = \varphi(a_2),$$

then we have

$$\begin{aligned}
\varphi(a_1 a_2^{-1}) &= \varphi(a_1)\varphi(a_2^{-1}) \text{ according to the definition of group homomorphism} \\
&= \varphi(a_1)\varphi(a_2)^{-1} \text{ according to Proposition 1.22} \\
&= \varphi(a_1)\varphi(a_1)^{-1} \\
&= e_B
\end{aligned}$$

Thus the element $a_1 a_2^{-1} = e_A$, implying $a_1 = a_2$ and φ is injective. □

Definition 1.29 (Isomorphism)**.** A homomorphism that is both injective and surjective is referred to as an **isomorphism**.

When two groups are **isomorphic**, in a sense they are the same.

Example 1.30 (Chinese Remainder Theorem)

Let m and n be coprime positive integers, the Chinese Remainder Theorem tells us that the system of congruences

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

has a unique solution mod mn. This implies the map $L_{m,n} : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$ by

$$L(a, b) = x$$

where x is the unique solution.

Here $L_{m,n}$ is an isomorphism of groups.

References

[1] Dummit, David Steven, and Richard M. Foote. *Abstract algebra*. Vol. 3. Hoboken: Wiley, 2004.

[2] Gallian, Joseph. *Contemporary abstract algebra*. Chapman and Hall/CRC, 2021.

Special thanks to Paco for his superb dorm lectures on group theory that covered basic group theory knowledge and led me on the journey of learning Abstract Algebra.