Summary for Modern Algebra I

SEUNGWOO HAN

Contents

Chapter 1

Groups

1.1 Definitions and Examples of Groups

Definition 1.1.1: Abelian Group

An *abelian group* is a nonempty set G equipped with a binary operation $+$ on G that satisfies the following.

(i) (associative) $\forall a, b, c \in G,\ a + (b + c) = (a + b) + c$.
(ii) (commutative) $\forall a, b \in G,\ a + b = b + a$.
(iii) (identity) $\exists 0 \in G,\ \forall a \in G,\ a + 0 = 0 + a = a$.
(iv) (inverse) $\forall a \in G,\ \exists b \in G,\ a + b = b + a = 0$.

Note:-

One may easily show that the identity is unique, and for each $a \in G$, an inverse of a is unique.

Notation 1.1.2

- We define $-\colon G \times G \to G$ by $a - b = a + (-b)$.
- We write, for each positive integer n, and for each $a \in G$,

$$na \triangleq \underbrace{a + a + \cdots + a}_{n \text{ times}}, \qquad 0a \triangleq 0_G, \qquad (-n)a \triangleq \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ times}}.$$

- Hence, $\forall m, n \in \mathbb{Z},\ \forall a \in G,\ (m+n)a = ma + na \wedge m(na) = (mn)a$.

Example 1.1.3

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, equipped with their ordinary additions, are abelian groups, while $(\mathbb{N}, +)$ is not.
(ii) $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$, equipped with their ordinary multiplications, are abelian groups.
(iii) If $G = \{1, -1, i, -i\} \subseteq \mathbb{C}$, then $(G, \cdot)$ is an abelian group. One may explicitly write the *group table* for this.
(iv) $\mathrm{GL}_n(\mathbb{C}) = \{\, n \times n \text{ invertible matrices over } \mathbb{C} \,\}$ (general linear group) equipped with $\cdot$ is not an abelian group but is a group. (See Definition 1.1.4.)

Definition 1.1.4: Group

An *group* is a nonempty set G equipped with a binary operation $\cdot$ on G that satisfies the following.

(i) (associative) $\forall a, b, c \in G,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(ii) (identity) $\exists 1 \in G,\ \forall a \in G,\ a \cdot 1 = 1 \cdot a = a$.

(iii) (inverse) $\forall a \in G,\ \exists b \in G,\ a \cdot b = b \cdot a = 1$.

Theorem 1.1.5

Let $(G, \cdot)$ be a group. Let $a, b, c \in G$.

(i) $ab = ac \implies b = c$

(ii) $(a^{-1})^{-1} = a$

(iii) $(ab)^{-1} = b^{-1}a^{-1}$

Proof. Trivial. □

Notation 1.1.6

- We write, for each positive integer n, and for each $a \in G$,

$$a^n \triangleq \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ times}}, \qquad a^0 \triangleq 1_G, \qquad a^{-n} \triangleq \underbrace{a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}}_{n \text{ times}}.$$

- Hence, $\forall m, n \in \mathbb{Z},\ \forall a \in G,\ a^m a^n = a^{m+n} \wedge (a^m)^n = a^{mn}$.

Note:-

We don't generally have $(ab)^n = a^n b^n$.

Definition 1.1.7: Order

We write $|G|$ to denote the number of elements in G and call it *order* of G.

Example 1.1.8 Dihedral Groups

$$\begin{aligned} D_n &\triangleq \{ r_i : [n] \hookrightarrow\!\!\!\!\rightarrow [n] \mid \forall j \in [n],\ r_i(j) = i +_n j \} \cup \{\text{reflections???}\} \\ &= \{ \text{all “rigid motions” for regular } n \text{ polygon} \} \end{aligned}$$

Then, $(D_n, \circ)$ is a group where $\circ$ is ordinary function composition operator. We claim that $|D_n| = 2n$ and D_n is not abelian.

Proof. If $r \in D_n$ is a rotation, then □

Example 1.1.9 Symmetric Group

Let T be a nonempty set. Then, the set $S(T) \triangleq \{ f : f : T \hookrightarrow\!\!\!\!\rightarrow T \}$ with the function composition operator $\circ$ is a group.

We write

$$S_n \triangleq S(\{1, 2, \cdots, n\})$$

and call it *symmetric group*. S_1 and S_2 are abelian, but S_n with $n \geq 3$ is not abelian. $((1\,2\,3) \circ (1\,2) \neq (1\,2) \circ (1\,2\,3))$

Definition 1.1.10: Group Action

Let G be a group and A be a set. A group action G on A is a map $f : G \times A \to A$ such that:

(i) $\forall g_1, g_2 \in G$, $\forall a \in A$, $f(g_1, f(g_2, a)) = f(g_1 g_2, a)$.

(ii) $\forall a \in A$, $f(1, a) = a$.

We write $G \curvearrowright A$ to write G acts on A.

Example 1.1.11 Quaternion Group

$Q_8 \triangleq \{\pm 1, \pm i, \pm j, \pm k\}$ as usual.

Example 1.1.12 General Linear Group

$\mathrm{GL}_n(R)$ is a group of all $n \times n$ invertible matrices over R.

Definition 1.1.13: Direct Product

If $(G, *_G)$ and $(H, *_H)$ are groups, then the binary operation $*$ on $G \times H$ defined by $(g, h) \times (g', h') \triangleq (g *_G g', h *_H h')$ forms a group $(G \times H, *)$.

1.2 Group Homomorphisms

Definition 1.2.1: Group Homomorphism

Let G and H be groups. A *group homomorphism* between G and H is a function $f : G \to H$ such that $\forall a, b \in G$, $f(ab) = f(a)f(b)$.

Definition 1.2.2: Group Isomorphism

Let G and H be groups. A *group isomorphism* is a bijective group homomorphism between G and H. (This means that G and H have the same group structure.) We write $G \cong H$.

Theorem 1.2.3

Let $f : G \to H$ be a group homomorphism.

(i) $f(1_G) = 1_H$.

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

(iii) $\operatorname{Im} f$ is a group under the group operation under H.

(iv) If f is injective, then $G \cong \operatorname{Im} f$.

Proof.

(i) $f(1_G)f(1_G) = f(1_G 1_G) = f(1_G) = f(1_G)1_H$. Hence, we have $f(1_G) = 1_H$ from Theorem 1.1.5 (i).

(ii) $f(a^{-1})f(a) = f(a^{-1}a) = f(1_G) = 1_H$ by (i). Hence, $f(a^{-1}) = f(a)^{-1}$.

(iii) Direct from definition.

(iv) Direct from definition. □

Note:-

There is only one way—the direct product—to give a group structure on $G \times H$ such that both projections are group homomorphisms.

Definition 1.2.4: Group Automorphism

An *automorphism* of G is an isomorphism $G \hookrightarrow\!\!\!\!\rightarrow G$ between G and itself. Then, the collection of all automorhpisms of G, $\mathrm{Aut}(G) \triangleq \{\text{automorphisms of } G\}$, equipped with $\circ$, is a group. Moreover, $\mathrm{Aut}(G) \curvearrowright G$ in the natural way $((\sigma, g) \mapsto \sigma(g))$.

Example 1.2.5

Fix any $c \in G$ and define $i_c : G \to G$ by $g \mapsto cgc^{-1}$. Then, $i_c \in \mathrm{Aut}(G)$.

Lemma 1.2.6

Let $G \curvearrowright A$. Then, every $g \in G$ induces a map

$$\begin{aligned} \varphi_g : A &\longrightarrow A \\ a &\longmapsto ga. \end{aligned}$$

Then, $\varphi_g \in S(A)$ and $\varphi : G \to S(A)$ defined by $g \mapsto \varphi_g$ is a group homomorphism, which is called the *permutation representation of the group action of G on A*.

Proof. For each $a \in A$, $(\varphi_{g^{-1}} \circ \varphi_g)(a) = g^{-1}(ga) = (g^{-1}g)a = 1a = a$. Thus, $\varphi_{g^{-1}} \circ \varphi_g = \varphi_g \circ \varphi_{g^{-1}} = \mathrm{id}$. Therefore, $\varphi_g \in S(A)$. It is easy to show that φ is a group homomorphism. □

Lemma 1.2.7

Let G be a group and let A be a set. If $\varphi : G \to S(A)$ is a group homomorphism, Then, the map $G \times A \to A$ defined by $(g, a) \mapsto \varphi(g)(a)$ is a group action of G on A.

Proof. Direct from Definition 1.1.10. □

Theorem 1.2.8

Let G be a group and let A be a nonempty set. Then, there exists one-to-one correspondence

$$\{\text{all group actions of } G \text{ on } A\} \overset{1\text{-}1}{\longleftrightarrow} \{\text{all group homomorphisms } G \to S(A)\}.$$

Proof. Direct from Lemmas 1.2.6 and 1.2.7. □

1.3 Subgroups

Definition 1.3.1: Subgroup

Let G be a group, and $\varnothing \subsetneq H \subseteq G$. H is a *subgroup* of G if H is a group under the binary operation of G. If H is a subgroup of G, we write $H \leq G$.

Note:-

(i) $1, G \leq G$.
(ii) If $H, K \leq G$ and $H \subseteq K$, then $H \leq K$.
(iii) If $f : H \to G$ is a group homomorphism, then $\operatorname{im}(f) \leq G$.
(iv) If $H \leq G$, then $\mathrm{id}_H : H \hookrightarrow G$ is a group homomorphism.
(v) For all $n \in \mathbb{Z}$, $n\mathbb{Z} = \{ nz \mid z \in \mathbb{Z} \} \leq \mathbb{Z}$.
(vi) $\{ \pm 1, \pm i \} \leq \mathbb{C}^*$.
(vii) $\{ 1, r_1, \cdots, r_{n-1} \} \leq D_n \leq S_n$ and $\{ 1, s \} \leq D_n$.

Theorem 1.3.2

TFAE. Let G be a group and $\varnothing \subsetneq H \subseteq G$.
(i) $H \leq G$.
(ii) $\forall a, b \in H, ab \in H$ and $\forall a \in H, a^{-1} \in H$.
(iii) $\forall a, b \in H, ab^{-1} \in H$.

Proof. Implications (i) → (ii) and (ii) → (iii) are trivial. For any $a, b \in H$, we have $1 = aa^{-1} \in H$, $a^{-1} = 1a^{-1} \in H$, and $ab = a(b^{-1})^{-1} \in H$. □

Definition 1.3.3: Kernel

Let $f : G \to H$ be a group homomorphism. The *kernel* of f is the set

$$\ker(f) \triangleq \{ g \in G \mid f(g) = 1_H \}.$$

Example 1.3.4 Kernel

Let $f : G \to H$ be a group homomorphism. Then, $\ker(f) \leq G$ since, $1 \in \ker(f)$ and, for each $a, b \in \ker(f)$, $f(ab^{-1}) = f(a)f(b)^{-1} = 1_H 1_H = 1_H$.

Corollary 1.3.5

Let G be a group and let H be a nonempty finite subset of G. Then,

$$H \leq G \iff \forall a, b \in H,\ ab \in H.$$

Proof. The direction ($\Leftarrow$) is trivial.

Take any $a \in H$. By the assumption, $a^n \in H$ for all $n \in \mathbb{Z}_+$. As H is finite, there exists $m, n \in \mathbb{Z}_+$ such that $a^n = a^m$. WLOG, $m < n$. Therefore, $1 = a^{n-m} \in H$. Moreover, we have $aa^{n-m-1} = 1$, which implies $a^{-1} = a^{n-m-1} \in H$. Therefore, by Theorem 1.3.2, $H \leq G$. □

Note:-

The finite condition in Corollary 1.3.5 is essential since $\mathbb{N} \not\leq \mathbb{Z}$ while $\mathbb{N}$ is closed under addition. ($\mathbb{N}$ is not a group at first.)

Corollary 1.3.6

Let G be a group and let $\langle H_i \mid i \in I \rangle$ be an indexed system of subgroups of G. Then, $\bigcap_{i \in I} H_i \leq G$.

Proof. Since $1 \in H_i$ for all $i \in I$, $\bigcap_{i \in I} H_i \neq \varnothing$. Take any $a, b \in \bigcap_{i \in I} H_i$. Then, as $\forall i \in I$, $ab^{-1} \in H_i$, we have $ab^{-1} \in \bigcap_{i \in I} H_i$. The result follows from Theorem 1.3.2. □

Note:-

Even though $H_1, H_2 \leq G$, it is not guaranteed that $H_1 \cup H_2 \leq G$. For instance, $2\mathbb{Z} \cup 3\mathbb{Z} \nleq \mathbb{Z}$. $(2+3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}.)$

Theorem 1.3.7 Cayley Theorem

Let G be a group. Then, $G \cong H$ for some $H \leq S(G)$.

Proof. Note that $(g, g') \mapsto gg'$ is a group action of G on G. Let $\varphi : G \to S(G)$ be the permutation representation of it. We only need to show that φ is injective.

Take any $x, y \in G$ and assume $\varphi_x = \varphi_y$. Then, $x = x \cdot 1 = \varphi_x(1) = \varphi_y(1) = y \cdot 1 = y$. Therefore, $G \cong \operatorname{im}(\varphi) \leq S(G)$. $\square$

Definition 1.3.8: Center

Let G be a group. The *center* of G is the set

$$Z(G) \triangleq \{ g \in G \mid \forall a \in G,\ ag = ga \}.$$

Theorem 1.3.9

Let G be a group. Then, $Z(G)$ is an abelian group.

Proof. Take any $a, b \in Z(G)$. Then for all $g \in G$, $(ab)g = a(gb) = a(gb) = (ag)b = g(ab)$; hence $ab \in Z(G)$. For all $g \in G$, $ga^{-1} = a^{-1}g(aa^{-1}) = a^{-1}(ga)a^{-1} = a^{-1}g(aa^{-1}) = a^{-1}g$; hence $a^{-1} \in Z(G)$. Therefore, $Z(G) \leq G$ by Theorem 1.3.2. $Z(G)$ is abelian by definition. $\square$

Definition 1.3.10: Centralizer

Let G be a group and let $\varnothing \subsetneq A \subseteq G$. The *centralizer* of A is the subset

$$C_G(A) = C(A) =\triangleq \{ g \in G \mid \forall a \in A,\ ag = ga \}.$$

We may also write $C(a)$ instead of $C(\{a\})$.

End.