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, $i_c \in \mathrm{Aut}(G)$.

End.