Analysis

Gaotang Li

July 23, 2022

Contents

Part I

Foundations

Chapter 1

Groups and Homomorphism

1.1 Basics

Definition 1.1.1 (Group). A pair $(G, \odot)$ consisting of a nonempty set G and an operation $\odot$ is called a **group** if the following holds:

- G is closed under the operation $\odot$
- $\odot$ is associative
- $\odot$ has an identity element e
- Each $g \in G$ has an **inverse** $h \in G$ such that $g \odot h = h \odot g = e$

Definition 1.1.2 (Abelian group). A group $G, \odot$ is called **commutative** or **Abelian** if $\odot$ is a commutative operation on G.

Remark. Let $G = (G, \odot)$

(a) the identity element e is unique

(b) Each $g \in G$ has a unique inverse which we denote by g^b. In particular $e^b = e$.

(c) For each $g \in G$, we have $\left(g^b\right)^b = g$.

(d) For arbitrary group elements g and h, $(g \odot h)^b = h^b \odot g^b$

Example. (a) Let $G := \{e\}$ be a one element set. Then $\{G, \odot\}$ is an Abelian group, the **trivial group**, with the (only possible) operation $e \odot e = e$.

(b) Let X be a nonempty set, and S_X be the set of all bijections from X to itself. Then $S_X := (S_X, \circ)$ is a group with identity element id_X when $\circ$ denotes the composition of functions. Further, the inverse function f^{-1} is the inverse of $f \in S_X$ in the group. When X is finite, the element of S_X are called permutations and S_X is called the **permutation group** of X.

(c) Let X be a nonempty set and $G, \odot$ a group. With the induced operation $\odot$, $\left(G^X, \odot\right)$ is a group. The inverse of $f \in G^X$ is the function

$$f^b \colon X \to G, \quad x \mapsto (f(x))^b$$

(d) Let $G_1, \ldots, G_m$ be groups. Then $G_1 \times \cdots \times G_m$ with the operation defined analogously to (d) is a group called the **direct product** of $G_1, \ldots, G_m$.

1.2 Subgroup

Definition 1.2.1 (Subgroup). Let $G = (G, \odot)$ be a group and H a nonempty subset of G, if

- $H \odot H \subseteq H$
- $h^b \in H$ for all $h \in H$

then $H := (H, \odot)$ is itself a group and is called a **subgroup** of G.

Remark. Here we use the same symbol $\odot$ for the restriction of the operation to H. Since H is nonempty, there is some $h \in H$ and so, from the two axioms above, $e = h^b \odot h$ is also in H.

Example. Let $G = (G, \odot)$ be a group.

(a) The trivial subgroup $\{e\}$ and G itself are subgroups of G, the smallest and largest subgroups with respect to inclusion

(b) If H_α, $\alpha \in A$ are subgroups of G, then $\bigcap_\alpha H_\alpha$ is also a subgroup of G.

1.3 Cosets

Definition 1.3.1 (Coset). Let N be a subgroup of G and $g \in G$. Then $g \odot N$ is the **left coset** and $N \odot g$ is the **right coset** of $g \in G$ with respect to N.

Remark. The definition of coset is related to the particular element.

Note. If we define

$$g \sim h \Leftrightarrow g \in h \odot N \tag{1.1}$$

Then $\sim$ is an equivalence on G.

Proof. $\sim$ is reflexive because $e \in N$
Let $g \in h \odot N$ and $h \in k \odot N$, then

$$g \in (k \odot N) \odot N = k \odot (N \odot N) = k \odot N$$

Let $g \in h \odot N$, then there is some $n \in N$ with $g = h \odot n$. Then it follows that $h = g \odot n^b \in N$. ■

Here 1.1 defines an equivalence relation on G. For the equivalence classes $[\cdot]$ with respect to $\sim$, we have

$$[g] = g \odot N, \quad g \in G. \tag{1.2}$$

For this reason, we denote $G/\sim$ by G/N, and call G/N the **set of left cosets** of G **modulo** N. Particularly, we have subgroups N such that

$$g \odot N = N \odot g, \quad g \in G. \tag{1.3}$$

Such a subgroup 1.3 is called a **normal subgroup** of G. We call $g \odot N$ the **coset of** g **modulo** N since each left coset is a right coset and vice versa. We have a well-defined operation on G/N where N is the normal subgroup of G, induced from $\odot$, such that

$$(G/N) \times (G/N) \to G/N, \quad (g \odot N, h \odot N) \mapsto (g \odot h) \odot N \tag{1.4}$$

Proposition 1.3.1. Let G be a group and N a normal subgroup of G. Then G/N with the induced operation is a group, the **quotient group of G modulo** N.

Proof. It is easy to check that the operation is associative. Since $(e \odot N) \odot (g \odot N) = (e \odot g) \odot N = g \odot N$, the identity element of G/N is $N = e \odot N$. Also

$$\left(g^b \odot N\right) \odot (g \odot N) = \left(g^b \odot g\right) \odot N = N$$

■

Remark. (a) In notion of 1.1, $[e] = N$ is the identity element of G/N and $[g]^b = [g^b]$ is the inverse of $[g] \in G/N$. We also have $[g] \odot h = [g \odot h]$, $g, h \in G$.

(b) Any subgroup N of an Abelian group G is normal and so G/N is a group. Meanwhile, G/N is Abelian.

1.4 Homomorphisms

Definition 1.4.1 (Homomorphism). Let $G = (G, \odot)$ and $G' = (G', \circledast)$ be groups... A function $\varphi\colon G \to G'$ is called a **(group) homomorphism** if

$$\varphi(g \odot h) = \varphi(g) \circledast \varphi(h), \quad g, h \in G$$

Definition 1.4.2 (Endomorphism). A homomorphism from G to itself

Remark. (a) Let e and e' be the identity elements of G and G' respectively, and let $\varphi\colon G \to G'$ be a homomorphism. Then

$$\varphi(e) = e' \quad \text{and} \quad (\varphi(g))^b = \varphi(g^b), \quad g \in G$$

Proof. $e' \circledast \varphi(e) = \varphi(e) = \varphi(e \odot e) = \varphi(e) \circledast \varphi(e)$
$e' = \varphi(e) = \varphi\left(g^b \odot g\right) = \varphi\left(g^b\right) \circledast \varphi(g)$ ■

(b) Let $\varphi\colon G \to G'$ be a homomorphism. The **kernel** of φ, $\ker(\varphi)$, defined by

$$\ker(\varphi) \coloneqq \varphi^{-1}(e') = \{g \in G\,;\ \varphi(g) = e'\}$$

is a normal subgroup of G.

Proof. First, try to prove $\ker(\varphi)$ is a subgroup of G. For all $g, h \in G$,

- $\varphi(g \odot h) = \varphi(g) \circledast \varphi(h) = e' \circledast e' = e'$
- $\varphi\left(g^b\right) = (\varphi(g))^b = (e')^b = e'$

Second, try to prove it is a normal subgroup. Let $h \in g \odot \ker(\varphi)$. Then we there is some $n \in G$ such that $\varphi(n) = e'$ and $h = g \odot n$. For $m \coloneqq g \odot n \odot g^b$, we have

$$\varphi(m) = \varphi(g) \circledast \varphi(n) \circledast \varphi(g^b) = \varphi(g) \circledast \varphi(g^b) = e'$$

and hence $m \in \ker(\varphi)$. Since $m \odot g = g \odot m = h$, this implies that $h \in \ker(\varphi) \odot g$. So $\ker(\varphi) \odot g \subseteq g \odot \ker(\varphi)$. Similarly one can show $g \odot \ker(\varphi) \subset \ker(\varphi) \odot g$. ■

(c) Let $\varphi\colon G \to G'$ be a homomorphism and $N \coloneqq \ker(\varphi)$. Then

$$g \odot N = \varphi^{-1}(\varphi(g)), \quad g \in G,$$

and so

$$g \sim h \Leftrightarrow \varphi(g) = \varphi(h), \quad g, h \in G,$$

where $\sim$ denotes the equivalence relation 1.1.

(d) A homomorphism is injective if and only if its kernel is trivial, that is, $\ker(\varphi) = \{e\}$

(e) The image $\mathrm{im}(\varphi)$ of a homomorphism $\varphi\colon G \to G'$ is a subgroup of G'.

Example. (a) The constant function $G \to G'$, $g \mapsto e'$ is a homorphism, the **trivial** homomorphism.

(b) The identity function $\mathrm{id}_G\colon G \to G$ is an endomorphism.

(c) Compositions of homomorphisms (endomorphisms) are homomorphisms (endomorphisms).

(d) If $\varphi\colon G \to G'$ is a bijective homomorphism, then so is $\varphi^{-1}\colon G \to G'$

Definition 1.4.3 (Isomorphism). A homomorphism $\varphi\colon G \to G'$ is called a (**group**) **isomorphism** from G to G' if φ is bijective.
In this circumstance, we say that the groups G and G' are **isomorphic** and write $G \cong G'$.

Definition 1.4.4 (Automorphism). An isomorphism from G to itself.

Chapter 2

Rings, Fields and Polynomials