Algebra

Chapter 1

Groups

1.1 Groups

Definition 1.1. Let G be a nonempty set. Let $\star$ be a binary operation such that $a \star b \in G$ for all $a, b \in G$. We say that $(G, \star)$ is a **semigroup** if

$$(a \star b) \star c = a \star (b \star c)$$

holds for any $a, b, c \in G$.

Definition 1.2. Let $(G, \star)$ be a semigroup. We say that $(G, \star)$ is a **monoid** if there exists an **identity element** $e \in G$ such that

$$a \star e = a = e \star a$$

for any $a \in G$.

Theorem 1.3. The identity element of a monoid is unique.

Proof. If e and e' are both identity elements of monoid $(G, \star)$, then

$$e = e \star e' = e'.$$ □

Definition 1.4. Let $(G, \star)$ be a monoid and let e be the identity element of G. We say that $(G, \star)$ is a **group** if for any $a \in G$, there exists an **inverse** $b \in G$ such that

$$b \star a = e.$$

Remark. In most cases, $\star$ is either multiplication (denoted by $\cdot$) or addition (denoted by $+$).

- If $\star$ is multiplication, then we denote the identity element by 1_G and denote the inverse of a by a^{-1}.
- If $\star$ is addition, then we denote the identity element by 0_G and denote the inverse of a by $-a$.

In the default settings, $\star$ is considered to be a multiplicative operation.

1.2 Subgroups

Definition 1.5. Let $(G, \star)$ be a group. A **subgroup** of $(G, \star)$ is a group $(H, \star)$ with $H \subseteq G$.

Theorem 1.6. Let $(G, \star)$ be a group and let $H \subseteq G$ be nonempty. Then H is a subgroup of G if and only if for any $a, b \in H$,

$$a \star b \in H \quad \text{and} \quad a^{-1} \in H.$$

Proof. ($\Rightarrow$) Straightforward. ($\Leftarrow$) It is obvious that $(H, \star)$ is a semigroup, and we have

$$e = a^{-1} \star a \in H.$$

where $a \in H$ is an arbitrary element. Thus, $(H, \star)$ is a monoid. Since every element of H has an inverse, $(H, \star)$ is a group. □

Definition 1.7. Let $(G, \star)$ be a group. The **cyclic subgroup** generated by $a \in G$, denoted by $\langle a \rangle$, is defined by

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}.$$

If $G = \langle a \rangle$ for some $a \in G$, then we say that $(G, \star)$ is **cyclic**.

1.3 Cosets

Definition 1.8. Let $(G, \star)$ be a group and let H be a subgroup of G. For any $a \in G$, we define

$$a \star H = \{a \star h : h \in H\}.$$

Theorem 1.9. Let $(G, \star)$ be a group and let H be a subgroup of G. Let $\sim$ be the relation such that for any $a, b \in G$,

$$a \sim b \quad \Leftrightarrow \quad a^{-1} \star b \in H.$$

Then $\sim$ is an equivalence relation on G.

Proof. Assume $a, b, c \in G$. We have $a \sim a$ since $a^{-1} \star a = 1_G \in H$. If $a \sim b$, then $b \sim a$ since

$$b^{-1} \star a = (a^{-1} \star b)^{-1} \in H.$$

Moreover, if $a \sim b$ and $b \sim c$, then $a \sim c$ since

$$a^{-1} \star c = (a^{-1} \star b) \star (b^{-1} \star c) \in H. \qquad \square$$

1.4 Homomorphisms

Definition 1.10. Let $(G, \star_G)$ and $(H, \star_H)$ be groups. A **homomorphism** from G to H is a function $\phi : G \to H$ such that

$$\phi(a \star_G b) = \phi(a) \star_H \phi(b)$$

holds for all $a, b \in G$.

Definition 1.11. Let $(G, \star_G)$ and $(H, \star_H)$ be groups and let $\phi : G \to H$ be a homomorphism.

- If ϕ is injective, then ϕ is called a **monomorphism**.
- If ϕ is surjective, then ϕ is called a **epimorphism**.
- If ϕ is bijective, then ϕ is called a **isomorphism**.

We say that G is **isomorphic** to H, denoted $G \cong H$, if there exists an isomorphism from G to H.