Algebra

Chapter 1

Groups

1.1 Groups

Definition 1.1. Let G be a nonempty set and let $\star : G \times G \to G$ be a binary operation. 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 $e \in G$ be the identity element. 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 addition or multiplication.

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

1.2 Subgroups

Definition 1.5. Let $(G, \star)$ be a group. A **subgroup** of $(G, \star)$ is a group $(H, \diamond)$ such that $H \subseteq G$ and $\diamond : H \times H \to H$ is a restriction of $\star$.

1.3 Homomorphisms

Definition 1.6. Let G and H be groups. A **homomorphism** from G to H is a function $\phi : G \to H$ such that

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

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

Definition 1.7. Let G and 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.