Abstract Algebra Notes

Definition. A **map** $f : A \to B$ is a subset $f \subset A \times B$ such that for all $a \in A$, there exists a $b \in B$ such that b is unique with $(a, b) \in f$.

Definition. We write $f(a) = b$ if $(a, b) \in f$. A is the **domain** of f and B is the **codomain**.

Definition. A **binary operation** on A is a map $\star : A \times A \to A$ such that $\star(a_1, a_2) = a_1 \star a_2$ for $a_1, a_2 \in A$.

Definition. A binary operation $\star$ is **associative** on A if for all $a, b, c \in A$, $a \star (b \star c) = (a \star b) \star c$.

Definition. An element $e \in A$ is an **identity** element of $\star$ if for each $a \in A$, $e \star a = a \star e = a$.

Definition. An element $a \in A$ has an **inverse** under $\star$ if there exists a $b \in A$ such that $a \star b = b \star a = e$.

Definition. A set A with an associative binary operation $\star$ is a **group** if A has an identity element under $\star$ and every $a \in A$ has an inverse.

Definition

A group is a pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G such that

1. For all $a, b, c \in A$, $a \star (b \star c) = (a \star b) \star c$.
2. There exists an $e \in G$ such that $a \star e = e \star a = a$ for all $a \in G$.
3. For all $a \in G$, there exists a $b \in G$ such that $a \star b = b \star a = e$.

Definition. A group $(G, \star)$ is **abelian** or commutative if for all $g, h \in G$, $g \star h = h \star g$.

Theorem. Let $(G, \star)$ be a group.

1. e is unique.
2. g^{-1} is unique.
3. $\forall g \in G, \left(g^{-1}\right)^{-1} = g$.
4. $\forall g, h \in G, (g \star h)^{-1} = h^{-1} \star g^{-1}$.

Proof. We may prove each part separately.

1. Suppose e, e' are identity elements. Then for all $a \in G$,

$$a \star e = e \star a = a \tag{i}$$
$$a \star e' = e' \star a = a \tag{ii}$$

   By (i), $e' = e \star e'$ and by (ii), $e = e \star e'$. Therefore, $e = e'$.

2. Supposed $a \star b = b \star a = e$, then

$$\begin{aligned} b &= b \star e \\ &= b \star (a \star a^{-1}) \\ &= (b \star a) \star a^{-1} \\ &= e \star a^{-1} \\ &= a^{-1} \end{aligned}$$

   Thus, $b = a^{-1}$.

3. $g^{-1} \star \left(g^{-1}\right)^{-1} = e = g^{-1} \star g$. By (ii), $g = \left(g^{-1}\right)^{-1}$.

4. Consider $(a \star b) \star (b^{-1} \star a^{-1})$.

$$\begin{aligned} (a \star b) \star (b^{-1} \star a^{-1}) &= a \star (b \star b^{-1}) \star a^{-1} \\ &= a \star e \star a^{-1} \\ &= a \star a^{-1} \\ &= e \end{aligned}$$

   Thus, $(b^{-1} \star a^{-1}) = (a \star b)^{-1}$.

Definition. Let $[n] = \{1, 2, \ldots, n\}$. The **symmetric group** denoted S_n of degree n is the set of all bijections on $[n]$ under the operation of composition.

$$S_n = \{\sigma : [n] \to [n] \mid \sigma \text{ is a bijection}\}$$

Definition. The **order** of $(G, \star)$ is the number of elements in G denoted $|G|$.

Definition. Let $n \geq 2$. The **dihedral group** of index n is the group of all symmetries of a regular polygon P_n with n vertices in the Euclidean plane.

Symmetries of P_n consist of rotations and reflections.

Choose a vertex v. Let L_0 be the line from the center of P_n through v. Let L_k be L_0 rotated by $\frac{\pi k}{n}$ for $1 \leq k \leq n$. Let σ_k be a reflection about L_k. Let ρ_k be a rotation about $\frac{2\pi k}{n}$, $1 \leq k \leq n$.