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 $\frac{2\pi k}{n}$, $1 \leq k \leq n$.

Definition. A subset $S \subseteq G$ of a group $(G, \star)$ is a set of **generators**, denoted $\langle S \rangle = G$, if and only if every element of G can be written as a product of elements of S and their inverses.

Definition. Any equation satisfied by generators is called a **relation**.

Definition. A **presentation** of G, denoted $\langle S \mid R\rangle$, is a set of generators of G and relations such that any other relation can be derived by those given.

Example.

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle$$

Definition. The cycles $\sigma = (\sigma_1\ \sigma_2\ \dots\ \sigma_n)$ and $\tau = (\tau_1\ \tau_2\ \dots\ \tau_n)$ are **disjoint** if $\sigma_i \neq \tau_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$.

Definition. A cycle of length 2 is called a **transposition**.

Definition. An expression of the form $(a_1\ a_2\ \dots\ a_m)$ is called a **cycle of length m** or an **m-cycle**.

Proposition. Let $\alpha = (a_1\ a_2\ \dots\ a_m)$ and $\beta = (b_1\ b_2\ \dots\ b_n)$. If $a_i \neq b_j$ for any i, j, then $\alpha\beta = \beta\alpha$.

Proposition. Every permutation can be written as a product of disjoint cycles.

Proposition. A cycle of length n has order n.

Proposition. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be disjoint cycles. Then,

$$|\alpha_1\alpha_2 \dots \alpha_n| = \operatorname{lcm}(|\alpha_1|, |\alpha_2|, \dots, |\alpha_n|)$$

Proposition. Every permutation is S_n is a product of 2-cycles (which are not necessarily disjoint).

Proposition. If $\alpha = \beta_1\beta_2 \dots \beta_r = \gamma_1\gamma_2 \dots \gamma_s$ where β_i, γ_j are transpositions, then r and s have the same parity.

Definition. If r and s are both odd, α is called an **odd permutation**. If r and s are both even, α is called an **even permutation**.

Definition. The set of even permutations in S_n form a group called the **alternating group**, denoted A_n.

Note. $|A_n| = \frac{n!}{2}$ for $n > 1$.

Definition

Let $(G, \star)$ and $(G', *)$ be groups. A map of sets $\varphi : G \to G'$ is a **group homomorphism** if for all $a, b \in G$,

$$\varphi(a \star b) = \varphi(a) * \varphi(b)$$

Example. The following are two very simple examples of homomorphisms.

Trivial Homomorphism

$$\varphi : G \to G', \varphi(g) = e, \forall g \in G$$

Identity Homomorphism

$$\varphi : G \to G', \varphi(g) = g, \forall g \in G$$

Definition. If $\varphi : G \to G'$ is a homomorphism, the **domain** of φ is $\text{Dom}(\varphi) = G$, the **codomain** of φ is $\text{Codom}(\varphi) = G'$, the **range** or **image** of φ is $\varphi(G) = \{\varphi(g) : g \in G\} \subseteq G'$ denoted $\text{Range}(\varphi)$ or $\text{Im}(\varphi)$.

Definition

A homomorphism which is bijective is called an **isomorphism**.

$\varphi : G \to G'$ is an isomorphism if and only if there exists $\psi : G' \to G$ such that ψ is a homomorphism and $\varphi \circ \psi = 1_{G'}$, $\psi \circ \varphi = 1_G$, i.e. ψ is an inverse homomorphism to φ. We say G is isomorphic to G' by $G \cong G'$ or $\phi : G \xrightarrow{\sim} G'$.

Definition. Let $(G, \star)$ be a group. A subset $H \subseteq G$ is a **subgroup** if $(H, *)$ is also a group.

If $H \neq \emptyset$ and $H \subseteq G$, $H \leq G$ or H is a subgroup of G if and only if

1. H is closed under $\star$ ($\forall h_1, h_2 \in H, h_1 \star h_2 \in H$).
2. H is closed under inverses ($h \in H \Rightarrow h^{-1} \in H$).

Note. The following is notation for arbitrary and abelian groups.

$$x \star y \to xy \text{ for arbitrary } G,\ x + y \text{ for abelian } G$$
$$e \to 1 \text{ for arbitrary } G,\ 0 \text{ for abelian } G$$

For an arbitrary subset $A \subseteq G$, and $g \in G$,

$$gA = \{ga : a \in A\} \qquad Ag = \{ag : a \in A\} \qquad gAg^{-1} = \{gag^{-1} : a \in A\}$$

Theorem

Let $\emptyset \neq H \subseteq G$, $H \leq G$ if and only if $\forall x, y \in H$, $xy^{-1} \in H$.