

# CHAPTER I

## Groups

### 1.1 Definitions and Examples

**Definition 1.1.1.** A **binary operation**  $*$  on a set  $S$  is a function from  $S \times S$  into  $S$ .  $(S, *)$  is then called a **binary structure**.

**Definition 1.1.2.** Let  $*$  be a binary operation on a nonempty set  $S$ .

$*$  is **associative** if  $(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$

$*$  is **commutative** if  $a * b = b * a \quad \forall a, b \in S$ .

An element  $e$  of  $S$  is an **identity element** for  $*$  if

$$e * x = x = x * e \quad \forall x \in S.$$

**Definition 1.1.3.** A binary structure  $(S, *)$  is called a **semigroup** if  $*$  is associative. A **monoid** is a semigroup that has an identity element.

**Definition 1.1.4.** A monoid  $(G, *)$  with the identity element is said to be a **group** if for each  $a \in G$ , there is  $b \in G$  such that

$$a * b = e = b * a.$$

This element  $b$  is called an **inverse** of  $a$ .

**Remark.** It is customary to denote a group  $(G, *)$  by its underlying set  $G$  and  $x * y$  by  $xy$  if there is no ambiguity.

**Definition 1.1.5.** The **order** of a group  $G$  is the cardinality of the set  $G$  and denoted  $|G|$ .

**Definition 1.1.6.** A group  $(G, *)$  is a **abelian** if  $*$  is commutative (ie.  $a * b = b * a \quad \forall a, b \in G$ ).

**Theorem 1.1.7.** Let  $(G, *)$  be a semigroup. Then the following are equivalence

- (i)  $(G, *)$  is a group.
- (ii) there is  $e_\ell \in G$  such that  $e_\ell a = a$  for all  $a \in G$ , and for each  $a \in G$ , there is  $a' \in G$  such that  $a'a = e_\ell$ .
- (iii) there is  $e_r \in G$  such that  $ae_r = a$  for all  $a \in G$ , and for each  $a \in G$ , there is  $b \in G$  such that  $ab = e_r$ .

## 1.2 Elementary Properties of Groups.

**Theorem 1.2.1.** In any group  $G$ , the following hold:

- (i) The identity element is unique.
- (ii) Each element  $a$  of  $G$  has a unique inverse. It will be denoted  $a^{-1}$ .

**Theorem 1.2.2.** Let  $a, b$  and  $c$  be elements of a group.  $ab = ac$  or  $ba = ca$  implies  $b = c$ .

**Theorem 1.2.3.** Let  $a$  and  $b$  be elements of a group  $G$ .

- (i)  $e^{-1} = e$ .
- (ii)  $(a^{-1})^{-1} = a$ .
- (iii)  $(ab)^{-1} = b^{-1}a^{-1}$ .

**Notation.** For each element  $a$  in a group  $G$ ,

$$\begin{aligned} a^0 &= e, & a^1 &= a \\ a^{n+1} &= (a^n)a & \text{for all } n \in \mathbb{N} \\ a^{-n} &= (a^{-1})^n & \text{for all } n \in \mathbb{N} \end{aligned}$$

**Theorem 1.2.4.** *Let  $a$  and  $b$  be elements of a group.*

- (i)  $(a^n)^{-1} = (a^{-1})^n (= a^{-n})$  for all  $n \geq 0$ .
- (ii)  $a^m a^n = a^{m+n}$  for all  $m, n \in \mathbb{Z}$ .
- (iii)  $(a^m)^n = a^{mn}$  for all  $m, n \in \mathbb{Z}$ .
- (iv) If  $ab = ba$ , then  $(ab)^n = a^n b^n$  for all  $n \in \mathbb{Z}$ .

**Theorem 1.2.5.** *Let  $G$  be a group and  $a \in G$ . If  $n$  is the smallest positive integer such that  $a^n = e$ , then*

$$a^k = e \text{ if and only if } n \mid k.$$

**Theorem 1.2.6.** *Let  $a$  and  $b$  be elements of group  $G$ .*

- (i) *The equation  $ax = b$  has a unique solution  $x = a^{-1}b$ .*
- (ii) *The equation  $xa = b$  has a unique solution  $x = b^{-1}a$ .*

### 1.3 Subgroups

**Definition 1.3.1.** If a subset  $H$  of a group  $G$  is itself a group under the operation of  $G$ , we say that  $H$  is a **subgroup** of  $G$ , denoted  $H \leq G$ .

**Theorem 1.3.2.** Let  $H$  be a subset of  $G$ . TFAE

(i)  $H$  is a subgroup of  $G$ .

(ii)  $ab \in H$  for all  $a, b \in H$  and  $a^{-1} \in H$  for all  $a \in H$ .

(iii)  $ab^{-1} \in H$  for all  $a, b \in H$ .

**Theorem 1.3.3.** Let  $H$  be a nonempty finite subset of a group  $G$ . If  $H$  is closed under the operation of  $G$ , then  $H \leq G$ .

**Theorem 1.3.4.** Let  $a$  be an element of a group  $G$ . Then

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

is the smallest subgroup of  $G$  containing  $a$ . It is called the **cyclic subgroup of  $G$  generated by  $a$** .

**Definition 1.3.5.** Let  $a$  be an element of a group  $G$ . The **order** of  $a$ , denoted  $\circ(a)$  is the smallest positive integer  $n$  such that  $a^n = e$  (if it exist). If no such that integer exists, we say that  $a$  has **infinite order**.

**Theorem 1.3.6.** Let  $G$  be a group and  $a \in G$ . Then  $|\langle a \rangle| = \circ(a)$ . In particular

$$\langle a \rangle = \begin{cases} \{e, a, a^2, \dots, a^{n-1}\} & \text{if } \circ(a) = n, \\ \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\} & \text{if } \circ(a) \text{ is infinite.} \end{cases}$$

**Theorem 1.3.7.** *Let  $a$  be an element of order  $n$  in a group  $G$ . Then*

(i)  $a^k = e$  if and only if  $n \mid k$ .

(ii)  $a^k = a^m$  if and only if  $k \equiv m \pmod{n}$ .

**Theorem 1.3.8.** *The **center** of a group  $G$ ,  $Z(G)$*

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

*is a subgroup of  $G$ .*

**Theorem 1.3.9.** *Let  $H$  and  $K$  be subgroups of a group  $G$ . Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

**Theorem 1.3.10.** *Let  $H$  and  $K$  be subgroups of a group  $G$ . Then  $HK$  is a subgroup of  $G$  if and only if  $HK = KH$ .*

## 1.4 Homomorphisms and Isomorphisms

**Definition 1.4.1.** *Let  $(G, \circ)$  and  $(G', *)$  be groups. A mapping  $\phi : G \rightarrow G'$  is called a **homomorphism** if*

$$\phi(a \circ b) = \phi(a) * \phi(b) \text{ for all } a, b \in G.$$

**Definition 1.4.2.** *Let  $\phi : G \rightarrow G'$  be a group homomorphism. The **kernel** of  $\phi$ , denoted  $\text{Ker } \phi$  is defined by*

$$\text{Ker } \phi = \{g \in G \mid \phi(g) = e'\}$$

*where  $e'$  is the identity element of  $G'$ .*

**Definition 1.4.3.** A bijective (1-1 and onto) homomorphism is called an **isomorphism**.  $G$  and  $G'$  is then said to be **isomorphic**, denoted  $G \cong G'$ . An isomorphism from a group  $G$  into it self is called an **automorphism**. The set of all automorphisms is denoted by  $\text{Aut}(G)$ .

Isomorphism preserves **algebraic property** e.g. order of group, order of element, commutativity etc.

**Theorem 1.4.4.** For any group  $G$ ,  $\text{Aut}(G)$  is a group under composition.

**Theorem 1.4.5.** The isomorphism relation  $\cong$  is an equivalence for groups.

**Theorem 1.4.6. Cayley's Theorem**

Every group is isomorphic to a subgroup of a permutation group. If a group is of order  $n$ , then it is isomorphic to a subgroup of  $S_n$ .

## 1.5 Cyclic Groups and generators

**Definition 1.5.1.** A group  $G$  is called a **cyclic group** if  $G = \langle a \rangle$  for some  $a \in G$ .  $a$  is then called a **generator** of  $G$ .

**Theorem 1.5.2.** Every cyclic group is abelian.

**Theorem 1.5.3.** A subgroup of a cyclic group is cyclic.

**Theorem 1.5.4.** Let  $G = \langle a \rangle$  be a cyclic group of order  $n$ .

(i)  $|\langle a^s \rangle| = \frac{n}{d}$  where  $d = \text{g.c.d.}(n, s)$ ,  $0 < s < n$ .

(ii) If  $k|n$ , then  $\langle a^{\frac{n}{k}} \rangle$  is the unique subgroup of  $G$  of order  $k$ .

(iii) The set of generators of  $G$  is  $\{a^k \mid \text{g.c.d.}(n, k) = 1\}$ .

**Theorem 1.5.5.** (i)  $(\mathbb{Z}, +)$  is the only infinite cyclic group.

(ii)  $(\mathbb{Z}_n, +)$  is the only cyclic group of order  $n$ .

**Definition 1.5.6.** Let  $X$  be a nonempty subset of a group  $G$ . The smallest subgroup of  $G$  containing  $X$ , denoted  $\langle X \rangle$  is called the **subgroup of  $G$  generated by  $X$** .

**Theorem 1.5.7.** Let  $X$  be a nonempty subset of a group  $G$ . Then

$$\langle X \rangle = \{x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} \mid x_i \in X, k_i \in \mathbb{Z}, n \geq 1\}.$$

**Definition 1.5.8.** A group  $G$  is called **finitely generated** if there is a finite subset  $X$  of  $G$  such that  $G = \langle X \rangle$ . We call  $X$  a set of generators for  $G$ . If  $X$  is finite,  $G$  is called a **finite generated group** and denoted  $G = \langle x_1, x_2, \dots, x_n \rangle$ .

**Theorem 1.5.9.** Let  $\sigma : G \rightarrow G_1$  and  $\tau : G \rightarrow G_1$  be homomorphism. Assume that  $G = \langle X \rangle$ . Then

$$\sigma = \tau \quad \text{if and only if} \quad \sigma(x) = \tau(x) \quad \text{for all } x \in X.$$

A group homomorphism  $\sigma : \langle X \rangle \rightarrow G_1$  is completely determined by its effect on  $X$ .

## 1.6 Direct Products

**Theorem 1.6.1.** *Let  $G_1, G_2, \dots, G_n$  be groups. Then  $G_1 \times G_2 \times \dots \times G_n$  is a group under the componentwise operation, that is*

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n).$$

*This group is called the **(external) direct product** of  $G_1, G_2, \dots, G_n$ .*

**Theorem 1.6.2.** *Let  $G_1, G_2, \dots, G_n$  be finite groups and  $(g_1, g_2, \dots, g_n)$  be an element of the group  $G_1 \times G_2 \times \dots \times G_n$ . Then*

$$\circ((g_1, g_2, \dots, g_n)) = \text{l.c.m.}(\circ(g_1), \circ(g_2), \dots, \circ(g_n)).$$

**Theorem 1.6.3.** *Let  $G_1$  and  $G_2$  be finite cyclic groups. Then  $G_1 \times G_2$  is cyclic if and only if  $|G_1|$  and  $|G_2|$  are relatively prime.*

**Corollary 1.6.4.** *The external direct product  $G_1 \times G_2 \times \dots \times G_n$  is cyclic if and only if  $|G_1|, |G_2|, \dots, |G_n|$  are pairwise relatively prime.*

**Theorem 1.6.5.** *Let  $H$  and  $K$  be subgroups of a group  $G$ . Assume that*

$$(i) \quad G = HK,$$

$$(ii) \quad H \cap K = \{e\},$$

$$(iii) \quad hk = kh \quad \text{for all } h \in H, k \in K.$$

*Then  $G \cong H \times K$ .*

*In this case, we say that  $G$  is the **internal direct product** of  $H$  and  $K$ .*



**Definition 1.6.6.** Let  $H_1, H_2, \dots, H_n$  be subgroups of a group  $G$ . We say  $G$  is the **internal direct product** of  $H_1, H_2, \dots, H_n$  if

- (i)  $G = H_1 H_2 \cdots H_n$ ,
- (ii)  $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$  for  $i = 1, 2, \dots, n - 1$ .
- (iii)  $h_i h_j = h_j h_i$  for all  $h_i \in H_i, h_j \in H_j, i \neq j$ .

## 1.7 Cosets and Lagrange's Theorem

**Definition 1.7.1.** Let  $H$  be a subgroup of a group  $G$  and  $g \in G$ . The **right coset**,  $Hg$ , of  $H$  generated by  $g$  and the **left coset**,  $gH$ , of  $H$  generated by  $g$  are defined as follows :

$$Hg = \{hg \mid h \in H\} \quad \text{and} \quad gH = \{gh \mid h \in H\}.$$

**Theorem 1.7.2.** Let  $H$  be a subgroup of a group  $G$  and  $a, b \in G$ .

- (i)  $a \in Ha$ .
- (ii)  $Ha = H$  iff  $a \in H$  [ $aH = H$  iff  $a \in H$ ].
- (iii)  $Ha = Hb$  iff  $ab^{-1} \in H$  [ $aH = bH$  iff  $a^{-1}b \in H$ ].
- (iv) If  $a \in Hb$ , then  $Ha = Hb$ . [If  $a \in bH$ , then  $aH = bH$ ].
- (v) Either  $Ha = Hb$  or  $Ha \cap Hb = \emptyset$  [Either  $aH = bH$  or  $aH \cap bH = \emptyset$ ].
- (vi) The set of distinct right(left) cosets of  $H$  is a partition of  $G$ .
- (vii) The set of all distinct right cosets and the set of all distinct left cosets have the same cardinality.

**Corollary 1.7.3.**  $Ha = Hb$  if and only if  $a^{-1}H = b^{-1}H$ .

**Definition 1.7.4.** let  $H$  be a subgroup of a group  $G$ . The **index** of  $H$ , denoted  $[G : H]$  is the cardinality of the set of all distinct right(left) cosets of  $H$ .

**Lemma 1.7.5.** *Let  $H \leq G$  and  $g \in H$ . Then*

$$\text{card } Hg = \text{card } H = \text{card } gH.$$

**Theorem 1.7.6. Lagrange**

*Let  $H$  be a subgroup of a finite group  $G$ . Then  $|H|$  divides  $|G|$ . In particular,*

$$|G| = [G : H] \cdot |H|.$$

**Corollary 1.7.7.** *Let  $G$  be a group of order  $n$ .*

(i)  $\circ(a)$  divides  $n \quad \forall a \in G$ .

(ii)  $a^n = e \quad \forall a \in G$ .

**Theorem 1.7.8.** *let  $H$  and  $K$  be subgroups of a group  $G$ .*

(i) *If  $H \subseteq K$ , then  $[G : H] = [G : K][K : H]$ .*

(ii) *If  $\text{g.c.d}(|H|, |K|) = 1$ , then  $H \cap K = \{e\}$ .*

## 1.8 Normal Subgroups and Factor Groups

**Definition 1.8.1.** *A subgroup  $N$  of a group  $G$  is called a **normal subgroup** if  $gN = Ng$  for all  $g \in G$ . We write  $N \triangleleft G$ .*

**Theorem 1.8.2.** *Every subgroup of an abelian group is normal.*

**Theorem 1.8.3.**  *$Z(G)$  is normal in  $G$ .*

**Theorem 1.8.4.** *Let  $N$  be a subgroup of a group  $G$ . Then TFAE*

(i)  *$N$  is normal in  $G$ .*

(ii)  *$gNg^{-1} = N$  for all  $g \in G$ .*

(iii)  *$gNg^{-1} \subseteq N$  for all  $g \in G$ .*

**Theorem 1.8.5.** *If  $H$  is a subgroup of index 2 in  $G$ , then  $H$  is normal in  $G$ .*

**Theorem 1.8.6.** *Let  $N \triangleleft G$  and  $G/N = \{Ng \mid g \in G\}$ . Then  $G/N$  is a group under the operation*

$$Na \cdot Nb = Nab.$$

*This group is called the **factor group(quotient group) of  $G$  by  $N$** . In addition, if  $G$  is finite, then  $|G/N| = \frac{|G|}{|N|}$ .*

**Theorem 1.8.7.** *Let  $N \triangleleft G$ .*

(i)  $\phi : G \rightarrow G/N$  defined by  $\phi(a) = Na$  is an onto homomorphism, called the natural homomorphism

(ii) If  $G$  is abelian, then  $G/N$  is abelian.

(iii) If  $G = \langle a \rangle$ , then  $G/N = \langle Na \rangle$ .

(iv)  $\bar{H}$  is a subgroup of  $G/N$  if and only if  $\bar{H} = H/N$  for some subgroup  $H$  of  $G$  containing  $N$ .

(v)  $HN$  is a subgroup of  $G$  for all subgroups  $H$  of  $G$ .

**Theorem 1.8.8.** *Let  $G$  be a group. If  $G/Z(G)$  is cyclic, then  $G$  is abelian.*

**Theorem 1.8.9.** *Let  $H$  and  $K$  be subgroups of a group  $G$ .*

(i) If  $H$  or  $K$  is normal in  $G$ , then  $HK = KH$  is a subgroup of  $G$ .

(ii) If  $H$  and  $K$  are normal in  $G$ , then  $HK$  is normal in  $G$ .

**Theorem 1.8.10.** *Let  $H$  and  $K$  be normal subgroups of  $G$  and  $H \cap K = \{e\}$ . Then  $hk = kh$  for all  $h \in H, k \in K$ . Consequently, if in addition  $G = HK$ , then  $G \cong H \times K$ .*

## 1.9 Cauchy's Theorem and Conjugates

**Definition 1.9.1.** Let  $a$  and  $b$  be elements of a group  $G$ .  $b$  is said to be a **conjugate of  $a$**  if  $b = xax^{-1}$  for some  $x \in G$ .

**Theorem 1.9.2.** The relation  $\sim$  defined on a group  $G$  by

$$a \sim b \text{ if and only if } b = xax^{-1} \text{ for some } x \in G$$

is an equivalence relation on  $G$ . The equivalence class of  $a$ , denoted  $Cl(a)$  is called a **conjugacy class** of  $a$ .

**Theorem 1.9.3.** Let  $G$  be a finite group. Then

$$|Cl(a)| = [G : C_G(a)] \quad \text{for all } a \in G$$

where  $C_G(a) = \{g \in G \mid gag^{-1} = a\}$ .

In particular,  $a \in Z(G)$  if and only if  $Cl(a) = \{a\}$ .

**Theorem 1.9.4.** Let  $G$  be a finite group and  $Cl(a_1), \dots, Cl(a_n)$  be distinct non-singleton conjugacy classes in  $G$ . Then

$$|G| = |Z(G)| + \sum_{i=1}^n [G : C_G(a_i)].$$

**Theorem 1.9.5. Cauchy's Theorem**

Let  $G$  be a group of order  $n$ . If  $p$  is a prime divisor of  $n$ , then  $G$  has an element of order  $p$ .

**Theorem 1.9.6.** If  $G \neq \{e\}$  is a group of prime power order, then  $Z(G) \neq \{e\}$ .

**Theorem 1.9.7.** If  $G$  is a group of order  $p^2$ , where  $p$  is a prime, then  $G$  is abelian.

## CHAPTER II

### Isomorphism Theorems

#### 2.1 Properties of homomorphisms

Recall that a mapping  $\phi : G \rightarrow G'$  is called a homomorphism if

$$\phi(xy) = \phi(x)\phi(y) \quad \text{for all } x, y \in G.$$

The kernel,  $\text{Ker}\phi$ , of  $\phi$  is  $\phi^{-1}[\{e\}]$ . An isomorphism is a bijective homomorphism.

**Theorem 2.1.1.** *Let  $\phi$  be a homomorphism from a group  $G$  to a group  $G'$ .*

- (i)  $\phi(e) = e'$  where  $e$  and  $e'$  are identities in  $G$  and  $G'$ , respectively.
- (ii)  $\phi(x^{-1}) = (\phi(x))^{-1}$  for all  $x \in G$ .
- (iii)  $\phi(x_1x_2 \cdots x_n) = \phi(x_1)\phi(x_2) \cdots \phi(x_n)$  for all  $x_1, x_2, \dots, x_n \in G$ .
- (iv) If  $H \leq G$ , then  $\phi[H] \leq G'$ . In particular,  $\text{Im}\phi$  is a subgroup of  $G'$ .
- (v) If  $H' \leq G$ , then  $\text{Ker}\phi \subseteq \phi^{-1}[H'] \leq G$ .
- (vi)  $\phi$  is 1-1 if and only if  $\text{Ker}\phi = \{e\}$ .

**Corollary 2.1.2.** *Let  $\phi : G \rightarrow G'$  be a group homomorphism and  $g \in G$ .*

- (i)  $\phi(g^n) = (\phi(g))^n$  for all  $n \in \mathbb{Z}$ .
- (ii) If  $g$  has a finite order, then  $\phi(g)$  has a finite order and  $\circ(\phi(g))$  divides  $\circ(g)$ .

**Theorem 2.1.3.** *if  $\psi : G \rightarrow G'$  is a group homomorphism, then  $\text{Ker}\psi$  is a normal subgroup.*

## 2.2 Isomorphism Theorems

### **Theorem 2.2.1. First Isomorphism Theorem**

Let  $\phi : G \rightarrow G'$  be a group homomorphism. Then  $G/\text{Ker}\phi \cong \text{Im}\phi$ .

### **Theorem 2.2.2. Second Isomorphism Theorem**

Let  $H$  and  $N$  be subgroups of  $G$  with  $N$  normal. Then  $H \cap N$  is normal in  $H$  and

$$H/H \cap N \cong HN/N.$$

### **Theorem 2.2.3. Third Isomorphism Theorem**

Let  $N \triangleleft G$ . then the map  $H \mapsto H/N$  gives a 1-1 correspondence between the set of subgroups of  $G$  containing  $N$  and the set of subgroups of  $G/N$ .

Moreover, this correspondence carries normal subgroups to normal subgroups.

If  $H \triangleleft G$  and  $N \subseteq H \subseteq G$ , then

$$G/H \cong (G/N) / (H/N).$$

## CHAPTER III

# Permutation Groups

### 3.1 Definitions and Notations

**Definition 3.1.1.** A *permutation* on a nonempty set  $X$  is a bijection on  $X$ . The set  $S(X)$  of all permutations on  $X$  is a group under composition, called the *symmetric group on  $X$* . Any subgroup of  $S(X)$  is called a *permutation group on  $X$* .

**Remark.** If sets  $A$  and  $B$  have the same cardinality, then  $S(A) \cong S(B)$ . When  $X$  is finite,  $S(X)$  can be considered as the symmetric group on  $\{1, 2, \dots, n\}$ . It will be denoted by  $S_n$ , called the **symmetric group of degree  $n$** . The order of  $S_n$  is  $n!$ .  $S_n$  is nonabelian where  $n \geq 3$ . Each  $\sigma$  in  $S_n$  can be represented in matrix form as

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

**Theorem 3.1.2. Cayley's Theorem**

*Every group is isomorphic to a permutation group.*

## 3.2 Cycles

**Definition 3.2.1.** A permutation  $\sigma$  in  $S_n$  is a **cycle** if there exist  $a_1, a_2, \dots, a_r$  in  $\{1, 2, \dots, n\}$  satisfying

$$(i) \sigma(a_i) = a_{i+1} \text{ for all } i \in \{1, 2, \dots, r-1\},$$

$$(ii) \sigma(a_r) = a_1, \text{ and}$$

$$(iii) \sigma(x) = x \text{ otherwise}$$

$r$  is then the **length of the cycle**.  $\sigma$  will be denoted by  $(a_1, a_2, \dots, a_r)$  and sometimes referred to as  $r$ -cycle.

### Remarks.

(i) The identity permutation is the only cycle of length 1 and will be denoted (1).

(ii)  $(a_1, a_2, \dots, a_r) = (b_1, b_2, \dots, b_s)$  iff  $r = s$  and there exists  $t$  such that  $b_i = a_{t+i}$  for all  $i = 1, 2, \dots, r$ .

(iii)  $(a_1, a_2, \dots, a_r)^{-1} = (a_r, a_{r-1}, \dots, a_1)$ .

(iv) The order of  $r$ -cycle is  $r$ .

**Definition 3.2.2.** Let  $\alpha = (a_1, a_2, \dots, a_r)$  and  $\beta = (b_1, b_2, \dots, b_s)$  be nonidentity permutation in  $S_n$ .  $\alpha$  and  $\beta$  are said to be **disjoint** if  $a_i \neq b_j$  for all  $i, j$ .

**Theorem 3.2.3.** Disjoint cycles commute.

**Theorem 3.2.4.** The order of a product of disjoint cycle is the l.c.m. of the length of cycles.



### 3.3 Properties of Permutations

From now on permutations are in  $S_n$  where  $n \geq 2$ .

**Theorem 3.3.1.** *Every permutation is a cycle or a product of disjoint cycles. This cycle decomposition is unique upto rearranging its cycles and cyclically permuting the numbers within each cycle.*

**Definition 3.3.2.** *A 2-cycle is called a **transposition**.*

**Theorem 3.3.3.** *Every permutation is either transposition or a product of transpositions.*

### 3.4 Alternating Groups

**Lemma 3.4.1.** *The identity permutation is always a product of an even number of transposition.*

**Theorem 3.4.2.** *If a permutation  $\alpha$  is a product of an even number of transpositions, then every decomposition of  $\alpha$  into a product of transpositions must have an even number of transpositions.  $\alpha$  is then called an **even permutation**.*

**Definition 3.4.3.** *A permutation which can be decomposed into a product of an odd number of transpositions is called an **odd permutation**.*

**Theorem 3.4.4.** *The set of even permutations in  $S_n$  form a normal subgroup of order  $\frac{n!}{2}$  of  $S_n$  called the **Alternating group of degree  $n$** , denoted  $A_n$ .*