

# Dummit and Foote Abridged

June 7, 2024

## Contents

<b>0 Preliminaries</b>	<b>1</b>
0.1 Basics . . . . .	1
<b>1 Group Theory</b>	<b>2</b>
1.1 Basic Axioms and Examples . . . . .	2
1.6 Homomorphism and Isomorphisms . . . . .	3
1.7 Group Actions . . . . .	3
<b>2 Subgroups</b>	<b>3</b>
2.1 Definition and Examples . . . . .	3
2.2 Centralizers and Normalizers, Stabilizers and Kernels . . . . .	4
2.3 Cyclic Groups and Cyclic Subgroups . . . . .	4
2.4 Subgroups Generated by Subsets of a Group . . . . .	5
<b>3 Quotient Groups and Homomorphisms</b>	<b>5</b>
3.1 Definitions and Examples . . . . .	5
3.2 More on Cosets and Lagrange's Theorem . . . . .	7
3.3 The Isomorphism Theorems . . . . .	8
3.4 Composition Series and the Hölder Program . . . . .	9
3.5 Transpositions and the Alternating Group . . . . .	9
<b>4 Group Actions</b>	<b>10</b>
4.1 Group Actions and Permutation Representations . . . . .	10
4.2 Group Acting on Themselves by Left Multiplication - Cayley's Theorem .	11
4.3 Groups Acting on Themselves by Conjugation - The Class Equation . . .	12

## 0 Preliminaries

### 0.1 Basics

**Proposition 1.** Let  $f: A \rightarrow B$ .

1. The map  $f$  is injective if and only if  $f$  has a left inverse.
2. The map  $f$  is surjective if and only if  $f$  has a right inverse.

3. The map  $f$  is a bijection if and only if there exist  $g: B \rightarrow A$  such that  $f \circ g$  is the identity map on  $B$  and  $g \circ f$  is the identity map on  $A$ .
4. If  $A$  and  $B$  are finite sets with the same number of elements then  $f: A \rightarrow B$  is bijective if and only if  $f$  is injective if and only if  $f$  is surjective.

**Proposition 2.** Let  $A$  be a nonempty set.

1. If  $\sim$  defines an equivalence relation on  $A$  then the set of equivalence classes of  $\sim$  form a partition of  $A$ .
2. If  $\{A_i \mid i \in I\}$  is a partition of  $A$  then there is an equivalence relation on  $A$  whose equivalence classes are precisely the sets  $A_i, i \in I$

# 1 Group Theory

## 1.1 Basic Axioms and Examples

**Definition.**

1. A *binary operation*  $\star$  on a set  $G$  is a function  $\star: G \times G \rightarrow G$ . For any  $a, b \in G$  we shall write  $a \star b$  for  $\star(a, b)$ .
2. A binary operation  $\star$  on a set  $G$  is associative if for all  $a, b, c \in G$  we have  $a \star (b \star c) = (a \star b) \star c$ .
3. If  $\star$  is a binary operation on a set  $G$  we say elements  $a$  and  $b$  of  $G$  *commute* if  $a \star b = b \star a$ . We say  $\star$  (or  $G$ ) is *commutative* if for all  $a, b \in G$ ,  $a \star b = b \star a$ .

**Proposition 1.** If  $G$  is a group under the operation  $\cdot$ , then

1. The identity of  $G$  is unique
2. for each  $a \in G$ ,  $a^{-1}$  is uniquely determined
3.  $(a^{-1})^{-1} = a$  for all  $a \in G$
4.  $(a \cdot b)^{-1} = (b^{-1}) \cdot (a^{-1})$
5. for any  $a_1, a_2, \dots, a_n \in G$  the value of  $a_1 a_2 \cdots a_n$  is independent of how the expression is bracketed

**Proposition 2.** Let  $G$  be a group and let  $a, b \in G$ . The equations  $ax = b$  and  $ya = b$  have unique solutions for  $x, y \in G$ . In particular, the left and right cancellation laws hold in  $G$ , i.e.,

1. if  $au = av$ , then  $u = v$ , and
2. if  $ub = vb$ , then  $u = v$ .

**Definition.** For  $G$  a group and  $x \in G$  define the *order* of  $x$  to be the smallest positive integer  $n$  such that  $x^n = 1$ , denoted  $|x|$ . If there is no such integer then we define the order of  $x$  to be infinity.

## 1.6 Homomorphism and Isomorphisms

**Definition.** Let  $(G, \star)$  and  $(H, \diamond)$  be groups. A map  $\phi: G \rightarrow H$  such that  $\phi(x \star y) = \phi(x) \diamond \phi(y)$ , for all  $x, y \in G$  is called a *homomorphism*. Moreover, if  $\phi$  is bijective it is called an *isomorphism* and we say that  $G$  and  $H$  are *isomorphic* or of the same *isomorphism type*, written  $G \cong H$ .

**Note.** If  $\phi: G \rightarrow H$  is an isomorphism then

1.  $|G| = |H|$
2.  $G$  is abelian if and only if  $H$  is abelian
3. for all  $x \in G$ ,  $|x| = |\phi(x)|$

## 1.7 Group Actions

**Definition.** A *group action* of a group  $G$  on a set  $A$  is a map from  $G \times A$  to  $A$  (written as  $g \cdot a$ , for all  $g \in G$  and  $a \in A$ ) satisfying the following properties:

1.  $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ , for all  $g_1, g_2 \in G, a \in A$ , and
2.  $1 \cdot a = a$  for all  $a \in A$ .

**Note.** Let the group  $G$  act on the set  $A$ . From each fixed  $g \in G$  we get a map  $\sigma_g$  defined by

$$\begin{aligned}\sigma_g: A &\rightarrow A \\ \sigma_g(a) &= g \cdot a.\end{aligned}$$

The following are true

1. for each fixed  $g \in G$ ,  $\sigma_g$  is a permutation of  $A$ , and
2. the map from  $G$  to  $S_A$  defined by  $g \mapsto \sigma_g$  is a homomorphism. Moreover this map is called the *permutation representation* associated to the given action.

**Note.** As a consequence of the above remark, if  $\phi: G \rightarrow S_A$  is a homomorphism (here  $S_A$  is the symmetric group on the set  $A$ ), then the map from  $G \times A$  to  $A$  defined by

$$g \cdot a = \phi(g)(a) \text{ for all } g \in G, \text{ and all } a \in A$$

is a group action of  $G$  on  $A$ .

## 2 Subgroups

### 2.1 Definition and Examples

**Definition.** Let  $G$  be a group. The subset  $H$  of  $G$  is a *subgroup* of  $G$  if  $H$  is nonempty and  $H$  is closed under products and inverse (i.e,  $x, y \in H$  implies  $x \in H$  and  $xy \in H$ ). If  $H$  is a subgroup of  $G$  we shall write  $H \leq G$ .

**Proposition 1.** (The Subgroup Criterion) A subset  $H$  of a group  $G$  is a subgroup if and only if

1.  $H \neq \emptyset$ , and
2. for all  $x, y \in H$ ,  $xy^{-1} \in H$

## 2.2 Centralizers and Normalizers, Stabilizers and Kernels

Let  $G$  be a group and  $A$  a nonempty subset of  $G$ .

**Definition.** The *centralizer* of  $A$  in  $G$  is  $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$ . Note that this is the set of elements of  $G$  which commute with every element of  $A$ . Note that  $C_G(A) \leq G$ .

**Definition.** The *center* of  $G$  is the set  $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$ . Note that,  $Z(G) = C_G(G)$ , thus  $Z(G) \leq G$ .

**Definition.** Define  $gAg^{-1} = \{gag^{-1} \mid a \in A\}$ . The *normalizer* of  $A$  in  $G$  is the set  $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ . Note that,  $C_G(A) \leq N_G(A) \leq G$ .

## 2.3 Cyclic Groups and Cyclic Subgroups

**Definition.** A group  $H$  is *cyclic* if  $H$  can be generated by a single element, i.e, there exist some  $x \in H$  such that  $H = \{x^n \mid n \in \mathbb{Z}\}$  when using multiplicative notation and  $H = \{nx \mid n \in \mathbb{Z}\}$  when using additive notation. In either case we write  $H = \langle x \rangle$ .

**Proposition 2.** If  $H = \langle x \rangle$ , then  $|H| = |x|$ . Moreover,

1. if  $|H| = n < \infty$ , then  $x^n = 1$  and  $1, x, x^2, \dots, x^{n-1}$  are all distinct elements of  $H$ , and
2. if  $|H| = \infty$ , then  $x^n \neq 1$  for all  $n \neq 0$  and  $x^a \neq x^b$  for all  $a \neq b \in \mathbb{Z}$ .

**Proposition 3.** Let  $G$  be an arbitrary group,  $x \in G$  and let  $m, n \in \mathbb{Z}$ . If  $x^n = 1$  and  $x^m = 1$  then  $x^d = 1$  where  $d = (m, n)$ . In particular, if  $x^m = 1$  for some  $m \in \mathbb{Z}$  then  $|x|$  divides  $m$ .

**Theorem 4.** Any two cyclic groups of the same order are isomorphic. Moreover,

1. if  $n \in \mathbb{Z}^+$  and  $\langle x \rangle$  and  $\langle y \rangle$  are both cyclic groups of order  $n$ , then the map

$$\begin{aligned} \phi: \langle x \rangle &\rightarrow \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

is well defined and is an isomorphism

2. if  $\langle x \rangle$  is an infinite cyclic group, the map

$$\begin{aligned} \phi: \mathbb{Z} &\rightarrow \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism

**Proposition 5.** Let  $G$  be a group, let  $x \in G$  and let  $a \in \mathbb{Z} - \{0\}$ .

1. If  $|x| = \infty$ , then  $|x^a| = \infty$ .
2. If  $|x| = n < \infty$ , then  $|x^a| = \frac{n}{(n, a)}$ .
3. In particular, if  $|x| = n < \infty$  and  $a$  is a positive integer dividing  $n$ , then  $|x^a| = \frac{n}{a}$ .

**Proposition 6.** Let  $H = \langle x \rangle$ .

1. Assume  $|x| = \infty$ . Then  $H = \langle x^a \rangle$  if and only if  $a = \pm 1$ .
2. Assume  $|x| = n < \infty$ . Then  $H = \langle x^a \rangle$  if and only if  $(a, n) = 1$ . In particular, the number of generators of  $H$  is  $\phi(n)$  (where  $\phi$  is Euler's  $\phi$ -function)

**Theorem 7.** Let  $H = \langle x \rangle$  be a cyclic group.

1. Every subgroup of  $H$  is cyclic. More precisely, if  $K \leq H$ , then either  $K = \{1\}$  or  $K = \langle x^d \rangle$ , where  $d$  is the smallest positive integer such that  $x^d \in K$ .
2. If  $|H| = \infty$ , then for any distinct nonnegative integers  $a$  and  $b$ ,  $\langle x^a \rangle \neq \langle x^b \rangle$ . Furthermore, for every integer  $m$ ,  $\langle x^m \rangle = \langle x^{|m|} \rangle$ , where  $|m|$  denotes the absolute value of  $m$ , so that the nontrivial subgroups of  $H$  correspond bijectively with the integers  $1, 2, 3, \dots$
3. If  $|H| = n < \infty$ , then for each positive integer  $a$  dividing  $n$  there is a unique subgroup of  $H$  of order  $a$ . This subgroup is the cyclic group  $\langle x^d \rangle$ , where  $d = \frac{n}{a}$ . Furthermore, for every integer  $m$ ,  $\langle x^m \rangle = \langle x^{(n,m)} \rangle$ , so that the subgroups of  $H$  correspond bijectively with the positive divisors of  $n$ .

## 2.4 Subgroups Generated by Subsets of a Group

**Proposition 8.** If  $\mathcal{A}$  is any nonempty collection of subgroups of  $G$ , then the intersection of all members of  $\mathcal{A}$  is also a subgroup of  $G$ .

**Definition.** If  $A$  is any subset of the group  $G$  define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

This is called the *subgroup of  $G$  generated by  $A$* .

**Note.**  $\langle A \rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \mid n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i\}$ .

## 3 Quotient Groups and Homomorphisms

### 3.1 Definitions and Examples

**Definition.** If  $\phi$  is a homomorphism  $\phi: G \rightarrow H$ , the *kernel* of  $\phi$  is the set

$$\{g \in G \mid \phi(g) = 1\}$$

and will be denoted by  $\ker \phi$  (here 1 is the identity of  $H$ ).

**Proposition 1.** Let  $G$  and  $H$  be groups and let  $\phi: G \rightarrow H$  be a homomorphism.

1.  $\phi(1_G) = 1_H$ , where  $1_G$  and  $1_H$  are the identities of  $G$  and  $H$ , respectively.
2.  $\phi(g^{-1}) = \phi(g)^{-1}$  for all  $g \in G$ .
3.  $\phi(g^n) = \phi(g)^n$  for all  $n \in \mathbb{Z}$ .

4.  $\ker\phi$  is a subgroup of  $G$ .

5.  $\text{im}\phi$ , the image of  $G$  under  $\phi$ , is a subgroup of  $H$ .

**Definition.** Let  $\phi: G \rightarrow H$  be a homomorphism with kernel  $K$ . The *quotient group* or *factor group*,  $G/K$  (read  $G$  modulo  $K$  or simply  $G \bmod K$ ), is the group whose elements are the fibers of  $\phi$  with the following group operation: If  $X$  is the fiber above  $a$  and  $Y$  is the fiber above  $b$  then the product  $XY$  in  $G/K$  is defined to be the fiber above the product  $ab$  in  $G$ .

**Proposition 2.** Let  $\phi: G \rightarrow H$  be a homomorphism with kernel  $K$ . Let  $X \in G/K$  be the fiber above  $a$ , i.e.,  $X = \phi^{-1}(a)$ . Then

1. For any  $u \in X$ ,  $X = \{uk \mid k \in K\}$
2. For any  $u \in X$ ,  $X = \{ku \mid k \in K\}$

**Definition.** For any  $N \leq G$  and any  $g \in G$  let

$$gN = \{gn \mid n \in N\} \text{ and } Ng = \{ng \mid n \in N\}$$

called respectively a *left coset* and a *right coset* of  $N$  in  $G$ . Any element of a coset is called a *representative* for the coset.

**Theorem 3.** Let  $G$  be a group and let  $K$  be the kernel of some homomorphism from  $G$  to another group. Then the set of whose elements are left coset of  $K$  in  $G$  with operation defined by

$$uK \circ vK = (uv)K$$

forms a group,  $G/K$ . This operation is well defined and does not depend on the choice of representatives.

**Proposition 4.** Let  $N$  be any subgroup of the group  $G$ . The set of left cosets of  $N$  in  $G$  form a partition of  $G$ . Furthermore, for all  $u, v \in G$ ,  $uN = vN$  if and only if  $v^{-1}u \in N$  and in particular,  $uN = vN$  if and only if  $u$  and  $v$  are representatives of the same coset.

**Proposition 5.** Let  $G$  be a group and let  $N$  be a subgroup of  $G$ .

1. The operation on the set of left cosets of  $N$  in  $G$  described by

$$uN \cdot vN = (uv)N$$

is well defined if and only if  $gng^{-1} \in N$  for all  $g \in G$  and all  $n \in N$ .

2. If the above operation is well defined, then it makes the set of left cosets of  $N$  in  $G$  into a group. In particular the identity of this group is the coset  $1N$  and the inverse of  $gN$  is the coset  $g^{-1}N$ , i.e.,  $(gN)^{-1} = g^{-1}N$ .

**Definition.** The element  $gng^{-1}$  is called the *conjugate* of  $n \in N$  by  $g$ . The set  $gNg^{-1} = \{gng^{-1} \mid n \in N\}$  is called the *conjugate* of  $N$  by  $g$ . The element  $g$  is said to *normalize*  $N$  if  $gNg^{-1} = N$ . A subgroup  $N$  of a group  $G$  is called *normal* if every element of  $G$  normalizes  $N$ , i.e., if  $gNg^{-1} = N$  for all  $g \in G$ . If  $N$  is a normal subgroup of  $G$  we shall write  $N \trianglelefteq G$ .

**Theorem 6.** Let  $N$  be a subgroup of the group  $G$ . The following are equivalent:

1.  $N \trianglelefteq G$
2.  $N_G(N) = G$  (recall  $N_G(N)$  is the normalizer in  $G$  of  $N$ )
3.  $gN = Ng$  for all  $g \in G$
4. the operation on left cosets of  $N$  in  $G$  described in Proposition 5 makes the set of left cosets into a group
5.  $gNg^{-1} \subseteq N$  for all  $g \in G$ .

**Proposition 7.** A subgroup  $N$  of the group  $G$  is normal if and only if it is the kernel of some homomorphism.

**Definition.** Let  $N \trianglelefteq G$ . The homomorphism  $\pi: G \rightarrow G/N$  defined by  $\pi(g) = gN$  is called the *natural projection (homomorphism)* of  $G$  onto  $G/N$ . If  $\overline{H} \leq G/N$ , then *complete preimage* of  $\overline{H}$  in  $G$  is the preimage of  $\overline{H}$  under the natural projection homomorphism.

### 3.2 More on Cosets and Lagrange's Theorem

**Theorem 8.** (*Lagrange's Theorem*) If  $G$  is a finite group and  $H$  is a subgroup of  $G$ , then the order of  $H$  divides the order of  $G$  and the number of left cosets of  $H$  in  $G$  equals  $\frac{|G|}{|H|}$ .

**Definition.** If  $G$  is a group and  $H \leq G$ , the number of left cosets of  $H$  in  $G$  is called the *index* of  $H$  in  $G$  and is denoted by  $|G : H|$ .

**Corollary 9.** If  $G$  is a finite group and  $x \in G$ , then the order of  $x$  divides the order of  $G$ . In particular,  $x^{|G|} = 1$  for all  $x$  in  $G$ .

**Corollary 10.** If  $G$  is a group of prime order  $p$ , then  $G$  is cyclic, hence  $G \cong Z_p$  (note that this text uses  $Z_n$  to denote the cyclic group of order  $n$  written in multiplicative notation and that given any  $n \in \mathbb{Z}$ ,  $Z_n \cong \mathbb{Z}/n\mathbb{Z}$ ).

**Note.** For finite abelian groups the full converse of Lagrange's theorem holds, that is the group has a subgroup of order  $n$  for each  $n$  that divides the order of the group.

**Theorem 11.** (Cauchy's Theorem) If  $G$  is a finite group and  $p$  is a prime dividing  $|G|$ , then  $G$  has an element of order  $p$ .

**Theorem 12.** (Sylow) If  $G$  is a finite group of order  $p^\alpha m$ , where  $p$  is a prime not dividing  $m$ , then  $G$  has a subgroup of order  $p^\alpha$ .

**Definition.** Let  $H$  and  $K$  be subgroups of a group and define

$$HK = \{hk \mid h \in H, k \in K\}.$$

**Proposition 13.** If  $H$  and  $K$  are finite subgroups of a group then

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

**Proposition 14.** If  $H$  and  $K$  are subgroups of a group,  $HK$  is a subgroup if and only if  $HK = KH$ .

**Note.**  $HK = KH$  does not imply that the elements of  $H$  commute with the elements of  $K$

**Corollary 15.** If  $H$  and  $K$  are subgroups of  $G$  and  $H \leq N_G(K)$ , then  $Hk$  is a subgroup of  $G$ . In particular, if  $K \trianglelefteq G$ , Then  $HK \leq G$  for any  $H \leq G$  (Since if  $K \trianglelefteq G$ ,  $N_G(k) = G$ ).

**Definition.** If  $A$  is any subset of  $N_G(K)$  (or  $C_G(K)$ ), we shall say  $A$  *normalizes*  $K$  (*centralizes*  $K$ , respectively).

### 3.3 The Isomorphism Thoerems

**Theorem 16.** (The First Isomorphism Theorem) If  $\phi: G \rightarrow H$  is a homomorphism, then  $\ker\phi \trianglelefteq G$  and  $G/\ker\phi \cong \phi(G)$ .

**Corollary 17.** Let  $\phi: G \rightarrow H$  be a homomorphism.

1.  $\phi$  is injective if and only if  $\ker\phi = 1$ .
2.  $|G : \ker\phi| = |\phi(G)|$ .

**Theorem 18.** (The Second or Diamond Isomorphism Theorem) Let  $G$  be a group, let  $A$  and  $B$  be subgroups of  $G$  and assume  $A \leq N_G(B)$ . Then  $AB$  is a subgroup of  $G$ ,  $B \trianglelefteq AB$ ,  $A \cap B \trianglelefteq A$ , and  $AB/B \cong A/A \cap B$ .

**Theorem 19.** (The Third Isomorphism Thoerem) Let  $G$  be a group and let  $H$  and  $K$  be normal subgroups of  $G$  with  $H \leq K$ . Then  $K/H \trianglelefteq G/H$  and

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

If we denote the quotient by  $H$  with a bar, this can be written

$$\overline{G}/\overline{K} \cong G/K.$$

**Theorem 20.** (The Fourth or Lattice Isomorphism Theorem) Let  $G$  be a group and let  $N$  be a normal subgroup of  $G$ . Then there is a bijection from the set of subgroups  $A$  of  $G$  which contains  $N$  onto the set of subgroups  $\overline{A} = A/N$  of  $G/N$ . In particular, every subgroup of  $\overline{G}$  is of the form  $A/N$  for some subgroup  $A$  of  $G$  containing  $N$  (namely, its preimage in  $G$  under the natural projection homomorphism from  $G$  to  $G/N$ ). This bijection has the following properties: for all  $A, B \leq G$  with  $N \leq A$  and  $N \leq B$ ,

1.  $A \leq B$  if and only if  $\overline{A} \leq \overline{B}$ ,
2. if  $A \leq B$ , then  $|B : A| = |\overline{B} : \overline{A}|$ ,
3.  $\langle \overline{A}, \overline{B} \rangle = \overline{\langle A, B \rangle}$ ,
4.  $\overline{A \cap B} = \overline{A} \cap \overline{B}$ , and
5.  $A \trianglelefteq G$  if and only if  $\overline{A} \trianglelefteq \overline{G}$ .



### 3.4 Composition Series and the Hölder Program

**Proposition 21.** If  $G$  is a finite abelian group and  $p$  is a prime dividing  $|G|$ , then  $G$  contains an element of order  $p$ .

**Definition.** A group  $G$  is called *simple* if  $|G| > 1$  and the only normal subgroups of  $G$  are 1 and  $G$ .

**Definition.** In a group  $G$  a sequence of subgroups

$$1 = N_0 \leq N_1 \leq N_2 \leq \dots \leq N_{k-1} \leq N_k = G$$

is called a composition series if  $N_i \trianglelefteq N_{i+1}$  and  $N_{i+1}/N_i$  is a simple group,  $0 \leq i \leq k-1$ . If the above sequence is a composition series, the quotient groups  $N_{i+1}/N_i$  are called *composition factors* of  $G$ .

**Theorem 22.** (Jordan-Hölder) Let  $G$  be a finite group with  $G \neq 1$ . Then

1.  $G$  has a composition series and
2. The composition factors in a composition series are unique, namely, if  $1 = N_0 \leq N_1 \leq \dots \leq N_r = G$  and  $1 = M_0 \leq M_1 \leq \dots \leq M_s = G$  are two composition series for  $G$ , then  $r = s$  and there is some permutation,  $\pi$ , of  $\{1, 2, \dots, r\}$  such that

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}, \quad 1 \leq i \leq r.$$

**Theorem.** There is a list consisting of 18 (infinite) families of simple groups and 26 simple groups not belonging to these families (the *sporadic* simple groups) such that every finite simple group is isomorphic to one of the groups in this list.

**Theorem.** (Feit-Thompson) If  $G$  is a simple group of odd order, then  $G \cong Z_p$  for some prime  $p$ .

**Definition.** A group  $G$  is *solvable* if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_s = G$$

such that  $G_{i+1}/G_i$  is abelian for  $i = 0, 1, \dots, s-1$ .

**Theorem.** The finite group  $G$  is solvable if and only if for every divisor  $n$  of  $|G|$  such that  $(n, \frac{|G|}{n}) = 1$ ,  $G$  has a subgroup of order  $n$ .

**Note.** If  $N$  and  $G/N$  are solvable, then so is  $G$ .

### 3.5 Transpositions and the Alternating Group

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

**Note.** Every element of  $S_n$  may be written as a product of transpositions.

**Definition.** Let  $x_1, \dots, x_n$  be independent variables and let  $\Delta$  be the polynomial

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

and for  $\sigma \in S_n$  let  $\sigma$  act on  $\Delta$  by

$$\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

One can show that for all  $\sigma \in S_n$  that  $\sigma(\Delta) = \pm\Delta$ . Now define,

$$\epsilon(\sigma) = \begin{cases} +1 & \text{if } \sigma(\Delta) = \Delta \\ -1 & \text{if } \sigma(\Delta) = -\Delta. \end{cases}$$

Now,

1.  $\epsilon(\sigma)$  is called the sign of  $\sigma$  and
2.  $\sigma$  is called an *even permutation* if  $\epsilon(\sigma) = 1$  and an *odd permutation* if  $\epsilon(\sigma) = -1$ .

**Proposition 23.** The map  $\epsilon: S_n \rightarrow \{\pm 1\}$  is a homomorphism (where  $\{\pm 1\}$  is a multiplicative version of the cyclic group of order 2).

**Proposition 24.** Transpositions are all odd permutations and  $\epsilon$  is a surjective homomorphism.

**Definition.** The *alternating group of degree  $n$* , denoted  $A_n$ , is the kernel of the homomorphism  $\epsilon$  (i.e., the set of even permutations).

**Note.**

1.  $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}(n!)$ .
2. Due to  $\epsilon$  being a homomorphism we get the rules

$$\begin{aligned} (\text{even})(\text{even}) &= (\text{odd})(\text{odd}) = \text{even} \\ (\text{even})(\text{odd}) &= (\text{odd})(\text{even}) = \text{odd}. \end{aligned}$$

3. An  $m$ -cycle is an odd permutation if and only if  $m$  is even

**Proposition 25.** The permutation  $\sigma$  is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

**Note.**  $A_n$  is a non-abelian simple group for all  $n \geq 5$ .

## 4 Group Actions

### 4.1 Group Actions and Permutation Representations

**Definition.** Let  $G$  be a group acting on a set  $A$

1. The *kernel* of the action is the set of elements of  $G$  that act trivially on every element of  $A$ :  $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$ .
2. For each  $a \in A$  the *stabilizer* of  $a$  in  $G$  is the set of elements of  $G$  that fix the element  $a$ :  $\{g \in G \mid g \cdot a = a\}$  and is denoted by  $G_a$ .
3. An action is *faithful* if its kernel is the identity.

**Note.** The kernel of an action is precisely the same as the kernel of the associated permutation representation as defined in the note in section 1.7 and is rephrased below.

**Proposition 1.** For any group  $G$  and any nonempty set  $A$  there is a bijection between the actions of  $G$  on  $A$  and the homomorphisms of  $G$  into  $S_A$ .

**Definition.** If  $G$  is a group a *permutation representation* of  $G$  into the symmetric group  $S_A$  for some nonempty set  $A$ . We shall say a given action of  $G$  on  $A$  *affords* or *induces* the associated representation of  $G$ .

**Proposition 2.** Let  $G$  be a group acting on the nonempty set  $A$ . the relation on  $A$  defined by

$$a \sim b \text{ if and only if } a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each  $a \in A$ , the number of elements in the equivalence class containing  $a$  is  $|G : G_a|$ , the index of the stabilizer of  $a$ .

**Definition.** Let  $G$  be a group acting on the set  $A$ .

1. The equivalence class  $\{g \cdot a \mid g \in G\}$  is called the *orbit* of  $G$  containing  $a$ .
2. The action of  $G$  on  $A$  is called *transitive* if there is only one orbit, i.e., given any two elements  $a, b \in A$  there is some  $g \in G$  such that  $a = g \cdot b$ .

**Note.**

1. Every element of  $S_n$  has a unique cycle decomposition
2. Subgroups of symmetric groups are called *permutation groups*.
3. The orbits of a permutation group will refer to its orbits on  $\{1, 2, \dots, n\}$
4. The orbits of an element  $\sigma \in S_n$  will refer to the orbits of the group  $\langle \sigma \rangle$ .

## 4.2 Group Acting on Themselves by Left Multiplication - Cayley's Theorem

**Note.** In this section  $G$  is any group and we first consider  $G$  acting on itself (i.e.,  $A = G$ ) by left multiplication:

$$g \cdot a = ga \quad \text{for all } g \in G, a \in G$$

When  $G$  is a finite group of order  $n$  it is convenient to label the elements of  $G$  with the integers  $1, 2, \dots, n$  in order to describe the permutation representation afforded by this action. In this way the elements of  $G$  are listed as  $g_1, g_2, \dots, g_n$  and for each  $g \in G$  the permutation  $\sigma_g$  may be described as a permutation of the indices  $1, 2, \dots, n$  as follows:

$$\sigma_g(i) = j \quad \text{if and only if} \quad gg_i = g_j.$$

**Theorem 3.** Let  $G$  be a group, let  $H$  be a subgroup and let  $G$  act by left multiplication on the set  $A$  of left cosets of  $H$  in  $G$ . Let  $\pi_H$  be the associated permutation representation afforded by this action. Then

1.  $G$  acts transitively on  $A$
2. the stabilizer of  $G$  of the point  $1H \in A$  is the subgroup  $H$
3. the kernel of the action (i.e., the kernel of  $\pi_H$ ) is  $\bigcap_{x \in G} xHx^{-1}$ , and  $\ker \pi_H$  is the largest normal subgroup of  $G$  contained in  $H$ .

**Corollary 4.** (Cayley's Theorem) Every group is isomorphic to a subgroup of symmetric group. If  $G$  is a group of order  $n$ , then  $G$  is isomorphic to a subgroup of  $S_n$ .

**Corollary 5.** If  $G$  is a finite group of order  $n$  and  $p$  is the smallest prime dividing  $|G|$ , then any subgroup of index  $p$  is normal (Note that a group of order  $n$  need not have a subgroup of order  $p$ ).

### 4.3 Groups Acting on Themselves by Conjugation - The Class Equation