

# Dummit and Foote Abridged

## Contents

<b>I</b>	<b>Group Theory</b>	<b>2</b>
<b>0</b>	<b>Preliminaries</b>	<b>2</b>
0.1	Basics . . . . .	2
<b>1</b>	<b>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</b>	<b>Subgroups</b>	<b>4</b>
2.1	Definition and Examples . . . . .	4
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 . . . . .	6
<b>3</b>	<b>Quotient Groups and Homomorphisms</b>	<b>6</b>
3.1	Definitions and Examples . . . . .	6
3.2	More on Cosets and Lagrange's Theorem . . . . .	8
3.3	The Isomorphism Theorems . . . . .	8
3.4	Composition Series and the Hölder Program . . . . .	9
3.5	Transpositions and the Alternating Group . . . . .	10
<b>4</b>	<b>Group Actions</b>	<b>11</b>
4.1	Group Actions and Permutation Representations . . . . .	11
4.2	Group Acting on Themselves by Left Multiplication - Cayley's Theorem . . . . .	12
4.3	Groups Acting on Themselves by Conjugation - The Class Equation . . . . .	12
4.4	Automorphisms . . . . .	13
4.5	Sylow's Theorem . . . . .	15
4.6	The Simplicity of $A_n$ . . . . .	15
<b>5</b>	<b>Direct and Semidirect Products and Abelian Groups</b>	<b>16</b>
5.1	Direct Products . . . . .	16
5.2	The Fundamental Theorem of Finitely Generated Abelian Groups . . . . .	17
5.3	Table of Groups of Small Order . . . . .	19
5.4	Recognizing Direct Products . . . . .	19

5.5	Semidirect Products . . . . .	20
<b>6</b>	<b>Further Topics in Group Theory</b>	<b>21</b>
6.1	$p$ -Groups, Nilpotent Groups, and Solvable Groups . . . . .	21
6.2	Applications in Groups of Medium Order . . . . .	24
6.3	A word on Free Groups . . . . .	24
<b>II</b>	<b>Ring Theory</b>	<b>25</b>
<b>7</b>	<b>Introduction to Rings</b>	<b>25</b>
7.1	Basic Definitions and Examples . . . . .	25

## Part I

# Group Theory

## 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 the  $f: A \rightarrow B$  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  $\varphi: G \rightarrow H$  such that  $\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$ , for all  $x, y \in G$  is called a *homomorphism*. Moreover, if  $\varphi$  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  $\varphi: G \rightarrow H$  is an isomorphism then

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

## 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  $\varphi: G \rightarrow S_A$  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

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

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

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

is well defined and is an isomorphism

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

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

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  $\varphi(n)$  (where  $\varphi$  is Euler's  $\varphi$ -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  $\varphi$  is a homomorphism  $\varphi: G \rightarrow H$ , the *kernel* of  $\varphi$  is the set

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

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

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

1.  $\varphi(1_G) = 1_H$ , where  $1_G$  and  $1_H$  are the identities of  $G$  and  $H$ , respectively.
2.  $\varphi(g^{-1}) = \varphi(g)^{-1}$  for all  $g \in G$ .
3.  $\varphi(g^n) = \varphi(g)^n$  for all  $n \in \mathbb{Z}$ .
4.  $\ker \varphi$  is a subgroup of  $G$ .
5.  $\text{im } \varphi$ , the image of  $G$  under  $\varphi$ , is a subgroup of  $H$ .

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

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

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

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

**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 Theorem) 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

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

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

**Note.** In this section we consider a group  $G$  acting on itself by *conjugation*

$$g \cdot a = gag^{-1} \quad \text{for all } g \in G, a \in G$$

**Definition.** Two elements  $a$  and  $a$  of  $G$  are said to be *conjugate* if  $G$  if there is some  $g \in G$  such that  $b = gag^{-1}$  (i.e., if and only if they are in some orbit of  $G$  acting on itself by conjugation). The orbits of  $G$  acting on itself by conjugation are called *conjugacy classes* of  $G$ .

**Definition.** Two subsets  $S$  and  $T$  of  $G$  are said to be *conjugate in  $G$*  if there is some  $g \in G$  such that  $T = gSg^{-1}$  (i.e., if and only if they are in the same orbit of  $G$  acting on its subsets by conjugation).

**Proposition 6.** The number of conjugates of a subset  $S$  in a group  $G$  is the index of the normalizer of  $S$ ,  $|G : N_G(S)|$ . In particular, the number of conjugates of an element  $s$  of  $G$  is the index of the centralizer of  $s$ ,  $|G : C_G(s)|$ .

**Theorem 7.** (The Class Equation) Let  $G$  be a finite group and let  $g_1, g_2, \dots, g_r$  be representatives of the distinct conjugacy classes of  $G$  not contained in the center  $Z(G)$  of  $G$ . Then

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|.$$

**Theorem 8.** If  $p$  is a prime and  $P$  is a group of prime order  $p^\alpha$  for some  $\alpha \geq 1$ , then  $P$  has a nontrivial center:  $Z(P) \neq 1$ .

**Proposition 9.** Let  $\sigma, \tau$  be elements of the symmetric group  $S_n$  and suppose  $\sigma$  has cycle decomposition

$$(a_1 a_2 \dots a_{k_1})(b_1 b_2 \dots b_{k_2}) \dots$$

Then  $\tau\sigma\tau^{-1}$  has cycle decomposition

$$(\tau(a_1)\tau(a_2) \dots \tau(a_{k_1}))(\tau(b_1)\tau(b_2) \dots \tau(b_{k_2})) \dots,$$

that is  $\tau\sigma\tau^{-1}$  is obtained from  $\sigma$  by replacing each  $i$  in the cycle decomposition for  $\sigma$  by the entry  $\tau(i)$ .

**Definition.**

1. If  $\sigma \in S_n$  is the product of disjoint cycles of length  $n_1, n_2, \dots, n_r$  with  $n_1 \leq n_2 \leq \dots \leq n_r$  (including its 1-cycles) then the integers  $n_1, n_2, \dots, n_r$  are called the *cycle type* of  $\sigma$ .
2. If  $n \in \mathbb{Z}^+$ , a *partition* of  $n$  is any nondecreasing sequence of positive integers whose sum is  $n$ .

**Proposition 10.** Two elements of  $S_n$  are conjugate in  $S_n$  if and only if they have the same cycle type. The number of conjugacy classes of  $S_n$  equals the number of partitions of  $n$ .

**Theorem 11.**  $A_5$  is a simple group.

## 4.4 Automorphisms

**Definition.** Let  $G$  be a group. An isomorphism from  $G$  onto itself is called an *automorphism* of  $G$ . The set of all automorphisms of  $G$  is denoted  $\text{Aut}(G)$ .

**Note.**  $\text{Aut}(G)$  is a group under composition.

**Proposition 12.** Let  $H$  be a normal subgroup of the group  $G$ . Then  $G$  acts by conjugation on  $H$  as automorphisms of  $H$ . More specifically, the action of  $G$  on  $H$  by conjugation is defined for each  $g \in G$  by

$$h \mapsto ghg^{-1} \quad \text{for each } h \in H.$$

For each  $g \in G$ , conjugation by  $g$  is an automorphism of  $H$ . The permutation representation afforded by this action is a homomorphism of  $G$  into  $\text{Aut}(H)$  with kernel  $C_G(H)$ . In particular,  $G/C_G(H)$  is isomorphic to a subgroup of  $\text{Aut}(H)$ .

**Corollary 13.** If  $K$  is any subgroup of the group  $G$  and  $g \in G$ , then  $K \cong gKg^{-1}$ . Conjugate elements and conjugate subgroups have the same order.

**Corollary 14.** For any subgroup  $H$  of a group  $G$ , the quotient group  $N_G(H)/C_G(H)$  is isomorphic to a subgroup of  $\text{Aut}(H)$ . In particular,  $G/Z(G)$  is isomorphic to a subgroup of  $\text{Aut}(G)$ .

**Definition.** Let  $G$  be a group and let  $g \in G$ . Conjugation by  $g$  is called an *inner automorphism* of  $G$  and the subgroup of  $\text{Aut}(G)$  consisting of all inner automorphisms is denoted  $\text{Inn}(G)$ .

**Definition.** A subgroup  $H$  of a group  $G$  is called *characteristic* in  $G$ , denoted  $H \text{ char } G$ , if every automorphism of  $G$  maps  $H$  to itself, i.e.,  $\sigma(H) = H$  for all  $\sigma \in \text{Aut}(G)$ .

**Note.**

1. Characteristic subgroups are normal,
2. if  $H$  is the unique subgroup of a given order, then  $H$  is characteristic in  $G$ , and
3. if  $K \text{ char } H$  and  $H \trianglelefteq G$ , then  $K \trianglelefteq G$ .

**Proposition 15.** The automorphism group of the cyclic group of order  $n$  is isomorphic to  $(\mathbb{Z}/n\mathbb{Z})^\times$ , an abelian group of order  $\varphi(n)$  (where  $\varphi$  is Euler's function).

**Proposition 16.**

1. If  $p$  is an odd prime and  $n \in \mathbb{Z}^+$ , then the automorphism group of the cyclic group of order  $p$  is cyclic of order  $p - 1$ . More generally, the automorphism group of the cyclic group of order  $p^n$  is cyclic of order  $p^{n-1}(p - 1)$ .
2. For all  $n \geq 3$  the automorphism group of the cyclic group of order  $2^n$  is isomorphic to  $Z_2 \times Z_{2^{n-2}}$ , and in particular is not cyclic but has a cyclic subgroup of index 2.
3. Let  $p$  be a prime and let  $V$  be an abelian group (written additively) with the property that  $pv = 0$  for all  $v \in V$ . If  $|V| = p^n$ , then  $V$  is an  $n$ -dimensional vector space over the field  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . The automorphisms of  $V$  are precisely the nonsingular linear transformations from  $V$  to itself, that is

$$\text{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p).$$

In particular, the order of  $\text{Aut}(V)$  is given in section 1.4.

4. For all  $n \neq 6$  we have  $\text{Aut}(S_n) = \text{Inn}(S_n) \cong S_n$ . For  $n = 6$  we have  $|\text{Aut}(S_6) : \text{Inn}(S_6)| = 2$ .
5.  $\text{Aut}(D_8) \cong D_8$  and  $\text{Aut}(Q_8) \cong S_4$ .

## 4.5 Sylow's Theorem

**Definition.** Let  $G$  be a group and let  $p$  be a prime.

1. A group of order  $p^\alpha$  for some  $\alpha \geq 0$  is called a  $p$ -group. Subgroups of  $G$  which are  $p$ -groups are called  $p$ -subgroups.
2. If  $G$  is a group of order  $p^\alpha m$ , where  $p \nmid m$ , then a subgroup of order  $p^\alpha$  is called a Sylow  $p$ -subgroup of  $G$ .
3. The set of Sylow  $p$ -subgroups of  $G$  will be denoted  $\text{Syl}_p(G)$  and the number of Sylow  $p$ -subgroups of  $G$  will be denoted by  $n_p(G)$  (or just  $n_p$  when  $G$  is clear from context).

**Theorem 17.** (Sylow's Theorem) Let  $G$  be a group of order  $p^\alpha m$ , where  $p$  is a prime not dividing  $m$ . ;

1. Sylow  $p$ -subgroups of  $G$  exist, i.e.,  $\text{Syl}_p(G) \neq \emptyset$ .
2. If  $P$  is a Sylow  $p$ -subgroup of  $G$  and  $Q$  is any  $p$ -subgroup of  $G$ , then there exists  $g \in G$  such that  $Q \leq gPg^{-1}$ , i.e.,  $Q$  is contained in some conjugate of  $P$ . In particular, any two Sylow  $p$ -subgroups of  $G$  are conjugate in  $G$ .
3. The number of Sylow  $p$ -subgroups of  $G$  is of the form  $1 + kp$ , i.e.,

$$n_p \equiv 1 \pmod{p}.$$

Further,  $n_p$  is the index in  $G$  of the normalizer of  $N_G(P)$  for any Sylow  $p$ -subgroup  $P$ , hence  $n_p$  divides  $m$ .

**Lemma 18.** Let  $P \in \text{Syl}_p(G)$ . If  $Q$  is any  $p$ -subgroup of  $G$ , then  $Q \cap N_G(P) = Q \cap P$ .

**Corollary 19.** Let  $P$  be a Sylow  $p$ -subgroup of  $G$ . Then the following are equivalent:

1.  $P$  is the unique Sylow  $p$ -subgroup of  $G$ , i.e.,  $n_p = 1$
2.  $P$  is normal in  $G$
3.  $P$  is characteristic in  $G$
4. All subgroups generated by elements of  $p$ -power order are  $p$ -groups, i.e., if  $X$  is any subset of  $G$  such that  $|x|$  is a power of  $p$  for all  $x \in X$ , then  $\langle X \rangle$  is a  $p$ -group.

**Proposition 20.** If  $|G| = 60$  and  $G$  has more than one Sylow 5-subgroups, then  $G$  is simple.

**Corollary 21.**  $A_5$  is simple

**Proposition 22.** If  $G$  is a simple group of order 60, then  $G \cong A_5$ .

## 4.6 The Simplicity of $A_n$

**Theorem 23.**  $A_n$  is simple for all  $n \geq 5$ .

# 5 Direct and Semidirect Products and Abelian Groups

## 5.1 Direct Products

**Definition.**

1. The *direct product*  $G_1 \times G_2 \times \cdots \times G_n$  of the groups  $G_1, G_2, \dots, G_n$  with operations  $\star_1, \star_2, \dots, \star_n$ , respectively, is the set of  $n$ -tuples  $(g_1, g_2, \dots, g_n)$  where  $g_i \in G_i$  with the operation defined componentwise:

$$(g_1, g_2, \dots, g_n) \star (h_1, h_2, \dots, h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots, g_n \star_n h_n).$$

2. Similarly, the *direct product*  $G_1 \times G_2 \times \cdots$  of the groups  $G_1, G_2, \dots$  with operations  $\star_1, \star_2, \dots$ , respectively, is the set of sequences  $(g_1, g_2, \dots)$  where  $g_i \in G_i$  with the operation defined componentwise:

$$(g_1, g_2, \dots) \star (h_1, h_2, \dots) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots).$$

**Proposition 1.** If  $G_1, \dots, G_n$  are groups, their direct product is a group of order  $|G_1||G_2| \cdots |G_n|$  (if any  $G_i$  is infinite, so is the direct product).

**Proposition 2.** Let  $G_1, G_2, \dots, G_n$  be group and let  $G = G_1 \times G_2 \times \cdots \times G_n$  be their direct product.

1. For each fixed  $i$  the set of elements of  $G$  which have the identity of  $G_j$  in the  $j^{\text{th}}$  position for all  $j \neq i$  and arbitrary elements of  $G_i$  in position  $i$  is a subgroup of  $G$  isomorphic  $G_i$ :

$$G_i \cong \{(1, 1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\},$$

(here  $g_i$  appears in the  $i^{\text{th}}$  position). If we identify  $G_i$  with this subgroup, then  $G_i \trianglelefteq G$  and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

2. For each fixed  $i$  define  $\pi_i: G \rightarrow G_i$  by

$$\pi_i((g_1, g_2, \dots, g_n)) = g_i.$$

Then  $\pi_i$  is a surjective homomorphism with

$$\begin{aligned} \ker \pi_i &= \{(g_1, g_2, \dots, g_{i-1}, 1, g_{i+1}) \mid g_j \in G_j \text{ for all } j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \end{aligned}$$

(here 1 appears in position  $i$ ).

3. Under the identifications in part 1, if  $x \in G_i$  and  $y \in G_j$  for some  $i \neq j$ , then  $xy = yx$ .



## 5.2 The Fundamental Theorem of Finitely Generated Abelian Groups

**Definition.**

1. A group  $G$  is *finitely generated* if there is some finite subset  $A$  of  $G$  such that  $G = \langle A \rangle$ .
2. For each  $r \in \mathbb{Z}$  with  $r \geq 0$  let  $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$  be the direct product of  $r$  copies of the group  $\mathbb{Z}$ , where  $\mathbb{Z}^0 = 1$ . The group  $\mathbb{Z}^r$  is called the *free abelian group of order  $r$* .

**Theorem 3.** (The Fundamental Theorem of Finitely Generated Abelian Groups) Let  $G$  be a finitely generated abelian group. Then

1.

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s},$$

for some  $r, n_1, n_2, \dots, n_s$  satisfying the following conditions:

- (a)  $r \geq 0$  and  $n_j \geq 2$  for all  $j$ , and
  - (b)  $n_{i+1} \mid n_i$  for all  $1 \leq i \leq s-1$
2. the expression in 1. is unique: if  $G \cong \mathbb{Z}^t \times Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_u}$ , where  $t$  and  $m_1, m_2, \dots, m_u$  satisfy (a) and (b), then  $t = r$  and  $m_i = n_i$  for all  $i$ .

**Definition.** The integer  $r$  in Theorem 3 is called the *free rank* or *Betti number* of  $G$  and the integers  $n_1, n_2, \dots, n_s$  are called the *invariant factors* of  $G$ . The description of  $G$  in Theorem 3(1) is called the *invariant factor decomposition* of  $G$ .

**Note.** There is a bijection between the set of isomorphism classes of finite abelian groups of order  $n$  and the set of integer sequences  $n_1, n_2, \dots, n_s$  such that

1.  $n_j \geq 2$  for all  $j \in \{1, 2, \dots, s\}$ ,
2.  $n_{i+1} \mid n_i, 1 \leq i \leq s-1$ , and
3.  $n_1 n_2 \cdots n_s = n$ .

Also notice that every prime divisor of  $n$  must be a divisor of  $n_1$  due to (2).

**Corollary 4.** If  $n$  is the product of distinct primes, then up to isomorphism the only abelian group of order  $n$  is the cyclic group of order  $n$ ,  $Z_n$ .

**Theorem 5.** Let  $G$  be an abelian group of order  $n > 1$  and let the unique factorization of  $n$  into distinct prime powers be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

1.  $G \cong A_1 \times A_2 \times \cdots \times A_k$ , where  $|A_i| = p_i^{\alpha_i}$

2. for each  $A \in \{A_1, A_2, \dots, A_k\}$  with  $|A| = p^\alpha$ ,

$$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \dots \times Z_{p^{\beta_t}}$$

with  $\beta_1 \geq \beta_2 \geq \dots \geq \beta_t \geq 1$  and  $\beta_1 + \beta_2 + \dots + \beta_t = \alpha$  (where  $t$  and  $\beta_1, \beta_2, \dots, \beta_t$  depend on  $i$ )

3. the decomposition in 1. and 2. is unique, i.e., if  $G \cong B_1 \times B_2 \times \dots \times B_m$ , with  $|B_i| = p_i^{\alpha_i}$  for all  $i$ , then  $B_i \cong A_i$  and  $B_i$  and  $A_i$  have the same invariant factors.

**Definition.** The integers  $p^{\beta_j}$  described in the proceeding theorem are called the *elementary divisors* of  $G$ . The description of  $G$  in Theorem 5(1) and 5(2) is called the *elementary divisor decomposition* of  $G$ .

**Note.** For a group of order  $p^\beta$  the invariant factors will be  $p^{\beta_1}, p^{\beta_2}, \dots, p^{\beta_t}$  such that

1.  $\beta_j \geq 1$  for all  $j \in \{1, 2, \dots, t\}$ ,
2.  $\beta_i \geq \beta_{i+1}$  for all  $i$ , and
3.  $\beta_1 + \beta_2 + \dots + \beta_t = \beta$

**Proposition 6.** Let  $m, n \in \mathbb{Z}^+$ .

1.  $Z_m \times Z_n \cong Z_{mn}$  if and only if  $(m, n) = 1$ .
2. If  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  then  $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \dots \times Z_{p_k^{\alpha_k}}$ .

### 5.3 Table of Groups of Small Order

Order	No. of Isomorphism Types	Abelian Groups	Non-abelian Groups
1	1	$Z_1$	none
2	1	$Z_2$	none
3	1	$Z_3$	none
4	2	$Z_4, Z_2 \times Z_2$	none
5	1	$Z_5$	none
6	2	$Z_6$	$S_3$
7	1	$Z_7$	none
8	5	$Z_8, Z_4 \times Z_2, Z_2 \times Z_2 \times Z_2$	$D_8, Q_8$
9	2	$Z_9, Z_3 \times Z_3$	none
10	2	$Z_{10}$	$D_{10}$
11	1	$Z_{11}$	none
12	5	$Z_{12}, Z_6 \times Z_2$	$A_4, D_{12}, Z_3 \rtimes Z_4$
13	1	$Z_{13}$	none
14	2	$Z_{14}$	$D_{14}$
15	1	$Z_{15}$	none
16	14	$Z_{16}, Z_8 \times Z_2, Z_4 \times Z_4, Z_4 \times Z_2 \times Z_2, Z_2 \times Z_2 \times Z_2 \times Z_2$	not listed
17	1	$Z_{17}$	none
18	5	$Z_{18}, Z_6 \times Z_3$	$D_{18}, S_3 \times Z_3, (Z_3 \times Z_3) \rtimes Z_2$
19	1	$Z_{19}$	none
20	5	$Z_{20}, Z_{10} \times Z_2$	$D_{20}, Z_5 \rtimes Z_4, F_{20}$

**Note.** The group  $F_{20}$  of order 20 has generators and relations

$$\langle x, y \mid x^4 = y^5 = 1, xyx^{-1} = y^2 \rangle.$$

This group is called the *Frobenius group* of order 20 and can be viewed as the subgroup  $F_{20} = \langle (2354), (12345) \rangle$  of  $S_5$ .

### 5.4 Recognizing Direct Products

**Definition.** Let  $G$  be a group, let  $x, y \in G$  and let  $A, B$  be nonempty subsets of  $G$ .

1. Define  $[x, y] = x^{-1}y^{-1}xy$ , called the *commutator* of  $x$  and  $y$ .
2. Define  $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$ , the group generated by commutators of elements of  $A$  and from  $B$ .
3. Define  $G' = \langle [x, y] \mid x, y \in G \rangle$ , the subgroup of  $G$  generated by commutators of elements from  $G$ , called the *commutator subgroup* of  $G$ .

**Proposition 7.** Let  $G$  be a group, let  $x, y \in G$  and let  $H \leq G$ . Then

1.  $xy = yx[x, y]$  (in particular,  $xy = yx$  if and only if  $[x, y] = 1$ ).

2.  $H \trianglelefteq G$  if and only if  $[H, G] \leq H$ .
3.  $\sigma[x, y] = [\sigma(x), \sigma(y)]$  for any automorphism  $\sigma$  of  $G$ ,  $G' \text{ char } G$  and  $G/G'$  is abelian
4.  $G/G'$  is the largest abelian quotient of  $G$  in the sense that if  $H \trianglelefteq G$  and  $G/H$  is abelian, then  $G' \leq H$ . Conversely, if  $G' \leq H$ , then  $H \trianglelefteq G$  and  $G/H$  is abelian.
5. If  $\varphi: G \rightarrow A$  is any homomorphism of  $G$  into an abelian group  $A$ , then  $\varphi$  factors through  $G'$  i.e.,  $G' \leq \ker \varphi$  and the following diagram commutes:

$$\begin{array}{ccc}
 G & \xrightarrow{\quad} & G/G' \\
 & \searrow \varphi & \downarrow \\
 & & A
 \end{array}$$

**Proposition 8.** Let  $H$  and  $K$  be subgroups of the group  $G$ . The number of distinct ways of writing each element of the set  $HK$  in the form  $hk$ , for some  $h \in H$  and  $k \in K$  is  $|H \cap K|$ . In particular, if  $H \cap K = 1$ , then each element of  $HK$  can be written uniquely as the product  $hk$ , for some  $h \in H$  and  $k \in K$ .

**Theorem 9.** Suppose  $G$  is a group with subgroups  $H$  and  $K$  such that

1.  $H$  and  $K$  are normal in  $G$ , and
2.  $H \cap K = 1$ .

Then  $HK \cong H \times K$ .

**Note.** The above conditions are simply the necessary conditions to ensure that the map

$$\begin{aligned}
 \varphi: HK &\rightarrow H \times K \\
 hk &\mapsto (h, k)
 \end{aligned}$$

is well defined and an isomorphism.

**Definition.** If  $G$  is a group and  $H$  and  $K$  are normal subgroups of  $G$  with  $H \cap K = 1$ , we call  $HK$  the *internal direct product* of  $H$  and  $K$ . We shall (when emphasis is called for) call  $H \times K$  the *external direct product* of  $H$  and  $K$ . (The distinction here is purely notational by Theorem 9).

## 5.5 Semidirect Products

**Theorem 10.** Let  $H$  and  $K$  be groups and let  $\varphi$  be a homomorphism from  $K$  into  $\text{Aut}(H)$ . Let  $\cdot$  denote the (left) action of  $K$  on  $H$  determined by  $\varphi$ . Let  $G$  be the set of order pairs  $(h, k)$  with  $h \in H$  and  $k \in K$  and define the following multiplication on  $G$ :

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2).$$

1. This multiplication makes  $G$  into a group of order  $|G| = |H||K|$ .

2. The sets  $\{(h, 1) \mid h \in H\}$  and  $\{(1, k) \mid k \in K\}$  are subgroups of  $G$  and the maps  $h \mapsto (h, 1)$  for  $h \in H$  and  $k \mapsto (1, k)$  for  $k \in K$  are isomorphisms of these subgroups with the groups  $H$  and  $K$  respectively;

$$H \cong \{(h, 1) \mid h \in H\} \quad \text{and} \quad K \cong \{(1, k) \mid k \in K\}.$$

Identifying  $H$  and  $K$  with their isomorphic copies in  $G$  described in 2. we have

3.  $H \trianglelefteq G$
4.  $H \cap K = 1$
5. for all  $h \in H$  and  $k \in K$ ,  $khk^{-1} = k \cdot h = \varphi(k)(h)$

**Definition.** Let  $H$  and  $K$  be groups and let  $\varphi$  be a homomorphism from  $K$  into  $\text{Aut}(H)$ . The group described in Theorem 10 is called the *semidirect product* of  $H$  and  $K$  with respect to  $\varphi$  and will be denoted by  $H \rtimes_{\varphi} K$  (when there is no danger of confusion we shall simply write  $H \rtimes K$ ).

**Proposition 11.** Let  $H$  and  $K$  be groups and let  $\varphi: K \rightarrow \text{Aut}(H)$  be a homomorphism. Then the following are equivalent:

1. the identity (set) map between  $H \rtimes K$  and  $H \times K$  is a group homomorphism (hence and isomorphism)
2.  $\varphi$  is the trivial homomorphism from  $K$  into  $\text{Aut}(H)$
3.  $K \trianglelefteq H \rtimes K$ .

**Theorem 12.** Suppose  $G$  is a group with subgroups  $H$  and  $K$  such that

1.  $H \trianglelefteq G$ , and
2.  $H \cap K = 1$ .

Let  $\varphi: K \rightarrow \text{Aut}(H)$  be the homomorphism defined by mapping  $k \in K$  to the automorphism of left conjugation by  $k$  on  $H$ . Then  $HK \cong H \rtimes K$ . In particular, if  $G = HK$  with  $H$  and  $K$  satisfying 1. and 2., then  $G$  is the semidirect product of  $H$  and  $K$ .

**Definition.** Let  $H$  be a subgroup of the group  $G$ . A subgroup  $K$  of  $G$  is called a *complement* for  $H$  in  $G$  if  $G = HK$  and  $H \cap K = 1$ .

**Note.** With the above terminology, the criterion for recognizing a semidirect product is simply that there must exist a complement for some proper normal subgroup of  $G$ .

## 6 Further Topics in Group Theory

### 6.1 $p$ -Groups, Nilpotent Groups, and Solvable Groups

**Definition.** A *maximal subgroup* of a group  $G$  is a proper subgroup  $M$  of  $G$  such that there is no subgroups  $H$  of  $G$  with  $M < H < G$ .

**Theorem 1.** Let  $p$  be a prime and let  $P$  be a group of order  $p^a$ ,  $a \geq 1$ . Then

1. The center of  $P$  is nontrivial:  $Z(P) \neq 1$ .
2. If  $H$  is a nontrivial normal subgroup of  $P$  then  $H$  contains a subgroup of order  $p^b$  that is normal in  $P$  for each divisor  $p^b$  of  $|H|$ . In particular,  $P$  has a normal subgroup of order  $p^b$  for every  $b \in \{0, 1, \dots, a\}$ .
3. If  $H < P$  then  $H < N_P(H)$  (i.e., every proper subgroup of  $P$  is a proper subgroup of its normalizer in  $P$ ).
4. Every maximal subgroup of  $P$  is of index  $p$  and is normal in  $P$ .

**Definition.**

1. For any (finite or infinite) group  $G$  define the following subgroups inductively:

$$Z_0(G) = 1 \quad Z_1(G) = Z(G)$$

and  $Z_{i+1}(G)$  is the subgroup of  $G$  containing  $Z_i(G)$  such that

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

(i.e.,  $Z_{i+1}(G)$  is the complete preimage in  $G$  of the center of  $G/Z_i(G)$  under the natural projection). The chain of subgroups

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

is called the *upper central series* of  $G$ . (The use of the term “upper” indicates that  $Z_i(G) \leq Z_{i+1}(G)$ .)

2. A group  $G$  is called *nilpotent* if  $Z_c(G) = G$  for some  $c \in \mathbb{Z}$ . The smallest  $c$  is called the *nilpotence class* of  $G$ .

**Note.**

1. If  $G$  is abelian then it is nilpotent since  $G = Z(G) = Z_1(G)$ .
2. The following containments are proper

cyclic groups  $\subset$  abelian groups  $\subset$  nilpotent groups  $\subset$  solvable groups  $\subset$  all groups

3. For any finite group there must, by order considerations, be an integer  $n$  such that

$$Z_n(G) = Z_{n+1} = Z_{n+2} = \dots$$

4. For infinite groups  $G$  it may happen that all  $Z_i(G)$  are proper subgroups of  $G$  (so  $G$  is not nilpotent) but

$$G = \bigcup_{i=0}^{\infty} Z_i(G).$$

**Proposition 2.** Let  $p$  be a prime and let  $P$  be a group of order  $p^a$ . Then  $P$  is nilpotent of nilpotence class at most  $a - 1$  for all  $a \geq 2$  (and class equal to  $a$  when  $a = 0$  or  $1$ ).

**Theorem 3.** Let  $G$  be a finite group, let  $p_1, p_2, \dots, p_s$  be the distinct primes dividing its order and let  $P_i \in \text{Syl}_{p_i}(G)$ ,  $1 \leq i \leq s$ . Then the following are equivalent:

1.  $G$  is nilpotent
2. if  $H < G$  then  $H < N_G(H)$ , i.e., every proper subgroup of  $G$  is a proper subgroup of its normalizer in  $G$
3.  $P_i \trianglelefteq G$  for  $1 \leq i \leq s$ , i.e., every Sylow subgroup is normal in  $G$
4.  $G \cong P_1 \times P_2 \times \cdots \times P_s$ .

**Corollary 4.** A finite abelian group is the direct product of its Sylow subgroups.

**Proposition 5.** If  $G$  is a finite group such that for all positive integers  $n$  dividing its order,  $G$  contains at most  $n$  elements  $x$  satisfying  $x^n = 1$ , then  $G$  is cyclic.

**Proposition 6.** (Fratini's Argument) Let  $G$  be a finite group, let  $H$  be a normal subgroup of  $G$  and let  $P$  be a Sylow  $p$ -subgroup of  $H$ . Then  $G = HN_G(P)$  and  $|G : H|$  divides  $|N_G(P)|$ .

**Proposition 7.** A finite group is nilpotent if and only if every maximal subgroup is normal.

**Definition.** For any (finite or infinite) group  $G$  define the following subgroups inductively:

$$G^0 = G, \quad G^1 = [G, G] \quad \text{and} \quad G^{i+1} = [G, G^i].$$

The chain of groups

$$G^0 \geq G^1 \geq G^2 \geq \cdots$$

is called the *lower central series* of  $G$ . (The term “lower” indicates that  $G^i \geq G^{i+1}$ .)

**Theorem 8.** A group  $G$  is nilpotent if and only if  $G^n = 1$  for some  $n \geq 0$ . More precisely,  $G$  is nilpotent of class  $c$  if and only if  $c$  is the smallest nonnegative integer such that  $G^c = 1$ . If  $G$  is nilpotent of class  $c$  then

$$G^{c-i} \leq Z_i(G) \quad \text{for all } i \in \{0, 1, 2, \dots, c\}.$$

**Note.**

1. If  $G$  is abelian, we have  $G' = G^1 = 1$
2. If  $G$  is a finite group there must, by order considerations, be an integer  $n$  such that

$$G^n = G^{n+1} = G^{n+2} = \cdots.$$

**Definition.** For any group  $G$  define the following sequence of subgroups inductively:

$$G^{(0)} = G, \quad G^{(1)} = [G, G], \quad \text{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad \text{for all } i \geq 1.$$

This series of subgroups is called the *derived* or *commutator series* of  $G$ .

**Theorem 9.** A group  $G$  is solvable if and only if  $G^{(n)} = 1$  for some  $n \geq 0$ .

**Proposition 10.** Let  $G$  and  $K$  be groups, let  $H$  be a subgroup of  $G$  and let  $\varphi: G \rightarrow K$  be a surjective homomorphism.

1.  $H^{(i)} \leq G^{(i)}$  for all  $i \geq 0$ . In particular, if  $G$  is solvable, then so is  $H$ , i.e., subgroups of solvable groups are solvable (and the solvable length of  $H$  is less than or equal to the solvable length of  $G$ ).
2.  $\varphi(G^{(i)}) = K^{(i)}$ . In particular, homomorphic images and quotient groups of solvable groups are solvable (of solvable length less than or equal to that of the domain group).
3. If  $N$  is normal in  $G$  and both  $N$  and  $G/N$  are solvable then so is  $G$ .

**Theorem 11.** Let  $G$  be a finite group.

1. (Burnside) If  $|G| = p^a q^b$  for some primes  $p$  and  $q$ , then  $G$  is solvable.
2. (Philip Hall) If for every prime  $p$  dividing  $|G|$  we factor the order of  $G$  as  $|G| = p^a m$  where  $(p, m) = 1$ , and  $G$  has a subgroup of order  $m$ , then  $G$  is solvable (i.e., if for all primes  $p$ ,  $G$  has a subgroup whose index equals the order of a Sylow  $p$ -subgroup, then  $G$  is solvable — such subgroups are called Sylow  $p$ -complements).
3. (Feit-Thompson) If  $|G|$  is odd then  $G$  is solvable.
4. (Thompson) If for every pair of elements  $x, y \in G$ ,  $\langle x, y \rangle$  is a solvable group, then  $G$  is solvable.

## 6.2 Applications in Groups of Medium Order

**Proposition 12.**

1. If  $G$  has no subgroup of index 2 and  $G \leq S_k$ , then  $G \leq A_k$ .
2. If  $P \in \text{Syl}_p(S_k)$  for some odd prime  $p$ , then  $P \in \text{Syl}_p(A_k)$  and  $|N_{A_k}(P)| = \frac{1}{2}|N_{S_k}(P)|$ .

**Lemma 13.** In a finite group  $G$  is  $n_p \not\equiv 1 \pmod{p^2}$ , then there are distinct Sylow  $p$ -subgroups  $P$  and  $R$  of  $G$  such that  $P \cap R$  is of index  $p$  in both  $P$  and  $R$  (hence is normal in each).

## 6.3 A word on Free Groups

**Note.** The way that a free group is defined is a bit involved and can be read on page 216

**Theorem 16.**  $F(S)$  is a group under the binary operation defined on page 216.

**Theorem 17.** Let  $G$  be a group,  $S$  a set and  $\varphi: S \rightarrow G$  a set map. Then there is a unique group homomorphism  $\Phi: F(S) \rightarrow G$  such that the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{\text{inclusion}} & F(S) \\ & \searrow \varphi & \downarrow \Phi \\ & & G \end{array}$$

**Corollary 18.**  $F(S)$  is unique up to a unique isomorphism which is the identity map on the set  $S$ .



**Definition.** The group  $F(S)$  is called the *free group* on the set  $S$ . A group  $F$  is a *free group* if there is some set  $S$  such that  $F = F(S)$  — in this case we call  $S$  a set of *free generators* (or a *free basis*) of  $F$ . The cardinality of  $S$  is called the *rank* of the free group.

**Theorem 19.** (Schreier) Subgroups of a free group are free.

**Definition.** Let  $S$  be a subset of a group  $G$  such that  $G = \langle S \rangle$ .

1. A *presentation* for  $G$  is a pair  $(S, R)$ , where  $R$  is a set of words in  $F(S)$  such that the normal closure of  $\langle R \rangle$  in  $F(S)$  (the smallest normal subgroup containing  $\langle R \rangle$ ) equals the kernel of the homomorphism  $\pi: F(S) \rightarrow G$  (where  $\pi$  extends the identity map from  $S$  to  $S$ ). The elements of  $S$  are called *generators* and those of  $R$  are called *relations* of  $G$ .
2. We say that  $G$  is *finitely generated* if there is a presentation  $(S, R)$  such that  $S$  is a finite set and we say  $G$  is *finitely presented* if there is a presentation  $(S, R)$  with both  $S$  and  $R$  finite sets.

## Part II

# Ring Theory

## 7 Introduction to Rings

### 7.1 Basic Definitions and Examples