Course 311: Michaelmas Term 2001
Part II: Topics in Group Theory

D. R. Wilkins

Copyright © David R. Wilkins 1997–2001

Contents

2 Topics in Group Theory **2**
2.1 Groups 2
2.2 Examples of Groups 3
2.3 Elementary Properties of Groups 4
2.4 Subgroups 6
2.5 Cyclic Groups 7
2.6 Cosets and Lagrange's Theorem 8
2.7 Normal Subgroups and Quotient Groups 10
2.8 Homomorphisms 13
2.9 The Isomorphism Theorems 15
2.10 Direct products of groups 16
2.11 Cayley's Theorem 17
2.12 Group Actions, Orbits and Stabilizers 17
2.13 Conjugacy 18
2.14 Permutations and the Symmetric Groups 19
2.15 The Alternating Groups 23
2.16 Normal Subgroups of the Symmetric Groups 26
2.17 Finitely Generated Abelian Groups 27
2.18 The Class Equation of a Finite Group 30
2.19 Cauchy's Theorem 30
2.20 The Structure of p-Groups 31
2.21 The Sylow Theorems 32
2.22 Some Applications of the Sylow Theorems 34
2.23 Simple Groups 36
2.24 Solvable Groups 41

2 Topics in Group Theory

2.1 Groups

A *binary operation* $*$ on a set G associates to elements x and y of G a third element $x * y$ of G. For example, addition and multiplication are binary operations of the set of all integers.

Definition A *group* G consists of a set G together with a binary operation $*$ for which the following properties are satisfied:

- $(x * y) * z = x * (y * z)$ for all elements x, y, and z of G (the *Associative Law*);
- there exists an element e of G (known as the *identity element* of G) such that $e * x = x = x * e$, for all elements x of G;
- for each element x of G there exists an element x' of G (known as the *inverse* of x) such that $x * x' = e = x' * x$ (where e is the identity element of G).

The *order* $|G|$ of a finite group G is the number of elements of G.

A group G is *Abelian* (or *commutative*) if $x * y = y * x$ for all elements x and y of G.

One usually adopts *multiplicative notation* for groups, where the product $x * y$ of two elements x and y of a group G is denoted by xy. The inverse of an element x of G is then denoted by x^{-1}. The identity element is usually denoted by e (or by e_G when it is necessary to specify explicitly the group to which it belongs). Sometimes the identity element is denoted by 1. Thus, when multiplicative notation is adopted, the group axioms are written as follows:-

- $(xy)z = x(yz)$ for all elements x, y, and z of G (the *Associative Law*);
- there exists an element e of G (known as the *identity element* of G) such that $ex = x = xe$, for all elements x of G;
- for each element x of G there exists an element x^{-1} of G (known as the *inverse* of x) such that $xx^{-1} = e = x^{-1}x$ (where e is the identity element of G).

The group G is said to be *Abelian* (or *commutative*) if $xy = yx$ for all elements x and y of G.

It is sometimes convenient or customary to use additive notation for certain groups. Here the group operation is denoted by $+$, the identity element of the group is denoted by 0, the inverse of an element x of the group is denoted by $-x$. By convention, additive notation is only used for Abelian groups. When expressed in additive notation the axioms for a Abelian group are as follows:

- $x + y = y + x$ for all elements x and y of G (the *Commutative Law*);
- $(x+y)+z = x+(y+z)$ for all elements x, y, and z of G (the *Associative Law*);
- there exists an element 0 of G (known as the *identity element* or *zero element* of G) such that $0 + x = x = x + 0$, for all elements x of G;
- for each element x of G there exists an element $-x$ of G (known as the *inverse* of x) such that $x + (-x) = 0 = (-x) + x$ (where 0 is the identity element of G).

We shall usually employ multiplicative notation when discussing general properties of groups. Additive notation will be employed for certain groups (such as the set of integers with the operation of addition) where this notation is the natural one to use.

2.2 Examples of Groups

The sets of integers, rational numbers, real numbers and complex numbers are Abelian groups, where the group operation is the operation of addition.

The sets of non-zero rational numbers, non-zero real numbers and non-zero complex numbers are also Abelian groups, where the group operation is the operation of multiplication.

For each positive integer m the set $\mathbb{Z}_m$ of congruence classes of integers modulo m is a group, where the group operation is addition of congruence classes.

For each positive integer m the set $\mathbb{Z}_m^*$ of congruence classes modulo m of integers coprime to m is a group, where the group operation is multiplication of congruence classes.

In particular, for each prime number p the set $\mathbb{Z}_p^*$ of congruence classes modulo p of integers not divisible by p is a group, where the group operation is multiplication of congruence classes.

For each positive integer n the set of all nonsingular $n \times n$ matrices is a group, where the group operation is matrix multiplication. These groups are not Abelian when $n \geq 2$.

Let E^n denote n-dimensional Euclidean space, so that E^2 denotes the Euclidean plane, and E^3 denotes three-dimensional Euclidean space. A geometrical figure may be represented as a subset S of E^n. A *symmetry* of S is a transformation $T: E^n \to E^n$ of E^n which sends straight lines to straight lines, preserves all lengths and angles, and has the property that $T(S) = S$. The collection of all symmetries of a geometrical figure is a group, the *symmetry group of* S, the group operation being that of composition of transformations.

For any natural number n greater than 2, the the *dihedral group* D_{2n} of order $2n$ is defined to be the symmetry group of a regular n-sided polygon in the Euclidean plane. It consists of rotations though an angle of $2\pi j/n$ about the centre of the polygon for $j = 0, 1, 2, \ldots, n-1$, together with the reflections in the n axes of symmetry of the polygon.

The symmetries of a rectangle that is not a square constitute a group of order 4. This group consists of the identity transformation, reflection in the axis of symmetry joining the midpoints of the two shorter sides, reflection in the axis of symmetry joining the two longer sides, and rotation though an angle of π radians (180°). If I denotes the identity transformation, A and B denote the reflections in the two axes of symmetry, and C denotes the rotation through π radians then $A^2 = B^2 = C^2 = I$, $AB = BA = C$, $AC = CA = B$ and $BC = CB = A$. This group is Abelian: it is often referred to as the *Klein 4-group* (or, in German, *Kleinsche Viergruppe*).

The symmetries of a regular tetrahedron in 3-dimensional space constitute a group. Any permutation of the vertices of the tetrahedron can be effected by an appropriate symmetry of the tetrahedron. Moreover each symmetry is completely determined by the permutation of the vertices which it induces. Therefore the group of symmetries of a regular tetrahedron is of order 24, since there are 24 permutations of a set with four elements. It turns out that this group is non-Abelian.

2.3 Elementary Properties of Groups

In what follows, we describe basic properties of a group G, using multiplicative notation and denoting the identity element of the group by the letter e.

Lemma 2.1 *A group G has exactly one identity element e satisfying $ex = x = xe$ for all $x \in G$.*

Proof Suppose that f is an element of G with the property that $fx = x$ for

all elements x of G. Then in particular $f = fe = e$. Similarly one can show that e is the only element of G satisfying $xe = x$ for all elements x of G. ∎

Lemma 2.2 *An element x of a group G has exactly one inverse x^{-1}.*

Proof We know from the axioms that the group G contains at least one element x^{-1} which satisfies $xx^{-1} = e$ and $x^{-1}x = e$. If z is any element of G which satisfies $xz = e$ then $z = ez = (x^{-1}x)z = x^{-1}(xz) = x^{-1}e = x^{-1}$. Similarly if w is any element of G which satisfies $wx = e$ then $w = x^{-1}$. In particular we conclude that the inverse x^{-1} of x is uniquely determined, as required. ∎

Lemma 2.3 *Let x and y be elements of a group G. Then $(xy)^{-1} = y^{-1}x^{-1}$.*

Proof It follows from the group axioms that

$$(xy)(y^{-1}x^{-1}) = x(y(y^{-1}x^{-1})) = x((yy^{-1})x^{-1}) = x(ex^{-1}) = xx^{-1} = e.$$

Similarly $(y^{-1}x^{-1})(xy) = e$, and thus $y^{-1}x^{-1}$ is the inverse of xy, as required. ∎

Note in particular that $(x^{-1})^{-1} = x$ for all elements x of a group G, since x has the properties that characterize the inverse of the inverse x^{-1} of x.

Given an element x of a group G, we define x^n for each positive integer n by the requirement that $x^1 = x$ and $x^n = x^{n-1}x$ for all $n > 1$. We also define $x^0 = e$, where e is the identity element of the group, and we define x^{-n} to be the inverse of x^n for all positive integers n.

Theorem 2.4 *Let x be an element of a group G. Then $x^{m+n} = x^m x^n$ and $x^{mn} = (x^m)^n$ for all integers m and n.*

Proof The identity $x^{m+n} = x^m x^n$ clearly holds when $m = 0$ and when $n = 0$. The identity $x^{m+n} = x^m x^n$ can be proved for all positive integers m and n by induction on n. The identity when m and n are both negative then follows from the identity $x^{-m-n} = x^{-n}x^{-m}$ on taking inverses. The result when m and n have opposite signs can easily be deduced from that where m and n both have the same sign.

The identity $x^{mn} = (x^m)^n$ follows immediately from the definitions when $n = 0$, 1 or -1. The result when n is positive can be proved by induction on n. The result when n is negative can then be obtained on taking inverses. ∎

If additive notation is employed for an Abelian group then the notation 'x^n' is replaced by 'nx' for all integers n and elements x of the group. The analogue of Theorem 2.4 then states that $(m+n)x = mx+nx$ and $(mn)x = m(n(x))$ for all integers m and n.

The associative law may be generalized to products of four or more elements of a group.

Example Given four elements x_1, x_2, x_3 and x_4 of a group, the products

$$((x_1x_2)x_3)x_4, \quad (x_1x_2)(x_3x_4), \quad (x_1(x_2x_3))x_4, \quad x_1((x_2x_3)x_4), \quad x_1(x_2(x_3x_4))$$

all have the same value. (Note that $x_1x_2x_3x_4$ is by definition the value of the first of these expressions.)

Two expressions, each specifying a finite product of elements of a group G, determine the same element of G if the same elements of G occur in both expressions, and in the same order. This result can be proved by induction on the number of elements of G making up such a product.

2.4 Subgroups

Definition Let G be a group, and let H be a subset of G. We say that H is a *subgroup* of G if the following conditions are satisfied:

- the identity element of G is an element of H;
- the product of any two elements of H is itself an element of H;
- the inverse of any element of H is itself an element of H.

Lemma 2.5 *Let x be an element of a group G. Then the set of all elements of G that are of the form x^n for some integer n is a subgroup of G.*

Proof Let $H = \{x^n : n \in \mathbb{Z}\}$. Then the identity element belongs to H, since it is equal to x^0. The product of two elements of H is itself an element of H, since $x^m x^n = x^{m+n}$ for all integers m and n (see Theorem 2.4). Also the inverse of an element of H is itself an element of H since $(x^n)^{-1} = x^{-n}$ for all integers n. Thus H is a subgroup of G, as required. ∎

Definition Let x be an element of a group G. The *order* of x is the smallest positive integer n for which $x^n = e$. The subgroup *generated* by x is the subgroup consisting of all elements of G that are of the form x^n for some integer n.

Lemma 2.6 *Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.*

Proof The identity element of G belongs to $H \cap K$ since it belongs to the subgroups H and K. If x and y are elements of $H \cap K$ then xy is an element of H (since x and y are elements of H), and xy is an element of K, and therefore xy is an element of $H \cap K$. Also the inverse x^{-1} of an element x of $H \cap K$ belongs to H and to K and thus belongs to $H \cap K$, as required. ∎

More generally, the intersection of any collection of subgroups of a given group is itself a subgroup of that group.

2.5 Cyclic Groups

Definition A group G is said to be *cyclic*, with generator x, if every element of G is of the form x^n for some integer n.

Example The group $\mathbb{Z}$ of integers under addition is a cyclic group, generated by 1.

Example Let n be a positive integer. The set $\mathbb{Z}_n$ of congruence classes of integers modulo n is a cyclic group of order n with respect to the operation of addition.

Example The group of all rotations of the plane about the origin through an integer multiple of $2\pi/n$ radians is a cyclic group of order n for all integers n. This group is generated by an anticlockwise rotation through an angle of $2\pi/n$ radians.

Lemma 2.7 *Let G be a finite cyclic group with generator x, and let j and k be integers. Then $x^j = x^k$ if and only if $j - k$ is divisible by the order of the group.*

Proof First we show that $x^m = e$ for some strictly positive integer m, where e is the identity element of G. Now $x^j = x^k$ for some integers j and k with $j < k$, since G is finite. Let $m = k - j$. Then $m > 0$ and $x^m = x^k(x^j)^{-1} = e$.

Let n be the smallest strictly positive integer for which $x^n = e$. Now any integer i can be expressed in the form $i = qn + r$, where q and r are integers and $0 \leq r < n$. (Thus q is the greatest integer for which $qn \leq i$.) Then $x^i = (x^n)^q x^r = x^r$ (since $x^n = e$). Now the choice of n ensures that $x^r \neq e$ if $0 < r < n$. It follows that an integer i satisfies $x^i = e$ if and only if n divides i.

Let j and k be integers. Now $x^j = x^k$ if and only if $x^{j-k} = e$, since $x^{j-k} = x^j(x^k)^{-1}$. It follows that $x^j = x^k$ if and only if $j - k$ is divisible by n. Moreover n is the order of the group G, since each element of G is equal to one of the elements x^i with $0 \leq i < n$ and these elements are distinct. ∎

We now classify all subgroups of a cyclic group G. Let x be a generator of G. Given a subgroup H of G with more than one element, let m be the smallest strictly positive integer for which $x^m \in H$. Suppose that $x^i \in H$ for some integer i. Now i can be expressed in the form $i = qm + r$, where q and r are integers and $0 \leq r < m$. (Thus q is the greatest integer for which $qm \leq i$.) But then $x^r = x^{i-qm} = x^i(x^m)^{-q}$, where $x^i \in H$ and $x^m \in H$, and therefore $x^r \in H$. The choice of m now ensures that $r = 0$, and hence $i = qm$. Thus $x^i \in H$ if and only if i is some integer multiple of m. This shows that H is the cyclic group generated by x^m, where m is the smallest strictly positive integer for which $x^m \in H$.

Let us consider the case when the cyclic group G is finite. Let s be the order of G. Then $x^s = e$, and hence x^s belongs to the subgroup H. It follows that s must be some integer multiple of m, where m is the smallest strictly positive integer for which $x^m \in H$. Thus the subgroups of a finite cyclic group G with generator g are the trivial subgroup $\{e\}$ and the cyclic subgroups generated by x^m for each divisor m of the order of G.

Consider now the case when the cyclic group G is infinite. For each positive integer m, the element x^m generates a subgroup of G, and moreover m is the smallest strictly positive integer for which x^m belongs to that subgroup. Thus if G is an infinite cyclic group with generator x then the subgroups of G are the trivial subgroup $\{e\}$ and the cyclic subgroups generated by x^m for each positive integer m.

We have thus classified all subgroups of a cyclic group. In particular we see that any subgroup of a cyclic group is itself a cyclic group.

2.6 Cosets and Lagrange's Theorem

Definition Let H be a subgroup of a group G. A *left coset* of H in G is a subset of G that is of the form xH, where $x \in G$ and

$$xH = \{y \in G : y = xh \text{ for some } h \in H\}.$$

Similarly a *right coset* of H in G is a subset of G that is of the form Hx, where $x \in G$ and

$$Hx = \{y \in G : y = hx \text{ for some } h \in H\}.$$

Note that a subgroup H of a group G is itself a left coset of H in G.

Lemma 2.8 *Let H be a subgroup of a group G. Then the left cosets of H in G have the following properties:—*

(i) *$x \in xH$ for all $x \in G$;*

(ii) *if x and y are elements of G, and if $y = xa$ for some $a \in H$, then $xH = yH$;*

(iii) *if x and y are elements of G, and if $xH \cap yH$ is non-empty then $xH = yH$.*

Proof Let $x \in G$. Then $x = xe$, where e is the identity element of G. But $e \in H$. It follows that $x \in xH$. This proves (i).

Let x and y be elements of G, where $y = xa$ for some $a \in H$. Then $yh = x(ah)$ and $xh = y(a^{-1}h)$ for all $h \in H$. Moreover $ah \in H$ and $a^{-1}h \in H$ for all $h \in H$, since H is a subgroup of G. It follows that $yH \subset xH$ and $xH \subset yH$, and hence $xH = yH$. This proves (ii).

Finally suppose that $xH \cap yH$ is non-empty for some elements x and y of G. Let z be an element of $xH \cap yH$. Then $z = xa$ for some $a \in H$, and $z = yb$ for some $b \in H$. It follows from (ii) that $zH = xH$ and $zH = yH$. Therefore $xH = yH$. This proves (iii). ∎

Lemma 2.9 *Let H be a finite subgroup of a group G. Then each left coset of H in G has the same number of elements as H.*

Proof Let $H = \{h_1, h_2, \ldots, h_m\}$, where $h_1, h_2, \ldots, h_m$ are distinct, and let x be an element of G. Then the left coset xH consists of the elements xh_j for $j = 1, 2, \ldots, m$. Suppose that j and k are integers between 1 and m for which $xh_j = xh_k$. Then $h_j = x^{-1}(xh_j) = x^{-1}(xh_k) = h_k$, and thus $j = k$, since $h_1, h_2, \ldots, h_m$ are distinct. It follows that the elements $xh_1, xh_2, \ldots, xh_m$ are distinct. We conclude that the subgroup H and the left coset xH both have m elements, as required. ∎

Theorem 2.10 (Lagrange's Theorem) *Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.*

Proof Each element of G belongs to at least one left coset of H in G, and no element can belong to two distinct left cosets of H in G (see Lemma 2.8). Therefore every element of G belongs to exactly one left coset of H. Moreover each left coset of H contains $|H|$ elements (Lemma 2.9). Therefore $|G| = n|H|$, where n is the number of left cosets of H in G. The result follows. ∎

Definition Let H be a subgroup of a group G. If the number of left cosets of H in G is finite then the number of such cosets is referred to as the *index* of H in G, denoted by $[G\colon H]$.

The proof of Lagrange's Theorem shows that the index $[G\colon H]$ of a subgroup H of a finite group G is given by $[G\colon H] = |G|/|H|$.

Corollary 2.11 *Let x be an element of a finite group G. Then the order of x divides the order of G.*

Proof Let H be the set of all elements of G that are of the form x^n for some integer n. Then H is a subgroup of G (see Lemma 2.5), and the order of H is the order of x. But the order of H divides G by Lagrange's Theorem (Theorem 2.10). The result follows. ∎

Corollary 2.12 *Any finite group of prime order is cyclic.*

Proof Let G be a group of prime order, and let x be some element of G that is not the identity element. Then the order of x is greater than one and divides the order of G. But then the order of x must be equal to the order of G, since the latter is a prime number. Thus G is a cyclic group generated by x, as required. ∎

2.7 Normal Subgroups and Quotient Groups

Let A and B be subsets of a group G. The *product* AB of the sets A and B is defined by

$$AB = \{xy : x \in A \text{ and } y \in B\}.$$

We denote $\{x\}A$ and $A\{x\}$ by xA and Ax, for all elements x of G and subsets A of G. The Associative Law for multiplication of elements of G ensures that $(AB)C = A(BC)$ for all subsets A, B and C of G. We can therefore use the notation ABC to denote the products $(AB)C$ and $A(BC)$; and we can use analogous notation to denote the product of four or more subsets of G.

If A, B and C are subsets of a group G, and if $A \subset B$ then clearly $AC \subset BC$ and $CA \subset CB$.

Note that if H is a subgroup of the group G and if x is an element of G then xH is the left coset of H in G that contains the element x. Similarly Hx is the right coset of H in G that contains the element x.

If H is a subgroup of G then $HH = H$. Indeed $HH \subset H$, since the product of two elements of a subgroup H is itself an element of H. Also $H \subset HH$ since $h = eh$ for any element h of H, where e, the identity element of G, belongs to H.

Definition A subgroup N of a group G is said to be a *normal subgroup* of G if $xnx^{-1} \in N$ for all $n \in N$ and $x \in G$.

The notation '$N \triangleleft G$' signifies 'N is a normal subgroup of G'.

Definition A non-trivial group G is said to be *simple* if the only normal subgroups of G are the whole of G and the trivial subgroup $\{e\}$ whose only element is the identity element e of G.

Lemma 2.13 *Every subgroup of an Abelian group is a normal subgroup.*

Proof Let N be a subgroup of an Abelian group G. Then

$$xnx^{-1} = (xn)x^{-1} = (nx)x^{-1} = n(xx^{-1}) = ne = n$$

for all $n \in N$ and $x \in G$, where e is the identity element of G. The result follows. ∎

Example Let S_3 be the group of permutations of the set $\{1, 2, 3\}$, and let H be the subgroup of S_3 consisting of the identity permutation and the transposition $(1\,2)$. Then H is not normal in G, since $(2\,3)^{-1}(1\,2)(2\,3) = (2\,3)(1\,2)(2\,3) = (1\,3)$ and $(1\,3)$ does not belong to the subgroup H.

Proposition 2.14 *A subgroup N of a group G is a normal subgroup of G if and only if $xNx^{-1} = N$ for all elements x of G.*

Proof Suppose that N is a normal subgroup of G. Let x be an element of G. Then $xNx^{-1} \subset N$. (This follows directly from the definition of a normal subgroup.) On replacing x by x^{-1} we see also that $x^{-1}Nx \subset N$, and thus $N = x(x^{-1}Nx)x^{-1} \subset xNx^{-1}$. Thus each of the sets N and xNx^{-1} is contained in the other, and therefore $xNx^{-1} = N$.

Conversely if N is a subgroup of G with the property that $xNx^{-1} = N$ for all $x \in G$, then it follows immediately from the definition of a normal subgroup that N is a normal subgroup of G. ∎

Corollary 2.15 *A subgroup N of a group G is a normal subgroup of G if and only if $xN = Nx$ for all elements x of G.*

Proof Let N be a subgroup of G, and let x be an element of G. If $xNx^{-1} = N$ then $xN = (xNx^{-1})x = Nx$. Conversely if $xN = Nx$ then $xNx^{-1} = Nxx^{-1} = Ne = N$, where e is the identity element of G. Thus $xN = Nx$ if and only if $xNx^{-1} = N$. It follows from Proposition 2.14 that a subgroup N of G is normal if and only if $xN = Nx$ for all elements x of G, as required. ∎

Let N be a normal subgroup of G. Corollary 2.15 shows that a subset of G is a left coset of N in G if and only if it is a right coset of N in G. We may therefore refer to the left and right cosets of a normal subgroup N as *cosets* of N in G (since it is not in this case necessary to distinguish between left and right cosets).

Lemma 2.16 *Let N be a normal subgroup of a group G and let x and y be elements of G. Then $(xN)(yN) = (xy)N$.*

Proof If N is a normal subgroup of G then $Ny = yN$, and therefore $(xN)(yN) = x(Ny)N = x(yN)N = (xy)(NN)$. But $NN = N$, since N is a subgroup of G. Therefore $(xN)(yN) = (xy)N$, as required. ∎

Proposition 2.17 *Let G be a group, and let N be a normal subgroup of G. Then the set of all cosets of N in G is a group under the operation of multiplication. The identity element of this group is N itself, and the inverse of a coset xN is the coset $x^{-1}N$ for any element x of G.*

Proof Let x, y and z be any elements of G. Then the product of the cosets xN and yN is the coset $(xy)N$. The subgroup N is itself a coset of N in G, since $N = eN$. Moreover

$$(xN)N = (xN)(eN) = (xe)N = xN,$$

$$N(xN) = (eN)(xN) = (ex)N = xN,$$

$$(xN)(x^{-1}N) = (xx^{-1})N = N,$$

$$(x^{-1}N)(xN) = (x^{-1}x)N = N.$$

for all elements x of G. Thus the group axioms are satisfied. ∎

Definition Let N be a normal subgroup of a group G. The *quotient group* G/N is defined to be the group of cosets of N in G under the operation of multiplication.

Example Consider the dihedral group D_8 of order 8, which we represent as the group of symmetries of a square in the plane with corners at the points whose Cartesian co-ordinates are $(1, 1)$, $(-1, 1)$, $(-1, -1)$ and $(1, -1)$. Then

$$D_8 = \{\mathbf{I}, \mathbf{R}, \mathbf{R}^2, \mathbf{R}^3, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \mathbf{T}_4\},$$

where $\mathbf{I}$ denotes the identity transformation, $\mathbf{R}$ denotes an anticlockwise rotation about the origin through a right angle, and $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ and $\mathbf{T}_4$ denote

the reflections in the lines $y = 0$, $x = y$, $x = 0$ and $x = -y$ respectively. Let $N = \{\mathbf{I}, \mathbf{R}^2\}$. Then N is a subgroup of D_8. The left cosets of N in D_8 are N, A, B and C, where

$$A = \{\mathbf{R}, \mathbf{R}^3\}, \qquad B = \{\mathbf{T}_1, \mathbf{T}_3\}, \qquad C = \{\mathbf{T}_2, \mathbf{T}_4\}.$$

Moreover N, A, B and C are also the right cosets of N in D_8, and thus N is a normal subgroup of D_8. On multiplying the cosets A, B and C with one another we find that $AB = BA = C$, $AC = CA = B$ and $BC = CB = A$. The quotient group D_8/N consists of the set $\{N, A, B, C\}$, with the group operation just described.

2.8 Homomorphisms

Definition A homomorphism $\theta: G \to K$ from a group G to a group K is a function with the property that $\theta(g_1 * g_2) = \theta(g_1) * \theta(g_2)$ for all $g_1, g_2 \in G$, where $*$ denotes the group operation on G and on K.

Example Let q be an integer. The function from the group $\mathbb{Z}$ of integers to itself that sends each integer n to qn is a homomorphism.

Example Let x be an element of a group G. The function that sends each integer n to the element x^n is a homomorphism from the group $\mathbb{Z}$ of integers to G, since $x^{m+n} = x^m x^n$ for all integers m and n (Theorem 2.4).

Lemma 2.18 *Let $\theta: G \to K$ be a homomorphism. Then $\theta(e_G) = e_K$, where e_G and e_K denote the identity elements of the groups G and K. Also $\theta(x^{-1}) = \theta(x)^{-1}$ for all elements x of G.*

Proof Let $z = \theta(e_G)$. Then $z^2 = \theta(e_G)\theta(e_G) = \theta(e_G e_G) = \theta(e_G) = z$. The result that $\theta(e_G) = e_K$ now follows from the fact that an element z of K satisfies $z^2 = z$ if and only if z is the identity element of K.

Let x be an element of G. The element $\theta(x^{-1})$ satisfies $\theta(x)\theta(x^{-1}) = \theta(xx^{-1}) = \theta(e_G) = e_K$, and similarly $\theta(x^{-1})\theta(x) = e_K$. The uniqueness of the inverse of $\theta(x)$ now ensures that $\theta(x^{-1}) = \theta(x)^{-1}$. ∎

An *isomorphism* $\theta: G \to K$ between groups G and K is a homomorphism that is also a bijection mapping G onto K. Two groups G and K are *isomorphic* if there exists an isomorphism mapping G onto K.

Example Let D_6 be the group of symmetries of an equilateral triangle in the plane with vertices A, B and C, and let S_3 be the group of permutations of the set $\{A, B, C\}$. The function which sends a symmetry of the triangle to the corresponding permutation of its vertices is an isomorphism between the dihedral group D_6 of order 6 and the symmetric group S_3.

Example Let $\mathbb{R}$ be the group of real numbers with the operation of addition, and let $\mathbb{R}^+$ be the group of strictly positive real numbers with the operation of multiplication. The function $\exp\colon \mathbb{R} \to \mathbb{R}^+$ that sends each real number x to the positive real number e^x is an isomorphism: it is both a homomorphism of groups and a bijection. The inverse of this isomorphism is the function $\log\colon \mathbb{R}^+ \to \mathbb{R}$ that sends each strictly positive real number to its natural logarithm.

Here is some further terminology regarding homomorphisms:

- A *monomorphism* is an injective homomorphism.
- An *epimorphism* is a surjective homomorphism.
- An *endomorphism* is a homomorphism mapping a group into itself.
- An *automorphism* is an isomorphism mapping a group onto itself.

Definition The *kernel* $\ker\theta$ of the homomorphism $\theta\colon G \to K$ is the set of all elements of G that are mapped by θ onto the identity element of K.

Example Let the group operation on the set $\{+1, -1\}$ be multiplication, and let $\theta\colon \mathbb{Z} \to \{+1, -1\}$ be the homomorphism that sends each integer n to $(-1)^n$. Then the kernel of the homomorphism θ is the subgroup of $\mathbb{Z}$ consisting of all even numbers.

Lemma 2.19 *Let G and K be groups, and let $\theta\colon G \to K$ be a homomorphism from G to K. Then the kernel $\ker\theta$ of θ is a normal subgroup of G.*

Proof Let x and y be elements of $\ker\theta$. Then $\theta(x) = e_K$ and $\theta(y) = e_K$, where e_K denotes the identity element of K. But then $\theta(xy) = \theta(x)\theta(y) = e_K e_K = e_K$, and thus xy belongs to $\ker\theta$. Also $\theta(x^{-1}) = \theta(x)^{-1} = e_K^{-1} = e_K$, and thus x^{-1} belongs to $\ker\theta$. We conclude that $\ker\theta$ is a subgroup of K. Moreover $\ker\theta$ is a normal subgroup of G, for if $g \in G$ and $x \in \ker\theta$ then

$$\theta(gxg^{-1}) = \theta(g)\theta(x)\theta(g)^{-1} = \theta(g)\theta(g^{-1}) = e_K. \qquad \blacksquare$$

If N is a normal subgroup of some group G then N is the kernel of the *quotient homomorphism* $\theta\colon G \to G/N$ that sends $g \in G$ to the coset gN. It follows therefore that a subset of a group G is a normal subgroup of G if and only if it is the kernel of some homomorphism.

Proposition 2.20 *Let G and K be groups, let $\theta: G \to K$ be a homomorphism from G to K, and let N be a normal subgroup of G. Suppose that $N \subset \ker \theta$. Then the homomorphism $\theta: G \to K$ induces a homomorphism $\hat{\theta}: G/N \to K$ sending $gN \in G/N$ to $\theta(g)$. Moreover $\hat{\theta}: G/N \to K$ is injective if and only if $N = \ker \theta$.*

Proof Let x and y be elements of G. Now $xN = yN$ if and only if $x^{-1}y \in N$. Also $\theta(x) = \theta(y)$ if and only if $x^{-1}y \in \ker \theta$. Thus if $N \subset \ker \theta$ then $\theta(x) = \theta(y)$ whenever $xN = yN$, and thus $\theta: G \to K$ induces a well-defined function $\hat{\theta}: G/N \to K$ sending $xN \in G/N$ to $\theta(x)$. This function is a homomorphism, since $\hat{\theta}((xN)(yN)) = \hat{\theta}(xyN) = \theta(xy) = \theta(x)\theta(y) = \hat{\theta}(xN)\hat{\theta}(yN)$.

Suppose now that $N = \ker \theta$. Then $\theta(x) = \theta(y)$ if and only if $xN = yN$. Thus the homomorphism $\hat{\theta}: G/N \to K$ is injective. Conversely if $\hat{\theta}: G/N \to K$ is injective then N must be the kernel of θ, as required. ∎

Corollary 2.21 *Let G and K be groups, and let $\theta: G \to K$ be a homomorphism. Then $\theta(G) \cong G/\ker \theta$.*

2.9 The Isomorphism Theorems

Lemma 2.22 *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then the set HN is a subgroup of G, where $HN = \{hn : h \in H \text{ and } n \in N\}$.*

Proof The set HN clearly contains the identity element of G. Let x and y be elements of HN. We must show that xy and x^{-1} belong to HN. Now $x = hu$ and $y = kv$ for some elements h and k of H and for some elements u and v of N. Then $xy = (hk)(k^{-1}ukv)$. But $k^{-1}uk \in N$, since N is normal. It follows that $k^{-1}ukv \in N$, since N is a subgroup and $k^{-1}ukv$ is the product of the elements $k^{-1}uk$ and v of N. Also $hk \in H$. It follows that $xy \in HN$.

We must also show that $x^{-1} \in HN$. Now $x^{-1} = u^{-1}h^{-1} = h^{-1}(hu^{-1}h^{-1})$. Also $h^{-1} \in H$, since H is a subgroup of G, and $hu^{-1}h^{-1} \in N$, since N is a normal subgroup of G. It follows that $x^{-1} \in HN$, and thus HN is a subgroup of G, as required. ∎

Theorem 2.23 (First Isomorphism Theorem) *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then*

$$\frac{HN}{N} \cong \frac{H}{N \cap H}.$$

Proof Every element of HN/N is a coset of N that is of the form hN for some $h \in H$. Thus if $\varphi(h) = hN$ for all $h \in H$ then $\varphi: H \to HN/N$ is a surjective homomorphism, and $\ker \varphi = N \cap H$. But $\varphi(H) \cong H/\ker \varphi$ (Corollary 2.21). Therefore $HN/N \cong H/(N \cap H)$ as required. ∎

Theorem 2.24 (Second Isomorphism Theorem) *Let M and N be normal subgroups of a group G, where $M \subset N$. Then*

$$\frac{G}{N} \cong \frac{G/M}{N/M}.$$

Proof There is a well-defined homomorphism $\theta: G/M \to G/N$ that sends gM to gN for all $g \in G$. Moreover the homomorphism θ is surjective, and $\ker \theta = N/M$. But $\theta(G/M) \cong (G/M)/\ker \theta$ (Corollary 2.21). Therefore G/N is isomorphic to $(G/M)\,/\,(N/M)$, as required. ∎

2.10 Direct products of groups

Let $G_1, G_2, \ldots, G_n$ be groups, and let G be the Cartesian product $G_1 \times G_2 \times \cdots \times G_n$ of $G_1, G_2, \ldots, G_n$ (when the latter are regarded as sets). Then the elements of G are n-tuples $(x_1, x_2, \ldots, x_n)$ where $x_i \in G_i$ for $i = 1, 2, \ldots, n$. We can multiply two elements of G as follows:

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

One can readily verify that G is a group with respect to this binary operation: multiplication is associative; the identity element of the group is $(e_1, e_2, \ldots, e_n)$, where e_i is the identity element of G_i for each i; and the inverse of an element $(x_1, x_2, \ldots, x_n)$ of G is $(x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1})$. We say that the group G is the *direct product* of the groups $G_1, G_2, \ldots, G_n$: this direct product is (not surprisingly) denoted by $G_1 \times G_2 \times \cdots \times G_n$.

Example Let C_2 and C_3 be cyclic groups of orders 2 and 3 respectively. Then $C_2 \times C_3$ is a cyclic group of order 6, and $C_2 \times C_2$ is isomorphic to the Klein 4-group that consists of the symmetries of a rectangle in the Euclidean plane that is not a square.

Let us first consider $C_2 \times C_3$. Let x and y be generators of C_2 and C_3 respectively, and let e and e' denote the identity elements of C_2 and C_3. Thus $C_2 = \{e, x\}$ and $C_3 = \{e', y, y^2\}$, where $x^2 = e$ and $y^3 = e'$. The elements of $C_2 \times C_3$ are

$$(e, e'), \quad (e, y), \quad (e, y^2), \quad (x, e'), \quad (x, y), \quad (x, y^2).$$

Let $z = (x, y)$. On computing the powers of z we find that

$$z^2 = (e, y^2), \quad z^3 = (x, e'), \quad z^4 = (e, y), \quad z^5 = (x, y^2), \quad z^6 = (e, e').$$

Thus 6 is the smallest positive integer n for which z^n is equal to the identity element (e, e') of the group. We deduce that the group $C_2 \times C_3$ (which is a group of order 6) must be a cyclic group generated by the element z.

Next consider $C_2 \times C_2$. This has four elements I, A, B and C, where $I = (e, e)$, $A = (e, x)$, $B = (x, e)$ and $C = (x, x)$. If we calculate the Cayley table for the group, we discover that it is that of the Klein 4-group.

2.11 Cayley's Theorem

Theorem 2.25 (Cayley's Theorem) *Let G be a group of order n. Then G is isomorphic to a subgroup of the group S_n of permutations of a set of n elements.*

Proof For each element x of G, let $\sigma_x : G \to G$ be the function defined such that $\sigma_x(g) = xg$ for all $g \in G$. Now

$$\sigma_{x^{-1}}(\sigma_x(g)) = x^{-1}(xg) = (x^{-1}x)g = g$$

and

$$\sigma_x(\sigma_{x^{-1}}(g)) = x(x^{-1}g) = (xx^{-1})g = g$$

for all $g \in G$. It follows that, for any $x \in G$, the function $\sigma_x : G \to G$ is a bijection whose inverse is $\sigma_{x^{-1}}$. It follows that σ_x is a permutation of G for all $x \in G$, and thus the function sending an element x of G to the permutation σ_x is a function from G to the group of permutations of G. This function is a homomorphism. Indeed $\sigma_{xy} = \sigma_x \circ \sigma_y$ since $\sigma_{xy}(g) = (xy)g = x(yg) = \sigma_x(\sigma_y(g))$ for all $g \in G$. The homomorphism sending $x \in G$ to σ_x is be injective, for if σ_x is the identity permutation then $xg = g$ for all $g \in G$, and hence x is the identity element of G. It follows that G is isomorphic to the image of the homomorphism. This image is a subgroup $\{\sigma_x : x \in G\}$ of the group of permutations of G. The result follows. ∎

2.12 Group Actions, Orbits and Stabilizers

Definition A *left action* of a group G on a set X associates to each $g \in G$ and $x \in X$ an element $g.x$ of X in such a way that $g.(h.x) = (gh).x$ and $1.x = x$ for all $g, h \in G$ and $x \in X$, where 1 denotes the identity element of G.

Given a left action of a group G on a set X, the *orbit* of an element x of X is the subset $\{g.x : g \in G\}$ of X, and the *stabilizer* of x is the subgroup $\{g \in G : g.x = x\}$ of G.

Lemma 2.26 *Let G be a finite group which acts on a set X on the left. Then the orbit of an element x of X contains $[G\colon H]$ elements, where $[G\colon H]$ is the index of the stabilizer H of x in G.*

Proof There is a well-defined function $\theta\colon G/H \to X$ defined on the set G/H of left cosets of H in G which sends gH to $g.x$ for all $g \in G$. Moreover this function is injective, and its image is the orbit of x. The result follows. ∎

2.13 Conjugacy

Definition Two elements h and k of a group G are said to be *conjugate* if $k = ghg^{-1}$ for some $g \in G$.

One can readily verify that the relation of conjugacy is reflexive, symmetric and transitive and is thus an equivalence relation on a group G. The equivalence classes determined by this relation are referred to as the *conjugacy classes* of G. A group G is the disjoint union of its conjugacy classes. Moreover the conjugacy class of the identity element of G contains no other element of G.

A group G is Abelian if and only if all its conjugacy classes contain exactly one element of the group G.

Definition Let G be a group. The *centralizer* $C(h)$ of an element h of G is the subgroup of G defined by $C(h) = \{g \in G : gh = hg\}$.

Lemma 2.27 *Let G be a finite group, and let $h \in G$. Then the number of elements in the conjugacy class of h is equal to the index $[G\colon C(h)]$ of the centralizer $C(h)$ of h in G.*

Proof There is a well-defined function $f\colon G/C(h) \to G$, defined on the set $G/C(h)$ of left cosets of $C(h)$ in G, which sends the coset $gC(h)$ to ghg^{-1} for all $g \in G$. This function is injective, and its image is the conjugacy class of h. The result follows. ∎

Let H be a subgroup of a group G. One can easily verify that gHg^{-1} is also a subgroup of G for all $g \in G$, where $gHg^{-1} = \{ghg^{-1} : h \in H\}$.

Definition Two subgroups H and K of a group G are said to be *conjugate* if $K = gHg^{-1}$ for some $g \in G$.

The relation of conjugacy is an equivalence relation on the collection of subgroups of a given group G.

2.14 Permutations and the Symmetric Groups

A *permutation* of a set S is a bijective function $p: S \to S$ from S to itself.

The *identity* permutation of a set S is the permutation that fixes every element of S.

Permutations of a finite set S are conveniently represented in a two row form

$$\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ p(x_1) & p(x_2) & \dots & p(x_n) \end{pmatrix},$$

where $x_1, x_2, \dots, x_n$ are the elements of the set S and $p(x_1), p(x_2), \dots, p(x_n)$ are the images of these elements under the permutation p being represented. Thus for example

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

represents the permutation of the set $\{1, 2, 3\}$ that sends 1 to 2, sends 2 to 3, and sends 3 to 1.

Example There are two permutations of a set $\{a, b\}$ with two elements. These are the identity permutation $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$ and the transposition $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ that interchanges the elements a and b.

Example There are six permutations of a set $\{a, b, c\}$ with three elements. These are

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix},$$

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}.$$

Let S be a set. Then the composition of any two permutations of S is itself a permutation of S (since the composition of two bijections is a bijection). Also any permutation p of S has a well-defined inverse p^{-1}. (This follows from the fact that the inverse of a bijection is itself a bijection.) Composition of permutations is associative: $(p \circ q) \circ r = p \circ (q \circ r)$ for all permutations p, q and r of S. (This can be verified by noting that $((p \circ q) \circ r)(x) = p(q(r(x))) = (p \circ (q \circ r))(x)$ for all elements x of S.) It follows from this that the set of all permutations of a set S is a group, where the group operation is composition of permutations.

Definition For each natural number n, the *symmetric group* Σ_n is the group of permutations of the set $\{1, 2, \dots, n\}$.

Let S be a set, and let $a_1, a_2, \ldots, a_n$ be distinct elements of S. We denote by $(a_1\, a_2 \cdots a_n)$ the permutation of S that sends a_i to a_{i+1} for $i = 1, 2, \ldots, n-1$, sends a_n to a_1, and fixes all other elements of S. Such a permutation is called a *cycle* of order n, or *n-cycle*. A cycle of length 2 is also called a *transposition*.

(Note that evaluating a composition of cycles, we shall compose them from right to left, in accordance with standard practice when composing functions.)

Example There are 24 permutations of a set $\{a, b, c, d\}$ with exactly four elements. These are the following: the identity permutation that fixes every element of the set; the six transpositions $(a\, b)$, $(a\, c)$, $(a\, d)$, $(b\, c)$, $(b\, d)$ and $(c\, d)$; the eight 3-cycles $(b\, c\, d)$, $(b\, d\, c)$, $(a\, c\, d)$, $(a\, d\, c)$, $(a\, b\, d)$, $(a\, d\, b)$, $(a\, b\, c)$ and $(a\, c\, b)$; the six 4-cycles $(a\, b\, c\, d)$, $(a\, b\, d\, c)$, $(a\, c\, b\, d)$, $(a\, c\, d\, b)$, $(a\, d\, b\, c)$ and $(a\, d\, c\, b)$; and three further permutations $(a\, b)(c\, d)$, $(a\, c)(b\, d)$ and $(a\, d)(b\, c)$.

Two cycles $(a_1\, a_2 \cdots a_m)$ and $(b_1\, b_2 \cdots b_n)$ are said to be *disjoint* when the elements $a_1, a_2, \ldots, a_m$ and $b_1, b_2, \ldots, b_n$ are distinct (i.e., no pair of these elements coincide).

It is easy to see that if $(a_1\, a_2 \cdots a_m)$ and $(b_1\, b_2 \cdots b_n)$ are disjoint cycles then

$$(a_1\, a_2 \cdots a_m)(b_1\, b_2 \cdots b_n) = (b_1\, b_2 \cdots b_n)(a_1\, a_2 \cdots a_m).$$

Proposition 2.28 *Any permutation of a finite set S is the identity permutation, a cycle, or a composition of two or more disjoint cycles.*

Proof We prove the result by induction on the number of elements in the set S. The result is trivially true if S has only one element, since in this case the only permutation of S is the identity permutation. Suppose that the result is known to be true for all permutations of sets with fewer than k elements. We show that the result then holds for all permutations of sets with k elements.

Let S be a set with k elements and let p be a permutation of S. Choose an element a_1 of S, and let elements $a_2, a_3, a_4, \ldots$ of S be defined by the requirement that $p(a_i) = a_{i+1}$ for all positive integers i. Let n be the largest positive integer for which the elements $a_1, a_2, \ldots, a_n$ of S are distinct. We claim that $p(a_n) = a_1$.

Now the choice of n ensures that the elements $a_1, a_2, \ldots, a_n, a_{n+1}$ are not distinct. Therefore $a_{n+1} = a_j$ for some positive integer j between 1 and n. If j were greater than one then we would have $a_j = p(a_{j-1})$ and $a_j = p(a_n)$, which is impossible since if p is a permutation of S then exactly one element

of S must be sent to a_j by p. Therefore $j = 1$, and thus $p(a_n) = a_1$. Let $\sigma_1 = (a_1\, a_2\, \cdots\, a_n)$.

Let T be the set $S \setminus \{a_1, a_2, \ldots, a_n\}$ consisting of all elements of S other than $a_1, a_2, \ldots, a_n$. Now $a_1 = p(a_n)$, and $a_i = p(a_{i-1})$ for $i = 2, 3, \ldots, n$. Thus if $x \in T$ then $p(x) \neq a_i$ for $i = 1, 2, \ldots, n$ (since the function $p\colon S \to S$ is injective), and therefore $p(x) \in T$. We can therefore define a function $q\colon T \to T$, where $q(x) = p(x)$ for all $x \in T$. This function has a well-defined inverse $q^{-1}\colon T \to T$ where $q^{-1}(x) = p^{-1}(x)$ for all $x \in T$. It follows that $q\colon T \to T$ is a permutation of T. The induction hypothesis ensures that this permutation is the identity permutation of T, or is a cycle, or can be expressed as a composition of two or more disjoint cyles. These cycles extend to permutations of S that fix the elements $a_1, a_2, \ldots, a_n$, and these permutations of S are also cycles. It follows that either $p = \sigma_1$ (and q is the identity permutation of T), or else $p = \sigma_1\sigma_2 \ldots \sigma_m$, where $\sigma_2, \sigma_3, \ldots, \sigma_m$ are disjoint cycles of S that fix $a_1, a_2, \ldots, a_n$ and correspond to cycles of T. Thus if the result holds for permutations of sets with fewer than k elements, then it holds for permutations of sets with k elements. It follows by induction on k that the result holds for permutations of finite sets. ∎

Recall that a *transposition* is a permutation $(a\, b)$ of a set S that interchanges two elements a and b of S and fixes the remaining elements.

Lemma 2.29 *Every permutation of a finite set with more than one element can be expressed as a finite composition of transpositions.*

Proof Each cycle can be expressed as a composition of transpositions. Indeed if $a_1, a_2, \ldots, a_n$ are distinct elements of a finite set S then

$$(a_1\, a_2\, \cdots\, a_n) = (a_1\, a_2)(a_2\, a_3) \cdots (a_{n-1}\, a_n).$$

It follows from Proposition 2.28 that a permutation of S that is not the identity permutation can be expressed as a finite composition of transpositions. Moreover the identity permutation of S can be expressed as the composition of any transposition with itself, provided that S has more than one element. The result follows. ∎

Theorem 2.30 *A permutation of a finite set cannot be expressed in one way as a composition of an odd number of transpositions and in another way as a composition of an even number of transpositions.*

Proof We can identify the finite set with the set $\{1, 2, \ldots, n\}$, where n is the number of elements in the finite set. Let $F\colon \mathbb{Z}^n \to \mathbb{Z}$ be the function sending

each n-tuple $(m_1, m_2, \ldots, m_n)$ of integers to the product $\prod_{1 \leq j < k \leq n} (m_k - m_j)$ of the quantities $m_k - m_j$ for all pairs (j, k) of integers satisfying $1 \leq j < k \leq n$. Note that $F(m_1, m_2, \ldots, m_n) \neq 0$ whenever the integers $m_1, m_2, \ldots, m_n$ are distinct. If we transpose two of the integers $m_1, m_2, \ldots, m_n$ then this changes the sign of the function F, since the number of factors of the product $\prod_{1 \leq j < k \leq n} (m_k - m_j)$ that change sign is odd. (Indeed if we transpose m_s and m_t, where $1 \leq s < t < n$ then the factor $m_t - m_s$ changes sign, the factor $m_t - m_i$ becomes $-(m_i - m_s)$ and the factor $m_i - m_s$ becomes $-(m_t - m_i)$ for each integer i for which $s < i < t$.) But any permutation σ of the set $\{1, 2, \ldots, n\}$ is a composition of transpositions. It follows that to each permutation σ of $\{1, 2, \ldots, n\}$ there corresponds a number ϵ_σ, where $\epsilon_\sigma = +1$ or -1, such that $F(m_{\sigma(1)}, m_{\sigma(2)}, \ldots, m_{\sigma(n)}) = \epsilon_\sigma F(m_1, m_2, \ldots, m_n)$ for all integers $m_1, m_2, \ldots, m_n$. Moreover $\epsilon_{\sigma\tau} = \epsilon_\sigma \epsilon_\tau$ for all permutations σ and τ of the set $\{1, 2, \ldots, n\}$. Also $\epsilon_\tau = -1$ if the permutation τ is a transposition. It follows that if σ is expressible as a composition of r transpositions then $\epsilon_\sigma = (-1)^r$. If σ is also expressible as a composition of s transpositions then $\epsilon_\sigma = (-1)^s$, and hence $(-1)^r = (-1)^s$. But then $r - s$ must be divisible by 2. The result follows. ∎

A permutation of a finite set is said to be *even* if it is expressible as the composition of an even number of transpositions. A permutation of a finite set is said to be *odd* if it is expressible as the composition of an odd number of transpositions.

Any permutation of a finite set is expressible as a composition of transpositions (Lemma 2.29) and must therefore be either even or odd. However Theorem 2.30 ensures that a permutation of a finite set cannot be both even and odd.

Lemma 2.31 *An n-cycle is even if n is odd, and is odd if n is even.*

Proof An n-cycle $(a_1, a_2, \ldots, a_n)$ is expressible as a composition of $n - 1$ transpositions, since

$$(a_1\, a_2\, \cdots\, a_n) = (a_1\, a_2)(a_2\, a_3) \cdots (a_{n-1}\, a_n).$$

Thus an n-cycle is even if $n - 1$ is even, and is odd if $n - 1$ is odd. ∎

Example Let us classify the permutations of a set $\{a, b, c, d\}$ of 4 elements into even and odd permutations. The identity permutation is even. The six transpositions are all odd. The eight 3-cycles are all even. The six 4-cycles are all odd. The three remaining permutations $(a\, b)(c\, d)$, $(a\, c)(b\, d)$ and $(a\, d)(b\, c)$ are all even. Note that there are 12 even permutations and 12 odd permutations of a set with 4 elements.

2.15 The Alternating Groups

A permutation of a finite set X is said to be *even* if it is the product of an even number of transpositions; it is said to be *odd* if it is the product of an odd number of transpositions. Note that the inverse of an even permutation and all products of even permutations are themselves even permutations.

Definition For each integer n satisfying $n > 1$, the *alternating group* A_n is the subgroup of the symmetric group Σ_n consisting of all even permutations of the set $\{1, 2, \ldots, n\}$.

Note that, for each integer n satisfying $n > 1$, the alternating group A_n is a normal subgroup of Σ_n of index 2.

Example The alternating group A_3 consists of the identity permutation and the cycles $(1\,2\,3)$ and $(1\,3\,2)$, and is thus isomorphic to the cyclic group C_3 of order 3.

Lemma 2.32 *Every even permutation of a finite set with at least three elements can be expressed as a product of cycles of order 3.*

Proof Let X be a finite set. Then $(a\,b)(b\,c) = (a\,b\,c)$ and $(a\,b)(c\,d) = (c\,a\,d)(a\,b\,c)$ for all distinct elements a, b, c and d of X. Therefore the product of any two transpositions can be expressed as a product of cycles of order 3. The result thus follows from the fact that an even permutation is the product of an even number of transpositions. ∎

Lemma 2.33 *All cycles of order k in the alternating group A_n are conjugate to one another, provided that $k \leq n - 2$.*

Proof Let $(m_1\,m_2\,\cdots\,m_k)$ be a cycle of order k in A_n. Then there exists a permutation ρ of $\{1, 2, \ldots, n\}$ with the property that $\rho(i) = m_i$ for $i = 1, 2, \ldots, k$. If $k \leq n - 2$ then any odd permutation with this property can be composed with the transposition that interchanges $n - 1$ and n to obtain an even permutation ρ with the required property. Then $(m_1\,m_2\,\cdots\,m_k) = \rho(1\,2\,\cdots\,k)\rho^{-1}$. Thus if $k \leq n-2$ then all cycles of order k in A_n are conjugate to $(1\,2\,\cdots\,k)$ and are therefore conjugate to one another, as required. ∎

Example We find all normal subgroups of the alternating group A_4. Let

$$V_4 = \{\iota,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\},$$

where ι is the identity permutation. If ρ is an even permutation sending i to m_i for $i = 1, 2, 3, 4$ then $\rho(1\,2)(3\,4)\rho^{-1} = (m_1\,m_2)(m_3\,m_4)$. Therefore the

permutations $(1\,2)(3\,4)$, $(1\,3)(2\,4)$ and $(1\,4)(2\,3)$ are conjugate to one another, and hence V_4 is a normal subgroup of A_4 of order 4. The group V_4 is referred to as the *Kleinsche Viergruppe*. It is isomorphic to the direct product $C_2 \times C_2$ of two cyclic groups of order 2.

Let N be a normal subgroup of A_4 that contains a cycle $(m_1\, m_2\, m_3)$ of order 3. Now $\rho(m_1\, m_2\, m_3)\rho^{-1} = (\rho(m_1)\, \rho(m_2)\, \rho(m_3))$ for all $\rho \in A_4$. Therefore any cycle in A_4 of order 3 is conjugate to either $(m_1\, m_2\, m_3)$ or to $(m_1\, m_3\, m_2)$. But $(m_1\, m_3\, m_2) \in N$, since $(m_1\, m_3\, m_2) = (m_1\, m_2\, m_3)^2$. Therefore every cycle of order 3 in A_4 belongs to the normal subgroup N. But then $N = A_4$, since A_4 is generated by cycles of order 3 (Lemma 2.32). We have thus shown that if a normal subgroup N of A_4 contains a cycle of order 3 then $N = A_4$.

Now let N be a normal subgroup of A_4 that does not contain any cycle of order 3. Then $N \subset V_4$, since all elements of $A_4 \setminus V_4$ are cycles of order 3. But the only normal subgroups of A_4 that are contained in V_4 are $\{\iota\}$ and V_4 itself, since the three elements of $V_4 \setminus \{\iota\}$ are conjugate to one another.

We conclude that the normal subgroups of A_4 are the trivial group $\{\iota\}$, the Kleinsche Viergruppe V_4 and A_4 itself.

We recall that a non-trivial group G is *simple* if and only if the only normal subgroups of G are G itself and the trivial subgroup whose only element is the identity element of G. The alternating group A_4 is not simple. We shall prove that A_n is simple when $n \geq 5$.

Lemma 2.34 *Let N be a non-trivial normal subgroup of the alternating group A_n, where $n \geq 5$. Then there exists $\sigma \in N$, where σ is not the identity permutation, and $a \in \{1, 2, \ldots, n\}$ such that $\sigma(a) = a$.*

Proof Let $X = \{1, 2, \ldots, n\}$. The proof divides into two cases, depending on whether or not the normal subgroup N contains a permutation ρ of X with the property that ρ^2 is not the identity permutation.

Suppose that the normal subgroup N contains a permutation ρ of X with the property that ρ^2 is not the identity permutation. Then there exists $a \in X$ such that $\rho(\rho(a)) \neq a$. Let $b = \rho(a)$ and $c = \rho(b)$. Then the elements a, b and c are distinct. Choose elements d and e of X such that a, b, c, d and e are distinct. (This is possible since the set X has n elements, where $n \geq 5$.) Let $\rho' = (c\, d\, e)\rho(c\, d\, e)^{-1}$. Then $\rho' \in N$ (since $\rho \in N$ and N is a normal subgroup), $\rho'(a) = b$ and $\rho'(b) = d$. Now $\rho' \neq \rho$, since $\rho'(b) \neq \rho(b)$. Thus if $\sigma = \rho^{-1}\rho'$ then $\sigma \in N$, $\sigma(a) = a$, and σ is not the identity permutation.

It remains to prove the result in the case where ρ^2 is the identity permutation for all $\rho \in N$. In this case choose $\rho \in N$, where ρ is not the identity

permutation, let a be an element of X for which $\rho(a) \neq a$, and let $b = \rho(a)$. The permutation ρ is even (since it belongs to the alternating group A_n), and therefore ρ cannot be the transposition $(a\,b)$. It follows that there exists an element c, distinct from a and b, such that $\rho(c) \neq c$. Let $d = \rho(c)$. Then the elements a, b, c and d of X are distinct. Choose an element e of X which is distinct from a, b, c and d. (This is possible since the set X has n elements, where $n \geq 5$.) Let $\rho' = (c\,d\,e)\rho(c\,d\,e)^{-1}$. Then $\rho'(a) = b$ and $\rho'(d) = e$. Now $\rho' \neq \rho$, since $\rho'(d) \neq \rho(d)$. Thus if $\sigma = \rho^{-1}\rho'$ then $\sigma \in N$, $\sigma(a) = a$, and σ is not the identity permutation. ∎

Lemma 2.35 *Let N be a normal subgroup of A_n, where $n \geq 5$. If N contains a 3-cycle then $N = A_n$.*

Proof Suppose that N contains a 3-cycle. Then N contains every 3-cycle of A_n, since all 3-cycles in A_n are conjugate (Lemma 2.33). But then N contains every even permutation, since every even permutation is the identity permutation, a 3-cycle or a finite product of 3-cycles (Lemma 2.32). Thus $N = A_n$. ∎

Theorem 2.36 *The alternating group A_n is simple when $n \geq 5$.*

Proof First we prove that A_5 is simple. Let N be a non-trivial normal subgroup of A_5. We shall show that $N \cap H$ is non-trivial, where $H = \{\rho \in A_5 : \rho(5) = 5\}$. Then H is a subgroup of A_5 that is isomorphic to A_4.

It follows from Lemma 2.34 that there exists $\sigma \in N$, where σ is not the identity permutation, and $a \in \{1, 2, 3, 4, 5\}$ such that $\sigma(a) = a$. Choose $\rho \in A_5$ such that $\rho(a) = 5$, and let $\sigma' = \rho\sigma\rho^{-1}$. Then $\sigma' \in N$ and $\sigma'(5) = 5$, and therefore $\sigma' \in H \cap N$. But σ' is not the identity permutation. Thus $H \cap N$ is a non-trivial normal subgroup of H. But the subgroup H of A_5 is isomorphic to A_4 (since each permutation of $\{1, 2, 3, 4\}$ can be regarded as a permutation of $\{1, 2, 3, 4, 5\}$ that fixes 5). It follows from this that $H \cap N$ must contain the permutations $(1\,2)(3\,4)$, $(1\,3)(2\,4)$ and $(1\,4)(2\,3)$ since the two non-trivial normal subgroups of A_4 each contain these permutations. But then the normal subgroup N of A_5 contains also the permutation $(1\,2)(4\,5)$, since $(1\,2)(4\,5) = (3\,4\,5)(1\,2)(3\,4)(3\,4\,5)^{-1}$. It follows that N contains the cycle $(3\,4\,5)$, since $(3\,4\,5) = (1\,2)(3\,4)(1\,2)(4\,5)$. It follows from Lemma 2.35 that $N = A_5$. Thus the group A_5 is simple.

We now prove that A_n is simple for $n > 5$ by induction on n. Thus suppose that $n > 5$ and the group A_{n-1} is simple. Let N be a non-trivial normal subgroup of A_n, and let $H = \{\rho \in A_n : \rho(n) = n\}$. It follows from Lemma 2.34 that there exists $\sigma \in N$, where σ is not the identity permutation,

and $a \in \{1, 2, \ldots, n\}$ such that $\sigma(a) = a$. Choose $\rho \in A_n$ such that $\rho(a) = n$, and let $\sigma' = \rho\sigma\rho^{-1}$. Then $\sigma' \in N$ and $\sigma'(n) = n$, and therefore $\sigma' \in H \cap N$. But σ' is not the identity permutation. Thus $H \cap N$ is a non-trivial normal subgroup of H. But the subgroup H of A_n is simple, since it is isomorphic to A_{n-1}. It follows that $N \cap H = H$, and thus $H \subset N$. But then N contains a 3-cycle, and therefore $N = A_n$ (Lemma 2.35). Thus the group A_n is simple. We conclude by induction on n that the group A_n is simple whenever $n \geq 5$, as required. ∎

2.16 Normal Subgroups of the Symmetric Groups

We can now find all normal subgroups of the symmetric groups Σ_n. If N is a normal subgroup of Σ_n then $N \cap A_n$ is a normal subgroup of A_n. Moreover it follows from the First Isomorphism Theorem (Theorem 2.23) that $N/(N \cap A_n) \cong NA_n/A_n$. But NA_n/A_n is a subgroup of Σ_n/A_n, and $|\Sigma_n/A_n| = 2$. Therefore either $N \subset A_n$ or else $N \cap A_n$ is a subgroup of N of index 2.

Example We show that if $n \geq 5$ then the only normal subgroups of Σ_n are the trivial subgroup, the alternating group A_n and Σ_n itself. Now these subgroups are all normal subgroups of Σ_n. Moreover the trivial subgroup and A_n are the only normal subgroups of Σ_n contained in A_n, since A_n is simple when $n \geq 5$ (Theorem 2.36).

Let N be a normal subgroup of Σ_n that is not contained in A_n. Then $N \cap A_n$ is a normal subgroup of A_n. Now if $N \cap A_n$ were the trivial subgroup then N would be a subgroup of Σ_n of order 2. But one can readily verify that Σ_n contains no normal subgroup of order 2 unless $n = 2$, in which case A_2 is itself the trivial group. It follows that $N \cap A_n = A_n$, and hence $N = \Sigma_n$. We have therefore shown that if $n \geq 5$ then the only normal subgroups of Σ_n are the trivial subgroup, the alternating group A_n and Σ_n itself.

Example We now show that the only normal subgroups of the symmetric group Σ_4 are the trivial subgroup, the Kleinsche Viergruppe V_4, the alternating group A_4 and Σ_4 itself.

The trivial group and the groups V_4 and A_4 are normal subgroups of Σ_4. Moreover they are the only normal subgroups of Σ_4 contained in A_4, since they are the only normal subgroups of A_4.

Let N be a normal subgroup of Σ_4 that is not contained in A_4. Then $N \cap A_4$ is a normal subgroup of A_4. One can readily verify that Σ_4 contains no normal subgroup of order 2. It follows that $V_4 \subset N$, since only normal subgroups of A_4 other than the trivial subgroup are the groups V_4 and A_4. Now the only odd permutations in Σ_4 are transpositions and cycles of order 4.

Moreover if N contains a cycle of order 4 then N contains a transposition, since $V_4 \subset N$ and

$$(m_1\, m_2)(m_3\, m_4)(m_1\, m_2\, m_3\, m_4) = (m_2\, m_4)$$

for all cycles $(m_1\, m_2\, m_3\, m_4)$ of order 4. It follows that if N is a normal subgroup of Σ_4 that is not contained in A_4 then N must contain at least one transposition. But then N contains all transpositions, and therefore $N = \Sigma_4$. This shows that the only normal subgroups of Σ_4 are the trivial group, the Kleinsche Viergruppe V_4, the alternating group A_4 and Σ_4 itself.

2.17 Finitely Generated Abelian Groups

Let H be a subgroup of the additive group $\mathbb{Z}^n$ consisting of all n-tuples of integers, with the operation of (vector) addition. A list $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_r$ of elements of $\mathbb{Z}^n$ is said to constitute an *integral basis* (or $\mathbb{Z}$*-basis*) of H if the following conditions are satisfied:

- the element $m_1\mathbf{b}_1 + m_2\mathbf{b}_2 + \cdots + m_r\mathbf{b}_r$ belongs to H for all integers $m_1, m_2, \ldots, m_r$;
- given any element $\mathbf{h}$ of H, there exist uniquely determined integers $m_1, m_2, \ldots, m_r$ such that $\mathbf{h} = m_1\mathbf{b}_1 + m_2\mathbf{b}_2 + \cdots + m_r\mathbf{b}_r$.

Note that elements $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ of $\mathbb{Z}^n$ constitute an integral basis of $\mathbb{Z}^n$ if and only if every element of $\mathbb{Z}^n$ is uniquely expressible as a linear combination of $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ with integer coefficients. It follows from basic linear algebra that the rows of an $n \times n$ matrix of integers constitute an integral basis of $\mathbb{Z}^n$ if and only if the determinant of that matrix is ± 1.

Theorem 2.37 *Let H be a non-trivial subgroup of $\mathbb{Z}^n$. Then there exists an integral basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ of $\mathbb{Z}^n$, a positive integer s, where $s \leq n$, and positive integers $k_1, k_2, \ldots, k_s$ for which $k_1\mathbf{b}_1, k_2\mathbf{b}_2, \ldots, k_s\mathbf{b}_s$ is an integral basis of H.*

Proof We prove the result by induction on n. The result is clearly true when $n = 1$, since every non-trivial subgroup of $\mathbb{Z}$ is of the form $k\mathbb{Z}$ for some positive integer k. Suppose therefore that $n > 1$ and that the result holds for all subgroups of $\mathbb{Z}^{n-1}$. We must show that the result then holds for all subgroups H of $\mathbb{Z}^n$.

Let k_1 be the smallest strictly positive integer for which there exists some integral basis $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ of $\mathbb{Z}^n$ and some element of H of the form $m_1\mathbf{u}_1 + m_2\mathbf{u}_2 + \cdots + m_n\mathbf{u}_n$ where $m_1, m_2, \ldots, m_n$ are integers and $m_i = k_1$ for some

integer i satisfying $1 \leq i \leq n$. Let $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ be such a basis, with $i = 1$, and let $\mathbf{h}_0$ be an element of H for which $\mathbf{h}_0 = m_1\mathbf{u}_1 + m_2\mathbf{u}_2 + \cdots + m_n\mathbf{u}_n$, where $m_1, m_2, \ldots, m_n$ are integers and $m_1 = k_1$.

We show that each coefficient m_i is divisible by k_1. Now, for each i, there exist integers q_i and r_i such that $m_i = q_i k_1 + r_i$ and $0 \leq r_i < k_1$. Let $\mathbf{b}_1 = \mathbf{u}_1 + \sum_{i=2}^{n} q_i \mathbf{u}_i$. Then $\mathbf{b}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ is an integral basis of $\mathbb{Z}^n$ and

$$\mathbf{h}_0 = k_1\mathbf{b}_1 + \sum_{i=2}^{n} r_i \mathbf{u}_i.$$

The choice of k_1 now ensures that the coefficients r_i cannot be strictly positive (as they are less than k_1), and therefore $r_i = 0$ and $m_i = q_i k_1$ for $i = 2, 3, \ldots, n$. Moreover $\mathbf{h}_0 = k_1\mathbf{b}_1$.

Now let $\varphi\colon \mathbb{Z}^{n-1} \to \mathbb{Z}^n$ be the injective homomorphism sending each element $(m_2, m_3, \ldots, m_n)$ of $\mathbb{Z}^{n-1}$ to $\sum_{i=2}^{n} m_i \mathbf{u}_i$, and let $\tilde{H} = \varphi^{-1}(H)$. Then, given any element $\mathbf{h}$ of H, there exist an integer m and an element $\tilde{\mathbf{h}}$ of $\mathbb{Z}^{n-1}$ such that $\mathbf{h} = m\mathbf{b}_1 + \varphi(\tilde{\mathbf{h}})$. Moreover m and $\tilde{\mathbf{h}}$ are uniquely determined by $\mathbf{h}$, since $\mathbf{b}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ is an integral basis of $\mathbb{Z}^n$. Let $m = qk_1 + r$, where q and r are integers and $0 \leq r < k_1$. Then $\mathbf{h} - q\mathbf{h}_0 = r\mathbf{b}_1 + \varphi(\tilde{\mathbf{h}})$, where $\varphi(\tilde{\mathbf{h}})$ is expressible as a linear combination of $\mathbf{u}_2, \ldots, \mathbf{u}_n$ with integer coefficients. The choice of k_1 now ensures that r cannot be strictly positive, and therefore $r = 0$. Then $\varphi(\tilde{\mathbf{h}}) \in H$, and hence $\tilde{\mathbf{h}} \in \tilde{H}$. We conclude from this that, given any element $\mathbf{h}$ of H, there exist an integer q and an element $\tilde{\mathbf{h}}$ of $\tilde{H}$ such that $\mathbf{h} = qk_1\mathbf{b}_1 + \varphi(\tilde{\mathbf{h}})$. Moreover q and $\tilde{\mathbf{h}}$ are uniquely determined by $\mathbf{h}$.

Now the induction hypothesis ensures the existence of an integral basis $\tilde{\mathbf{b}}_2, \tilde{\mathbf{b}}_3, \ldots, \tilde{\mathbf{b}}_n$ of $\mathbb{Z}^{n-1}$ for which there exist positive integers $k_2, k_3, \ldots, k_s$ such that $k_2\tilde{\mathbf{b}}_2, k_3\tilde{\mathbf{b}}_3, \ldots, k_s\tilde{\mathbf{b}}_s$ is an integral basis of $\tilde{H}$. Let $\mathbf{b}_i = \varphi(\tilde{\mathbf{b}}_i)$ for each integer i between 2 and n. One can then readily verify that $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ is an integral basis of $\mathbb{Z}^n$ and $k_1\mathbf{b}_1, k_2\mathbf{b}_2, \ldots, k_s\mathbf{b}_s$ is an integral basis of H, as required. ∎

An Abelian group G is generated by elements $g_1, g_2, \ldots, g_n$ if and only if every element of G is expressible in the form $g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}$ for some integers $m_1, m_2, \ldots, m_n$.

Lemma 2.38 *A non-trivial Abelian group G is finitely generated if and only if there exists a positive integer n and some surjective homomorphism $\theta\colon \mathbb{Z}^n \to G$.*

Proof Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ be the integral basis of $\mathbb{Z}^n$ with $\mathbf{e}_1 = (1, 0, \ldots, 0)$, $\mathbf{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \mathbf{e}_n = (0, \ldots, 0, 1)$. If there exists a surjective homomorphism $\theta\colon \mathbb{Z}^n \to G$ then G is generated by $g_1, g_2, \ldots, g_n$, where $g_i = \theta(\mathbf{e}_i)$

for $i = 1, 2, \ldots, n$. Conversely if G is generated by $g_1, g_2, \ldots, g_n$ then there is a surjective homomorphism $\theta: \mathbb{Z}^n \to G$ that sends $(m_1, m_2, \ldots, m_n) \in \mathbb{Z}^n$ to $g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}$. ∎

Theorem 2.39 *Let G be a non-trivial finitely generated Abelian group. Then there exist a positive integer n and a non-negative integer s between 0 and n, such that if $s = 0$ then $G \cong \mathbb{Z}^n$, and if $s > 0$ then there exist positive integers $k_1, k_2, \ldots, k_s$ such that*

$$G \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \times \mathbb{Z}^{n-s},$$

where C_{k_i} is a cyclic group of order k_i for $i = 1, 2, \ldots, s$.

Proof There exists a positive integer n and some surjective homomorphism $\theta: \mathbb{Z}^n \to G$, since G is finitely-generated. Let H be the kernel of θ. If H is trivial then the homomorphism θ is an isomorphism between $\mathbb{Z}^n$ and G. If H is non-trivial then G is isomorphic to $\mathbb{Z}^n/H$, and there exists an integral basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ of $\mathbb{Z}^n$, a positive integer s, where $s \leq n$, and positive integers $k_1, k_2, \ldots, k_s$ for which $k_1\mathbf{b}_1, k_2\mathbf{b}_2, \ldots, k_s\mathbf{b}_s$ is an integral basis of H (Theorem 2.37). Then the group $\mathbb{Z}^n/H$, and thus G, is isomorphic to $C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \times \mathbb{Z}^{n-s}$, where C_i is a cyclic group of order k_i for $i = 1, 2, \ldots, s$. Indeed there is a well-defined homomorphism $\varphi: \mathbb{Z}^n \to C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \times \mathbb{Z}^{n-s}$ which sends each element

$$m_1\mathbf{b}_1 + m_2\mathbf{b}_2 + \cdots + m_n\mathbf{b}_n$$

of $\mathbb{Z}^n$ to $(a_1^{m_1}, a_2^{m_2}, \ldots, a_s^{m_s}, m_{s+1}, \ldots, m_n)$, where a_i is a generator of the cyclic group C_i for $i = 1, 2, \ldots, s$. The homomorphism φ is surjective, and its kernel is the subgroup H. Therefore $G \cong \mathbb{Z}^n/H \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_s} \times \mathbb{Z}^{n-s}$, as required. ∎

Corollary 2.40 *Let G be a non-trivial finite Abelian group. Then there exist positive integers $k_1, k_2, \ldots, k_n$ such that $G \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_n}$, where C_{k_i} is a cyclic group of order k_i for $i = 1, 2, \ldots, n$.*

With some more work it is possible to show that the positive integers $k_1, k_2, \ldots, k_s$ in Theorem 2.39 may be chosen such that $k_1 > 1$ and k_{i-1} divides k_i for $i = 2, 3, \ldots, s$, and that the Abelian group is then determined up to isomorphism by the integer n and the sequence of positive integers $k_1, k_2, \ldots, k_s$.

2.18 The Class Equation of a Finite Group

Definition The *centre* $Z(G)$ of a group G is the subgroup of G defined by

$$Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}.$$

One can verify that the centre of a group G is a normal subgroup of G.

Let G be a finite group, and let $Z(G)$ be the centre of G. Then $G \setminus Z(G)$ is a disjoint union of conjugacy classes. Let r be the number of conjugacy classes contained in $G \setminus Z(G)$, and let $n_1, n_2, \ldots, n_r$ be the number of elements in these conjugacy classes. Then $n_i > 1$ for all i, since the centre $Z(G)$ of G is the subgroup of G consisting of those elements of G whose conjugacy class contains just one element. Now the group G is the disjoint union of its conjugacy classes, and therefore

$$|G| = |Z(G)| + n_1 + n_2 + \cdots + n_r.$$

This equation is referred to as the *class equation* of the group G.

Definition Let g be an element of a group G. The *centralizer* $C(g)$ of g is the subgroup of G defined by $C(g) = \{h \in G : hg = gh\}$.

Proposition 2.41 *Let G be a finite group, and let p be a prime number. Suppose that p^k divides the order of G for some positive integer k. Then either p^k divides the order of some proper subgroup of G, or else p divides the order of the centre of G.*

Proof Choose elements $g_1, g_2, \ldots, g_r$ of $G \setminus Z(G)$, where $Z(G)$ is the centre of G, such that each conjugacy class included in $G \setminus Z(G)$ contains exactly one of these elements. Let n_i be the number of elements in the conjugacy class of g_i and let $C(g_i)$ be the centralizer of g_i for each i. Then $C(g_i)$ is a proper subgroup of G, and $|G| = n_i|C(g_i)|$. Thus if p^k divides $|G|$ but does not divide the order of any proper subgroup of G then p must divide n_i for $i = 1, 2, \ldots, r$. Examination of the class equation $|G| = |Z(G)| + n_1 + n_2 + \cdots + n_r$ now shows that p divides $|Z(G)|$, as required. ∎

2.19 Cauchy's Theorem

Theorem 2.42 (Cauchy) *Let G be an finite group, and let p be a prime number that divides the order of G. Then G contains an element of order p.*

Proof We prove the result by induction on the order of G. Thus suppose that every finite group whose order is divisible by p and less than $|G|$ contains an element of order p. If p divides the order of some proper subgroup of G then that subgroup contains the required element of order p. If p does not divide the order of any proper subgroup of G then Proposition 2.41 ensures that p divides the order of the centre $Z(G)$ of G, and thus $Z(G)$ cannot be a proper subgroup of G. But then $G = Z(G)$ and the group G is Abelian.

Thus let G be an Abelian group whose order is divisible by p, and let H be a proper subgroup of G that is not contained in any larger proper subgroup. If $|H|$ is divisible by p then the induction hypothesis ensures that H contains the required element of order p, since $|H| < |G|$. Suppose then that $|H|$ is not divisible by p. Choose $g \in G \setminus H$, and let C be the cyclic subgroup of G generated by g. Then $HC = G$, since $HC \neq H$ and HC is a subgroup of G containing H. It follows from the First Isomorphism Theorem (Theorem 2.23) that $G/H \cong C/H \cap C$. Now p divides $|G/H|$, since $|G/H| = |G|/|H|$ and p divides $|G|$ but not $|H|$. Therefore p divides $|C|$. Thus if $m = |C|/p$ then g^m is the required element of order p. This completes the proof of Cauchy's Theorem. ∎

2.20 The Structure of p-Groups

Definition Let p be a prime number. A *p-group* is a finite group whose order is some power p^k of p.

Lemma 2.43 *Let p be a prime number, and let G be a p-group. Then there exists a normal subgroup of G of order p that is contained in the centre of G.*

Proof Let $|G| = p^k$. Then p^k divides the order of G but does not divide the order of any proper subgroup of G. It follows from Proposition 2.41 that p divides the order of the centre of G. It then follows from Cauchy's Theorem (Theorem 2.42) that the centre of G contains some element of order p. This element generates a cyclic subgroup of order p, and this subgroup is normal since its elements commute with every element of G. ∎

Proposition 2.44 *Let G be a p-group, where p is some prime number, and let H be a proper subgroup of G. Then there exists some subgroup K of G such that $H \triangleleft K$ and K/H is a cyclic group of order p.*

Proof We prove the result by induction on the order of G. Thus suppose that the result holds for all p-groups whose order is less than that of G. Let Z be the centre of G. Then ZH is a well-defined subgroup of G, since Z is a normal subgroup of G.

Suppose that $ZH \neq H$. Then H is a normal subgroup of ZH. The quotient group ZH/H is a p-group, and contains a subgroup K_1 of order p (Lemma 2.43). Let $K = \{g \in ZH : gH \in K_1\}$. Then $H \triangleleft K$ and $K/H \cong K_1$, and therefore K is the required subgroup of G.

Finally suppose that $ZH = H$. Then $Z \subset H$. Let $H_1 = \{hZ : h \in H\}$. Then H_1 is a subgroup of G/Z. But G/Z is a p-group, and $|G/Z| < |G|$, since $|Z| \geq p$ (Lemma 2.43). The induction hypothesis ensures the existence of a subgroup K_1 of G/Z such that $H_1 \triangleleft K_1$ and K_1/H_1 is cyclic of order p. Let $K = \{g \in G : gZ \in K_1\}$. Then $H \triangleleft K$ and $K/H \cong K_1/H_1$. Thus K is the required subgroup of G. ∎

Repeated applications of Proposition 2.44 yield the following result.

Corollary 2.45 *Let G be a finite group whose order is a power of some prime number p. Then there exist subgroups $G_0, G_1, \ldots, G_n$ of G, where G_0 is the trivial subgroup and $G_n = G$, such that $G_{i-1} \triangleleft G_i$ and G_i/G_{i-1} is a cyclic group of order p for $i = 1, 2, \ldots, n$.*

2.21 The Sylow Theorems

Definition Let G be a finite group, and let p be a prime number dividing the order $|G|$ of G. A *p-subgroup* of G is a subgroup whose order is some power of p. A *Sylow p-subgroup* of G is a subgroup whose order is p^k, where k is the largest natural number for which p^k divides $|G|$.

Theorem 2.46 (First Sylow Theorem) *Let G be a finite group, and let p be a prime number dividing the order of G. Then G contains a Sylow p-subgroup.*

Proof We prove the result by induction on the order of G. Thus suppose that all groups whose order is less than that of G contain the required Sylow p-subgroups. Let k be the largest positive integer for which p^k divides $|G|$. If p^k divides the order of some proper subgroup H of G then the induction hypothesis ensures that H contains the required Sylow p-subgroup of order p^k. If p^k does not divide the order of any proper subgroup of G then p divides the order of the centre $Z(G)$ of G (Proposition 2.41). It follows from Cauchy's Theorem (Theorem 2.42) that $Z(G)$ contains an element of order p, and this element generates a normal subgroup N of G of order p. The induction hypothesis then ensures that G/N has a Sylow p-subgroup L of order p^{k-1}, since $|G/N| = |G|/p$. Let $K = \{g \in G : gN \in L\}$. Then $|K| = p|L| = p^k$, and thus K is the required Sylow p-subgroup of G. ∎

Theorem 2.47 (Second Sylow Theorem) *Let G be a finite group, and let p be a prime number dividing the order of G. Then all Sylow p-subgroups of G are conjugate, and any p-subgroup of G is contained in some Sylow p-subgroup of G. Moreover the number of Sylow p-subgroups in G divides the order of $|G|$ and is congruent to 1 modulo p.*

Proof Let K be a Sylow p-subgroup of G, and let X be the set of left cosets of K in G. Let H be a p-subgroup of G. Then H acts on X on the left, where $h(gK) = hgK$ for all $h \in H$ and $g \in G$. Moreover $h(gK) = gK$ if and only if $g^{-1}hg \in K$. Thus an element gK of X is fixed by H if and only if $g^{-1}Hg \subset K$.

Let $|G| = p^k m$, where k and m are positive integers and m is coprime to p. Then $|K| = p^k$. Now the number of left cosets of K in G is $|G|/|K|$. Thus the set X has m elements. Now the number of elements in any orbit for the action of H on X divides the order of H, since it is the index in H of the stabilizer of some element of that orbit (Lemma 2.26). But then the number of elements in each orbit must be some power of p, since H is a p-group. Thus if an element of X is not fixed by H then the number of elements in its orbit is divisible by p. But X is a disjoint union of orbits under the action of H on X. Thus if m' denotes the number of elements of X that are fixed by H then $m - m'$ is divisible by p.

Now m is not divisible by p. It follows that $m' \neq 0$, and m' is not divisible by p. Thus there exists at least one element g of G such that $g^{-1}Hg \subset K$. But then H is contained in the Sylow p-subgroup gKg^{-1}. Thus every p-subgroup is contained in a Sylow p-subgroup of G, and this Sylow p-subgroup is a conjugate of the given Sylow p-subgroup K. In particular any two Sylow p-subgroups are conjugate.

It only remains to show that the number of Sylow p-subgroups in G divides the order of $|G|$ and is congruent to 1 modulo p. On applying the above results with $H = K$, we see that $g^{-1}Kg = K$ for some $g \in G$ if and only if gK is a fixed point for the action of K on X. But the number of elements g of G for which gK is a fixed point is $m'|K|$, where m' is the number of fixed points in X. It follows that the number of elements g of G for which $g^{-1}Kg = K$ is $p^k m'$. But every Sylow p-subgroup of G is of the form $g^{-1}Kg$ for some $g \in G$. It follows that the number n of Sylow p-subgroups in G is given by $n = |G|/p^k m' = m/m'$. In particular n divides $|G|$. Now we have already shown that $m - m'$ is divisible by p. It follows that m' is coprime to p, since m is coprime to p. Also $m - m'$ is divisible by m', since $(m - m')/m' = n - 1$. Putting these results together, we see that $m - m'$ is divisible by $m'p$, and therefore $n - 1$ is divisible by p. Thus n divides $|G|$ and is congruent to 1 modulo p, as required. ∎

2.22 Some Applications of the Sylow Theorems

Theorem 2.48 *Let p and q be prime numbers, where $p < q$ and $q \not\equiv 1 \pmod{p}$. Then any group of order pq is cyclic.*

Proof Let G be a group of order pq. It follows from the First Sylow Theorem that G contains Sylow subgroups N_p and N_q of orders p and q respectively. Now the number n_p of Sylow p-subgroups divides pq and satisfies $n_p \equiv 1 \pmod{p}$, by the Second Sylow Theorem. Clearly n_p cannot be divisible by p, and therefore either $n_p = 1$ or $n_p = q$. But $q \not\equiv 1 \pmod{p}$. It follows that $n_p = 1$. Thus the group G has just one subgroup of order p.

Now, given any element g of G, the subgroups N_p and gN_pg^{-1} are of order p. It follows that $gN_pg^{-1} = N_p$ for all elements g of G. Thus N_p is a normal subgroup of G.

A similar argument shows that N_q is also a normal subgroup of G, since $p < q$, and therefore $p \not\equiv 1 \pmod{q}$.

Now $N_p \cap N_q$ is a subgroup of both N_p and N_q. It follows from Lagrange's Theorem that the order of $N_p \cap N_q$ divides both of the prime numbers p and q, and therefore $|N_p \cap N_q| = 1$ and $N_p \cap N_q = \{e\}$, where e is the identity element of G.

Let $x \in N_p$ and $y \in N_q$. Then $yx^{-1}y^{-1} \in N_p$ and $xyx^{-1} \in N_q$, since N_p and N_q are normal subgroups of G. But then $xyx^{-1}y^{-1} \in N_p \cap N_q$, since $xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) = (xyx^{-1})y^{-1}$, and therefore $xyx^{-1}y^{-1} = e$. Thus $xy = yx$ for all $x \in N_p$ and $y \in N_q$. It follows easily from this that the function $\varphi\colon N_p \times N_q \to G$ which sends $(x, y) \in N_p \times N_q$ to xy is a homomorphism. This homomorphism is injective, for if $xy = e$ for some $x \in N_p$ and $y \in N_q$, then $x = y^{-1}$, and hence $x \in N_p \cap N_q$, from which it follows that $x = e$ and $y = e$. But any injective homomorphism between two finite groups of the same order is necessarily an isomorphism. Therefore the function $\varphi\colon N_p \times N_q \to G$ is an isomorphism, and thus $G \cong N_p \times N_q$.

Now any group whose order is prime number must be cyclic. Therefore the groups N_p and N_q are cyclic. Let x be an element of N_p that generates N_p, and let y be an element of N_q that generates N_q. Then $(x, y)^n = (x^n, y^n)$ for all integers n. It follows from this that the order of (x, y) cannot be equal to 1, p or q, and must therefore be equal to pq. Thus $N_p \times N_q$ is a cyclic group generated by (x, y), and therefore G is a cyclic group, generated by xy, as required. ∎

Example Any finite group whose order is 15, 33, 35, 51, 65, 69, 85, 87, 91 or 95 is cyclic.

Theorem 2.49 *Let G be a group of order $2p$ where p is a prime number greater than 2. Then either the group G is cyclic, or else the group G is isomorphic to the dihedral group D_{2p} of symmetries of a regular p-sided polygon in the plane.*

Proof It follows from the First Sylow Theorem, or from Cauchy's Theorem, that the group G contains elements x and y whose orders are 2 and p respectively. The subgroup N generated by y is then a Sylow p-subgroup of G. Now it follows from the Second Sylow Theorem that the number of Sylow p-subgroups of G divides $2p$ and is congruent to 1 modulo p. There can therefore be only one such Sylow p-subgroup, since 2, p and $2p$ are not congruent to 1 modulo p. Now if g is any element of G then gNg^{-1} is a Sylow p-subgroup of G, and therefore $gNg^{-1} = N$. We deduce that N is a normal subgroup of G, of order p.

Now consider the element xyx^{-1} of G. This must be an element of the normal subgroup N of G generated by y. Therefore $xyx^{-1} = y^k$ for some integer k. Moreover k is not divisible by p, since xyx^{-1} is not the identity element e of G. Then

$$y^{k^2} = (y^k)^k = (xyx^{-1})^k = xy^kx^{-1} = x(xyx^{-1})x^{-1} = x^2yx^{-2}.$$

But $x^2 = x^{-2} = e$, since x is an element of G of order 2. It follows that $y^{k^2} = y$, and thus $y^{k^2-1} = e$. But then p divides $k^2 - 1$, since y is an element of order p. Moreover $k^2 - 1 = (k-1)(k+1)$. It follows that either p divides $k-1$, in which case $xyx^{-1} = y$, or else p divides $k+1$, in which case $xyx^{-1} = y^{-1}$.

In the case when $xyx^{-1} = y$ we see that $xy = yx$, and one can then readily verify that the group G is a cyclic group of order $2p$ generated by xy.

In the case when $xyx^{-1} = y^{-1}$ the group G is isomorphic to the dihedral group D_{2p} of order $2p$. In this case the elements x and y generate G (since they generate a subgroup of G whose order divides $2p$ but is greater than p, and must therefore be equal to $2p$). Under the isomorphism with the dihedral group D_{2p} the element x corresponds to a reflection in one of the axes of symmetry of the regular p-sided polygon, and the element y corresponds to a rotation of that polygon about its centre through an angle of $2\pi/p$ radians. ∎

Theorem 2.50 *Let p and q be prime numbers with $p < q$, and let d be the smallest positive integer for which $p^d \equiv 1 \pmod{q}$. If G is a group of order $p^k q$, where $0 < k < d$ then G contains a normal subgroup of order q. If G is a group of order $p^d q$ then either G contains a normal subgroup of order q or else G contains a normal subgroup of order p^d.*

Proof It follows from the First Sylow Theorem (or directly from Cauchy's Theorem) that the group G contains at least one Sylow q-subgroup K, and this is of order q. If $|G| = p^k q$ then the number n_q of such Sylow q-subgroups divides $p^k q$ and satisfies $n_q \equiv 1 \pmod{q}$, by the Second Sylow Theorem. It follows that n_q is coprime to q, and therefore $n_q = p^j$ for some integer j satisfying $0 \leq j \leq k$.

If $k < d$ then none of the integers $p, p^2, \ldots, p^k$ are congruent to 1 modulo q, and therefore $j = 0$ and $n_q = 1$. In this case there is just one Sylow q-subgroup K, and this is a normal subgroup. (Given any element g of G, the subgroup gKg^{-1} is a Sylow q-subgroup, and therefore $gKg^{-1} = K$.)

If $k = d$ then none of the integers p^j with $0 < j < d$ are congruent to 1 modulo q, and therefore either $n_q = 1$ or $n_q = p^d$. If $n_q = 1$ then there is just one Sylow q-subgroup K, and this is a normal subgroup.

If $n_q > 1$ then $n_q = p^d$, and thus there are p^d Sylow q-subgroups, and these are of order q. Now if K_i and K_j are two distinct subgroups of order q then $K_i \cap K_j$ is a proper subgroup of both K_i and K_j, and its order is a proper divisor of the order q of K_i and K_j, by Lagrange's Theorem. But q is a prime number. It follows that $K_i \cap K_j = \{e\}$, where e is the identity element of G. We deduce from this that no element of G of order q can belong to more than one subgroup of order q. But each subgroup of G of order q contains $q-1$ elements of order q (namely all elements of that subgroup with the exception of the identity element). It follows that the group G contains $p^d(q-1)$ elements of order q. Now $|G| = p^d q$. It follows that G contains exactly p^d elements that are not of order q. But it follows from the First Sylow Theorem that G contains at least one Sylow p-subgroup H, and this is of order p^d. This subgroup must therefore contain all the elements of G that are not of order q. It follows that the group G cannot contain more than one such Sylow p-subgroup. This Sylow p-subgroup H is therefore a normal subgroup of G of order p^d, as required. ∎

2.23 Simple Groups

Definition A non-trivial group G is said to be *simple* if the only normal subgroups of G are the whole of G and the trivial subgroup $\{e\}$ whose only element is the identity element e of G.

Lemma 2.51 *Any non-trivial Abelian simple group is a cyclic group whose order is a prime number.*

Proof Let G be a non-trivial Abelian simple group, and let x be an element of G that is not equal to the identity element e of G. All subgroups of an

Abelian group are normal subgroups. Therefore the subgroup of G generated by x is a normal subgroup of G, and must therefore be the whole of G. Therefore G is a cyclic group, generated by the element x. Moreover all elements of G other than the identity element are generators of G, and are therefore of order p, where $p = |G|$. Let d be a divisor of p. Then x^d is an element of order p/d, since p/d is the smallest positive integer k for which $x^{dk} = e$. It follows that either $d = 1$ or $d = p$ (since the group G contains no element whose order is greater than 1 but less than p). It follows that the order p of G is a prime number, as required. ∎

We have already proved that if $n \geq 5$ then the alternating group A_n has no normal subgroups other than the trivial subgroup and the whole of A_n. Thus A_n is a simple group when $n \geq 5$. The order of the group A_n is $n!/2$. In particular $|A_5| = 60$.

Using the Sylow Theorems and related results, we can prove that any finite simple group whose order is less than 60 is a cyclic group of prime order.

Now the prime numbers less than 60 are the following: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 and 59. All groups of these orders are simple groups, and are cyclic groups.

If p is a prime number greater than 2 then any group of order $2p$ is either a cyclic group or else is isomorphic to the dihedral group D_{2p} of order $2p$ (Theorem 2.49). In either case such a group contains a normal subgroup of order p, and therefore not a simple group. In particular, there are no simple groups of orders 6, 10, 14, 22, 26, 34, 38, 46 or 58.

If G is a group of order p^k for some prime number p and for some integer k satisfying $k \geq 2$, then G contains a normal subgroup of order p (Lemma 2.43). It follows that such a group is not simple. In particular, there are no simple groups of orders 4, 8, 16, 32, 9, 27, 25 and 49.

Let G be a group of order pq, where p and q are prime numbers and $p < q$. Any Sylow q-subgroup of G is of order q, and the number of such Sylow q-subgroups must divide pq and be congruent to 1 modulo q. Now p cannot be congruent to 1 modulo q, since $1 < p < q$. Therefore G has just one Sylow q-subgroup, and this is a normal subgroup of G of order q. It follows that such a group is not a simple group. In particular there are no simple groups of orders 15, 21, 33, 35, 39, 51, 55 or 57. (In particular it follows from Theorem 2.48 that any group whose order is 15, 33, 35, or 51 is a cyclic group.)

It only remains to verify that there are no simple groups of orders 12, 18, 20, 24, 28, 30, 36, 40, 42, 44, 45, 48, 50, 52, 54 or 56.

We can deal with many of these on applying Theorem 2.50. On applying this theorem with $p = 2$, $q = 3$ and $d = 2$, we see that there are no simple groups of orders 6 or 12. On applying the theorem with $p = 2$, $q = 5$ and $d = 4$, we see that there are no simple groups of orders 10, 20, 40 or 80. On applying the theorem with $p = 2$, $q = 7$ and $d = 3$, we see that there are no simple groups of orders 14, 28 or 56. On applying the theorem with $p = 2$, $q = 11$ we see that there are no simple groups of orders 22, 44 etc., on applying the theorem with $p = 2$, $q = 13$ we see that there are no simple groups of orders 26, 52 etc., and on applying the theorem with $p = 3$ and $q = 5$, we see that there are no simple groups of orders 15, 45 etc.

It now remains to verify that there are no simple groups of orders 18, 24, 30, 36, 42, 48, 50 or 54.

Using the Second Sylow Theorem, we see that any group of order 18 has just one Sylow 3-subgroup. This Sylow 3-subgroup is then a normal group of order 9, and therefore no group of order 18 is simple. Similarly a group of order 50 has just one Sylow 5-subgroup, which is then a normal subgroup of order 25, and therefore no group of order 50 is simple. Also a group of order 54 has just one Sylow 3-subgroup, which is then a normal subgroup of order 27, and therefore no group of order 54 is simple.

On applying the Second Sylow Theorem, we see the number of Sylow 7-subgroups of any group of order 42 must divide 42 and be congruent to 1 modulo 7. This number must then be coprime to 7 and therefore divide 6, since $42 = 7 \times 6$. But no divisor of 6 greater than 1 is coprime to 1 modulo 7. It follows that any group of order 42 has just one Sylow 7-subgroup, and this subgroup is therefore a normal subgroup of order 7. Thus no group of order 42 is simple.

On applying the Second Sylow Theorem, we see that if a group of order 30 has more than one subgroup of order 3 then it must have 10 such subgroups, and must therefore have 20 elements of order 3 (since each subgroup of order 3 contains two elements of order 3, and the intersection of two distinct subgroups of order 3 must be the trivial subgroup). Similarly if a group of order 30 has more than one subgroup of order 5 then it must have 6 such subgroups, and must therefore have 24 elements of order 5. Obviously such a group cannot have both 20 elements of order 3 and 24 elements of order 5. Therefore it either has a single subgroup of order 3 or a single subgroup of order 5. This subgroup is normal. Therefore no group of order 30 is simple.

In order to show that there are no simple groups of order less than 60, apart from the cyclic groups whose order is prime, it only remains to verify that there are no simple groups of orders 24, 36 and 48. In order to deal with these remaining cases, we need to make use of the following result.

Lemma 2.52 *Let H and K be subgroups of a finite group G. Then*

$$|H \cap K| \geq \frac{|H|\,|K|}{|G|}.$$

Proof Let $\varphi: H \times K \to G$ be the function with $\varphi(h,k) = hk$ for all $h \in H$ and $k \in K$. (This function is not in general a homomorphism.) Let (h_1, k_1) and (h_2, k_2) be elements of $H \times K$. Then $h_1 k_1 = h_2 k_2$ if and only if $h_2^{-1} h_1 = k_2 k_1^{-1}$, in which case $h_2^{-1} h_1 \in H \cap K$. But then $h_2 = h_1 x^{-1}$ and $k_2 = x k_1$ for some element x of $H \cap K$. Thus $\varphi(h_1, k_1) = \varphi(h_2, k_2)$ if and only if $(h_2, k_2) = (h_1 x^{-1}, x k_1)$ for some element x of $H \cap K$. It follows that each element of the range $\varphi(H \times K)$ of the function φ is the image of exactly $|H \cap K|$ elements of $H \times K$. It follows from this that $\varphi(H \times K)$ has $\dfrac{|H|\,|K|}{|H \cap K|}$ elements. But $\varphi(H \times K)$ is a subset of G. Therefore

$$\frac{|H|\,|K|}{|H \cap K|} \leq |G|.$$

The required inequality now follows directly. ∎

Let G be a finite group, and let H be a subgroup of index 2 in G (i.e., a subgroup with half as many elements as G). Then H is a normal subgroup of G. Indeed the subsets H and $G \setminus H$ of G are the left cosets and are also the right cosets of H in G, and therefore the left cosets of H in G coincide with the right cosets.

Example We now show that there are no simple groups of order 24. Let G be a group of order 24. Then G contains a Sylow 2-subgroup H of order 8. If this is the only Sylow 2-subgroup, then it is a normal subgroup, and therefore the group G is not simple. Otherwise the group G contains at least two distinct subgroups H and K of order 8. It then follows from Lemma 2.52 that $|H \cap K| \geq \frac{8}{3}$. But $|H \cap K|$ divides 8, by Lagrange's Theorem, since $H \cap K$ is a subgroup of H and of K. Therefore $|H \cap K| = 4$. It follows that $H \cap K$ is a subgroup of index 2 in H and K, and is therefore a normal subgroup of both H and K. Let

$$J = \{g \in G : g(H \cap K)g^{-1} = H \cap K\}.$$

Then J is a subgroup of G, and $H \cap K$ is a normal subgroup of J. Moreover H and K are subgroups of J, and therefore $|J|$ is divisible by 8, by Lagrange's Theorem. But J is a subgroup of G, and hence $|J|$ divides 24. Also $|J| > 8$, since H (and K) are proper subgroups of J. It follows that $|J| = 24$, and therefore $J = G$. But then $H \cap K$ is a normal subgroup of G of order 4, and therefore G is not simple.

An analogous argument shows that there are no simple groups of order 48: a group G of order 48 contains either a single Sylow 2-subgroup of order 16, which is then a normal subgroup of G, or else it contains a normal subgroup of order 8 which is the intersection of two distinct Sylow 2-subgroups of G.

The following result will be needed in order to show that there are no simple groups of order 36. (It may be obtained as an immediate corollary of Proposition 2.44.)

Lemma 2.53 *Let G be a group of order p^2 where p is a prime number, and let H be a subgroup of G of order p. Then H is a normal subgroup of G.*

Proof Let $J = \{g \in G : gHg^{-1} = H\}$. Then J is a subgroup of G and H is a normal subgroup of J. We shall show that $J = G$.

Now the centre $Z(G)$ of G is contained in J. Moreover it follows from Lemma 2.43 that $|Z(G)|$ is divisible by p. Were it the case that $|J| = p$ then $J = H = Z(G)$. But then J would consist of all elements of G for which $gZ(G)g^{-1} = Z(G)$, and thus would be the whole of G, which is impossible. It follows that $|J| = p^2$ (since $|J| > p$ and $|J|$ divides p^2). But then $J = G$, and hence H is a normal subgroup of G, as required. ∎

Example We now show that there are no simple groups of order 36. Let G be a group of order 36. Then G contains a Sylow 3-subgroup H of order 9. If this is the only Sylow 3-subgroup, then it is a normal subgroup, and therefore the group G is not simple. Otherwise the group G contains at least two distinct subgroups H and K of order 9. It then follows from Lemma 2.52 that $|H \cap K| \geq \frac{9}{4}$. But $|H \cap K|$ divides 9, by Lagrange's Theorem, since $H \cap K$ is a subgroup of H and of K. Therefore $|H \cap K| = 3$. On applying Lemma 2.53 we see that $H \cap K$ is a normal subgroup of H and of K.

Let

$$J = \{g \in G : g(H \cap K)g^{-1} = H \cap K\}.$$

Then J is a subgroup of G, and $H \cap K$ is a normal subgroup of J. Moreover H and K are subgroups of J, and therefore $|J|$ is divisible by 9, by Lagrange's Theorem. But J is a subgroup of G, and hence $|J|$ divides 36. Also $|J| > 9$, since H (and K) are proper groups of J. It follows that either $|J| = 18$ or 36. If $|J| = 36$ then $J = G$ and $H \cap K$ is a normal subgroup of G of order 3. If $|J| = 18$ then J is a subgroup of G of index 2, and is therefore a normal subgroup of order 18. We conclude that any group of order 36 contains at least one non-trivial normal subgroup. Therefore there are no simple groups of order 36.

We have now shown that there are indeed no simple groups of order less than 60, other than the cyclic groups of prime order.

2.24 Solvable Groups

Definition A group G is said to be *solvable* (or *soluble*) if there exists a finite sequence $G_0, G_1, \ldots, G_n$ of subgroups of G, where $G_0 = \{1\}$ and $G_n = G$, such that G_{i-1} is normal in G_i and G_i/G_{i-1} is Abelian for $i = 1, 2, \ldots, n$.

Example The symmetric group Σ_4 is solvable. Indeed let V_4 be the *Kleinsche Viergruppe* consisting of the identity permutation ι and the permutations (12)(34), (13)(24) and (14)(23), and let A_4 be the alternating group consisting of all even permutations of $\{1, 2, 3, 4\}$. Then $\{\iota\} \triangleleft V_4 \triangleleft A_4 \triangleleft \Sigma_4$, V_4 is Abelian, A_4/V_4 is cyclic of order 3, and Σ_4/A_4 is cyclic of order 2.

Lemma 2.54 *Let G be a group, let H_1 and H_2 be subgroups of G, where $H_1 \triangleleft H_2$, and let $J_1 = H_1 \cap N$, $J_2 = H_2 \cap N$, $K_1 = H_1N/N$ and $K_2 = H_2N/N$, where N is some normal subgroup of G. Then $J_1 \triangleleft J_2$ and $K_1 \triangleleft K_2$. Moreover there exists a normal subgroup of H_2/H_1 isomorphic to J_2/J_1, and the quotient of H_2/H_1 by this normal subgroup is isomorphic to K_2/K_1.*

Proof It is a straightforward exercise to verify that $J_1 \triangleleft J_2$ and $K_1 \triangleleft K_2$. Let $\theta\colon H_2 \to K_2$ be the surjective homomorphism sending $h \in H_2$ to the coset hN. Now θ induces a well-defined surjective homomorphism $\psi\colon H_2/H_1 \to K_2/K_1$, since $\theta(H_1) \subset K_1$. Also $\theta^{-1}(K_1) = H_2 \cap (H_1N)$. But $H_2 \cap (H_1N) = H_1(H_2 \cap N)$, for if $a \in H_1$, $b \in N$ and $ab \in H_2$ then $b \in H_2 \cap N$. Therefore

$$\ker \psi = \theta^{-1}(K_1)/H_1 = H_1(H_2 \cap N)/H_1 \cong H_2 \cap N/H_1 \cap N = J_2/J_1$$

by the First Isomorphism Theorem (Theorem 2.23). Moreover the quotient of H_2/H_1 by the normal subgroup $\ker \psi$ is isomorphic to the image K_2/K_1 of ψ. Thus $\ker \psi$ is the required normal subgroup of H_2/H_1. ∎

Proposition 2.55 *Let G be a group, and let H be a subgroup of G. Then*

(i) *if G is solvable then any subgroup H of G is solvable;*

(ii) *if G is solvable then G/N is solvable for any normal subgroup N of G;*

(iii) *if N is a normal subgroup of G and if both N and G/N are solvable then G is solvable.*

Proof Suppose that G is solvable. Let $G_0, G_1, \ldots, G_m$ be a finite sequence of subgroups of G, where $G_0 = \{1\}$, $G_n = G$, and $G_{i-1} \triangleleft G_i$ and G_i/G_{i-1} is Abelian for $i = 1, 2, \ldots, m$.

We first show that the subgroup H is solvable. Let $H_i = H \cap G_i$ for $i = 0, 1, \ldots, m$. Then $H_0 = \{1\}$ and $H_m = H$. If $u \in H_i$ and $v \in H_{i-1}$ then

$uvu^{-1} \in H$, since H is a subgroup of G. Also $uvu^{-1} \in G_{i-1}$, since $u \in G_{i-1}$, $v \in G_i$ and G_{i-1} is normal in G_i. Therefore $uvu^{-1} \in H_{i-1}$. Thus H_{i-1} is a normal subgroup of H_i for $i = 1, 2, \ldots, m$. Moreover

$$\frac{H_i}{H_{i-1}} = \frac{G_i \cap H}{G_{i-1} \cap (G_i \cap H)} \cong \frac{G_{i-1}(G_i \cap H)}{G_{i-1}}$$

by the First Isomorphism Theorem (Theorem 2.23), and thus H_i/H_{i-1} is isomorphic to a subgroup of the Abelian group G_i/G_{i-1}. It follows that H_i/H_{i-1} must itself be an Abelian group. We conclude therefore that the subgroup H of G is solvable.

Now let N be a normal subgroup of G, and let $K_i = G_iN/N$ for all i. Then K_0 is the trivial subgroup of G/N and $K_m = G/N$. It follows from Lemma 2.54 that $K_{i-1} \triangleleft K_i$ and K_i/K_{i-1} is isomorphic to the quotient of G_i/G_{i-1} by some normal subgroup. But a quotient of any Abelian group must itself be Abelian. Thus each quotient group K_i/K_{i-1} is Abelian, and thus G/N is solvable.

Finally suppose that G is a group, N is a normal subgroup of G and both N and G/N are solvable. We must prove that G is solvable. Now the solvability of N ensures the existence of a finite sequence $G_0, G_1, \ldots, G_m$ of subgroups of N, where $G_0 = \{1\}$, $G_m = N$, and $G_{i-1} \triangleleft G_i$ and G_i/G_{i-1} is Abelian for $i = 1, 2, \ldots, m$. Also the solvability of G/N ensures the existence of a finite sequence $K_0, K_1, \ldots, K_n$ of subgroups of G/N, where $K_0 = N/N$, $K_n = G/N$, and $K_{i-1} \triangleleft K_i$ and K_i/K_{i-1} is Abelian for $i = 1, 2, \ldots, n$. Let G_{m+i} be the preimage of K_i under the the quotient homomorphism $\nu: G \to G/N$, for $i = 1, 2, \ldots, n$. The Second Isomorphism Theorem (Theorem 2.24) ensures that $G_{m+i}/G_{m+i-1} \cong K_i/K_{i-1}$ for all $i > 0$. Therefore $G_0, G_1, \ldots, G_{m+n}$ is a finite sequence of subgroups of G, where $G_0 = \{1\}$, $G_n = G$, and $G_{i-1} \triangleleft G_i$ and G_i/G_{i-1} is Abelian for $i = 1, 2, \ldots, m+n$. Thus the group G is solvable, as required. ∎

Example The alternating group A_n is simple for $n \geq 5$ (see Theorem 2.36). Moreover the definition of solvable groups ensures that that any simple solvable group is cyclic, and A_n is not cyclic when $n \geq 5$. Therefore A_n is not solvable when $n \geq 5$. It then follows from Proposition 2.55 that the symmetric group Σ_n is not solvable when $n \geq 5$.