

Chapter 2

Elementary Group Properties

In this chapter, we introduce our main objects of study—groups. A general overview including some historical comments was given in Chapter 1. More detail on the history of the theory can be found in Wussing (1984), van der Waerden (1985), and at www-gap.dcs.st-andrews.ac.uk/~history/. Here we give the basic definitions and an extensive list of examples, introduce subgroups and cosets, normal subgroups and simple groups, and prove the first major result in the theory—Lagrange’s Theorem.

2.1 Basic Definitions

We begin by defining the group concept. Maps between groups will be discussed in Chapter 4. As a preliminary to this we introduce *semigroups* as follows.

Definition 2.1 A *semigroup* is a non-empty set $X = \{\dots, x, y, z, \dots\}$ together with a binary operation \odot (page 281) which satisfies the following two conditions (axioms):

- (i) it is *closed*, or *well-defined*: for all $x, y \in X$, we can perform the operation $x \odot y$ and

$$x \odot y \in X,$$

- (ii) it is *associative*: for all $x, y, z \in X$,

$$x \odot (y \odot z) = (x \odot y) \odot z.$$

Note that (i) is implied by the definition of the operation \odot ; see the comments below Definition 2.2.

Examples The following sets with operations are semigroups.

- (a) The positive integers with addition.
- (b) The set of all one-variable functions with domain and codomain \mathbb{R} , and with the operation of composition of functions.

There is an extensive theory of semigroups which is of particular interest in some branches of analysis and combinatorics. Also a number of similar systems that are not quite groups have been studied, for instance, the operation may be only partially defined, or there may be a neutral element but no inverses, *et cetera*. We shall not consider these systems; Bruck (1966) provides a good introduction.

Definition 2.2 A group (G, \odot) is a semigroup which satisfies the following extra conditions (axioms):

- (iii) G contains a unique element e which satisfies, for all $g \in G$,

$$e \odot g = g \odot e = g,$$

- (iv) for each $g \in G$, there exists a unique $g' \in G$ satisfying

$$g \odot g' = g' \odot g = e.$$

The element e is called the *neutral element* of the group G , see page 4. Some authors use the term *identity* for e , and if the operation (\odot) is written additively $(+)$ then it is called the *zero* and denoted by 0. There are a number of redundancies in this definition—in particular, in axioms (i), (iii) and (iv). Strictly speaking, (i) is unnecessary as it is implied by the fact that \odot is an operation; see Appendix A. But we have left it in to remind the reader that closure is vitally important—this property must be checked whenever it is required to show that a particular set and product form a group. For (iii) and (iv), see Theorem 2.5.

Definition 2.3 A group (G, \odot) is called *Abelian*, or occasionally *commutative*, if its operation is commutative: For all $g, h \in G$

$$g \odot h = h \odot g.$$

The term ‘Abelian’ commemorates the Norwegian mathematician Niels Abel who died at the age of 27 in 1829. He was working on solutions to polynomial equations, and needed to apply a condition similar to the one above; see the Introduction to Chapter 11 and van der Waerden (1985), page 88.

Examples We give four here, and an extensive list in the next section.

- (a) The set $\{1, -1\}$ with the operation of standard multiplication forms a finite Abelian group which we denote by T_1 (one copy of ‘two’). The neutral element is 1, and each element is self-inverse.
- (b) The set of *permutations* of a set $\{1, 2, 3\}$. The elements are the six permutations of this set, and the operation is composition: Do the first permutation, then do the

second permutation on the result of the first. For example, if the first permutation maps $1 \mapsto 1$, $2 \mapsto 3$ and $3 \mapsto 2$, and the second maps $1 \mapsto 3$, $2 \mapsto 2$ and $3 \mapsto 1$, then their composition maps $1 \mapsto 3$, $2 \mapsto 1$ and $3 \mapsto 2$. The neutral element is the permutation that moves no symbols, and the inverse of a permutation is its reverse (Section 3.1). This system forms a finite non-Abelian group which we denote by S_3 and call the *symmetric group* of the set $\{1, 2, 3\}$. Reader, why is this group not Abelian?

- (c) The positive real numbers \mathbb{R}^+ with multiplication form an infinite Abelian group. The neutral element is 1, and the inverse of x is $1/x$.
- (d) The set of all non-singular 2×2 matrices having rational number entries with the operation of matrix multiplication is an example of an infinite non-Abelian group, it is denoted by $GL_2(\mathbb{Q})$ and called the 2×2 *general linear group* over \mathbb{Q} . The neutral element is I_2 , the 2-dimensional identity matrix, and inverses exist by definition.

The symbols (G, \odot) , G , H , J , or K , sometimes with primes or subscripts, will always denote groups. We use lower case Roman letters a, b, c, d, g, h, j, k , and l , again sometimes with primes or suffixes, to stand for group elements, and we use x, y and z for set elements or occasionally for group elements following the usual mathematical convention that these letters denote entities which satisfy a proposition or equation. The words ‘operation’, ‘multiplication’ and ‘product’ are used more or less synonymously: If $g, h \in G$ we say that we apply the operation \odot to form the product $g \odot h$, or we multiply g by h to obtain $g \odot h$.

The *underlying set* of a group G is the set of elements of G stripped of its operation; where there is no confusion, this will also be denoted by G . Also, we sometimes say that a group G is *generated* by a set X , or X is a *generating set* for G , where X is a subset of the underlying set of G , and we write $G = \langle X \rangle$. This means that the collection of all products of powers (both positive and negative) of elements of X coincides with G . For example, the set $\{1\}$ is a generating set for \mathbb{Z} , that is, $\mathbb{Z} = \langle 1 \rangle$ because every integer can be expressed as a sum of 1s or -1 s. Note that a group may have many different generating sets, and it always has at least one because the underlying set of G clearly acts as a generating set for G . This notion is defined formally in Definition 2.16. We also write $\langle e \rangle$ for the (unique) group containing the single element e (with operation $e \odot e = e$), we call it the *neutral group*. Some authors use the term ‘trivial group’ for $\langle e \rangle$; it is an important component of a group and certainly not ‘trivial’ using the normal meaning of this word, hence we shall not use this term; see also the comments on page 4.

We noted above that Definition 2.2 can be weakened considerably without affecting our objects of study. Consider

Definition 2.2’ A group (G, \odot) is a semigroup, see Definition 2.1, which satisfies the following two conditions:

- (iii)’ there is an element $f \in G$ with the property: $f \odot g = g$, for all $g \in G$;
- (iv)’ for each $g \in G$, and with f as in (iii)’, there exists $h \in G$ satisfying $h \odot g = f$.

These conditions imply that G has at least one *left neutral element* f , and each $g \in G$ has at least one *left inverse* h relative to f .

Definition 2.2' is equivalent to Definition 2.2; see also Problem 2.4. Note that this equivalence is useful, for when checking if the group axioms hold for a particular set and map, once closure and associativity have been established (Axioms (i) and (ii)), it is not necessary to prove that either the neutral element or the inverse operation is unique, or two-sided, because these properties follow by Theorem 2.5 below. Also, if we find *an* inverse of an element g , then we can be sure that it is the *unique* inverse of g , again by Theorem 2.5.

We begin with the following result: In all groups, the only element which equals its square is the neutral element (in algebra generally, such elements are called *idempotents*).

Lemma 2.4 *Let (G, \odot) be a semigroup satisfying the conditions of Definition 2.2'. If $a \in (G, \odot)$ and $a \odot a = a$, then $a = f$ where f is given by (iii)'.*

*Proof*¹ By (iv)', if $a \in G$ we can find $b \in G$ satisfying $b \odot a = f$, so by (iii)'

$$a = f \odot a = (b \odot a) \odot a = b \odot (a \odot a) = b \odot a = f,$$

by associativity, the hypothesis and (iv)' again. □

Theorem 2.5 *A semigroup (G, \odot) satisfying Conditions (iii)' and (iv)' in Definition 2.2' forms a group as given by Definition 2.2.*

Proof We need to show that f , and the inverses, apply both on the left and on the right, and are unique; that is, f as *the* neutral element, and h as *the* inverse of g . First, we show that if $a \in (G, \odot)$ and $b \odot a = f$, then $a \odot b = f$ (a left inverse is also a right inverse). We have

$$b \odot (a \odot b) = (b \odot a) \odot b = f \odot b = b.$$

by (ii), (iv)', and (iii)'. Hence, by (ii) again

$$(a \odot b) \odot (a \odot b) = a \odot (b \odot (a \odot b)) = a \odot b.$$

By Lemma 2.4, this shows that $a \odot b = f$; the first part follows. Secondly f is a right identity. We have, using the above subresult and (ii),

$$a \odot f = a \odot (b \odot a) = (a \odot b) \odot a = f \odot a = a$$

by (iii)'. Thirdly, we show that b is unique (that is, inverses are unique). For suppose $c \odot a = f$, then we have by the above and (ii)

$$c = c \odot f = c \odot (a \odot b) = (c \odot a) \odot b = f \odot b = b,$$

¹To emphasise their importance, and to aid clarity, all proofs are typeset indented.

by hypothesis and (iii)' applied to b . Lastly, the neutral element. For if e also satisfies (iii)', that is $e \odot a = a$ for $a \in G$, then substituting e for a we obtain $e \odot e = e$, and so, by Lemma 2.4, $e = f$. This completes the proof. \square

From now on, we adopt the following conventions. We write ab for $a \odot b$, e for the neutral element, and G for (G, \odot) when it is clear which operation is being used. Also, the inverse of g given by (iv) in Definition 2.2 will be written in the standard notation g^{-1} (and $-g$ if we are using addition). We normally drop brackets and write xyz for either $x(yz)$, or $(xy)z$. In some cases, we do not delete the brackets if this aids clarity.

The next three results apply to all groups, and they will often be used in the sequel usually without being specifically identified. Note that no restrictions apply, a rare occurrence in the theory!

Theorem 2.6 (Cancellation) *Suppose $a, b, x, y \in G$. If $ax = bx$, or if $ya = yb$, then $a = b$.*

Proof From $ax = bx$ we obtain, by Definition 2.2 and associativity,

$$a = ae = a(xx^{-1}) = (ax)x^{-1} = (bx)x^{-1} = b(xx^{-1}) = b.$$

A similar argument applies in the second case. \square

Theorem 2.7 *Suppose a and b are elements of a group G .*

- (i) $(ab)^{-1} = b^{-1}a^{-1}$.
- (ii) $(a^{-1})^{-1} = a$.
- (iii) *If G is finite, then a^{-1} equals some positive power of a .*
- (iv) *If a commutes with b , then a^{-1} also commutes with b .*

Proof (i) As $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e$ and, by Theorem 2.5, inverses are unique and two-sided, it follows that $b^{-1}a^{-1}$ is the inverse of ab . A similar argument applies for (ii).

(iii) If G has n elements and $a \neq e$, then an integer m must exist satisfying $1 < m \leq n$ and $a^m = e$ (the powers of a cannot all be distinct in the finite case). Now $a^{m-1} = a^{-1}a^m = a^{-1}$.

(iv) If $ab = ba$ then $b = a^{-1}ba$, and so $ba^{-1} = a^{-1}b$. \square

Using induction we can extend (i) to prove that $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

Theorem 2.8 *If we treat the group G as a set (that is, we consider the underlying set of G) then, for all fixed $a \in G$,*

$$G = \{ag : g \in G\} = \{g^{-1} : g \in G\}.$$

Proof Use Theorems 2.6 and 2.7; see Problem 2.1. \square

Most elementary exponent properties apply to groups. Note that as the group in question may not be Abelian some properties do not always hold. For example, $(ab)^2$ may, or may not, equal a^2b^2 .

For all elements a in a group, if $n \geq 0$ we write

$$a^0 = e \quad \text{and} \quad a^{n+1} = a^n a, \quad \text{that is} \quad a^n = aa \cdots a \text{ (} n \text{ copies of } a \text{)}.$$

Also, again if $n \geq 0$ we write a^{-n} in place of $(a^{-1})^n$. By Theorem 2.7, this also equals $(a^n)^{-1}$; reader, why?

Theorem 2.9 Suppose a is a group element, and $r, s \in \mathbb{Z}$.

- (i) $a^{r+s} = a^r a^s$.
- (ii) $(a^r)^s = a^{rs}$.

Proof (i) By induction on s . Suppose s is non-negative. We have $a^{r+0} = a^r = a^r e = a^r a^0$ and, using the inductive hypothesis in the third equation,

$$a^{r+(s+1)} = a^{(r+s)+1} = a^{r+s} a = a^r a^s a = a^r a^{s+1}.$$

Now apply induction. Using this we have $a^{r-s} a^s = a^{(r-s)+s} = a^r$, hence $a^{r-s} = a^r (a^s)^{-1} = a^r a^{-s}$ and (i) follows for negative s .

(ii) Assume first that s is non-negative. As above we use induction on s , we have $(a^r)^0 = e = a^{0r}$ and

$$(a^r)^{(s+1)} = (a^r)^s a^r = a^{rs} a^r = a^{r(s+1)},$$

and this case follows by the inductive hypothesis and (i). The reader should do the remaining case using a similar method to that given in the last part of the proof of (i). \square

We shall see below that an important invariant of a group is the number of elements in its underlying set, we define this as follows.

Definition 2.10 (i) Two groups G and H are called *equal*, $G = H$, if and only if their underlying sets are equal (page 277), and they have the same operation.

(ii) The *order* of a group G is the number (or cardinality) of elements in the underlying set of G , this is denoted by $o(G)$.

Some comments on cardinality are given in Appendix A. One or two authors reserve the word ‘order’ for groups and use the word ‘size’ for sets, we shall use ‘order’ for both. Note that $o(G)$ can be finite or infinite, and this distinction is important; see page 5. If the order of G is finite, then the usual number-theoretic rules apply and, as we shall show later, they have a powerful controlling influence on the structure of G . If $o(G)$ is infinite, then different considerations apply and care is needed when interpreting results.

Isomorphism—A Preliminary Note

Several groups can appear to be distinct but are, in fact, identical from the group-theoretical point of view. If we have two groups G_1 and G_2 with a bijection θ between their underlying sets which preserves or transforms all group-theoretic properties of G_1 to G_2 , and vice versa, then we say they are *isomorphic*, and θ is an *isomorphism* between them, symbolically this is written $G_1 \simeq G_2$. The main property is

$$(ab)\theta = a\theta \cdot b\theta, \quad (2.1)$$

for all $a, b \in G_1$; see page 68. We shall give a formal definition of this concept at the beginning of Chapter 4, but it will be convenient to be able to use this notion from now on. As an illustration, we give two examples here. If $G = H$, see Definition 2.10(i), then the identity map (page 281) clearly acts as an isomorphism. Secondly, the real numbers with addition \mathbb{R} , and the positive reals with multiplication \mathbb{R}^+ , both form groups. They are isomorphic, and one isomorphism θ defined by

$$x\theta = 2^x, \quad \text{for } x \in \mathbb{R},$$

demonstrates this fact. The map $\theta : \mathbb{R} \rightarrow \mathbb{R}^+$ is a bijection (with inverse \log_2) and it transfers all group-theoretic properties of the first group to the second, and vice versa via (2.1). For instance, the neutral element 0 of \mathbb{R} is mapped to $2^0 = 1$, the neutral element of \mathbb{R}^+ , and if $a, b \in \mathbb{R}$ then $(a + b)\theta = 2^{a+b} = 2^a 2^b = a\theta b\theta$ which verifies (2.1) in this case.

Isomorphism Class

Consider the statement: “There are only two groups of order 6” (Problem 2.20). This is not correct as it stands because there are infinitely many distinct groups of order 6, but many are isomorphic to one another. So to be more precise, we should say that “there are exactly two *isomorphism classes* of groups of order 6”. If we take the group with elements $\{0, 1, 2, 3, 4, 5\}$ and operation addition modulo 6 ($\mathbb{Z}/6\mathbb{Z}$, the cyclic group of order 6), and D_3 (page 3) as our ‘standard’ groups of order 6, then it is true that all groups of order 6 are isomorphic to one of these two groups. When discussing groups of a fixed size we shall often use this short-hand.

2.2 Examples

Groups are found throughout mathematics, there is hardly a branch of the subject where they do not occur, they are also widely used in many branches of the physical sciences. We give here an extensive list of examples to illustrate the range and applicability of the group concept. No proofs will be given, in most cases it is not

difficult to check that the group axioms are satisfied. Note that the notation for individual groups given in this section will be used throughout the book, see pages 303 and 304.

Number Systems

Our first examples are the standard number systems. The integers \mathbb{Z} , the rational numbers \mathbb{Q} , the real numbers \mathbb{R} , and the complex numbers \mathbb{C} , with the operation of standard addition in each case, all form infinite Abelian groups. The non-zero rational numbers \mathbb{Q}^* , non-zero real numbers \mathbb{R}^* , and non-zero complex numbers \mathbb{C}^* , with the operation of multiplication in each case, also form infinite Abelian groups distinct from the above. In general, for a ring or field F we let F^* denote the multiplicative group of the non-zero elements of F . Further, the positive rationals \mathbb{Q}^+ with multiplication form a group (which is a subgroup of \mathbb{Q}^* ; see Section 2.3), with a similar construction for \mathbb{R}^+ . Note that neither the non-zero integers with multiplication nor the positive integers with multiplication form groups as inverses do not exist.

Modular Arithmetic

Our second collection of examples are finite groups from number theory. If $m > 0$, the *congruence*

$$a \equiv b \pmod{m}$$

stands for: a and b have the same remainder after division by m (in symbols, $m \mid b - a$). This notation was first introduced by C.F. Gauss in 1801 in his famous number theory text called ‘Disquisitiones arithmeticae’. Let $\mathbb{Z}/m\mathbb{Z}$ denote the set $\{0, 1, \dots, m-1\}$. If $a, b \in \mathbb{Z}/m\mathbb{Z}$, the operation $+_m$ is given by

$$a +_m b = a + b, \quad \text{if } a + b < m, \quad \text{and}$$

$$a +_m b = a + b - m, \quad \text{if } a + b \geq m,$$

(so $a +_m b \equiv a + b \pmod{m}$), this is called *addition modulo m*). The set $\mathbb{Z}/m\mathbb{Z}$ with the operation $+_m$ is an Abelian group of order m , the notation $\mathbb{Z}/m\mathbb{Z}$ which relates to cosets and factor groups will be explained in Chapter 4. This implies that at least one group of order m exists for each positive integer m ; in some cases this is essentially the only group of this order (that is, up to isomorphism); for example, when $m = 13$ or 15 , see Appendix D.

If m is a prime number p , then $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ with multiplication modulo p , defined similarly to addition modulo p , forms another finite Abelian group. Inverses exist by the Euclidean Algorithm (Theorem B.2 in Appendix B). Also note that the group $T_1 = \{-1, 1\}$ (page 42) is isomorphic both to the group $\mathbb{Z}/2\mathbb{Z}$, and to the group $(\mathbb{Z}/3\mathbb{Z})^*$.

Product Groups

Given groups G_1, \dots, G_n , we can form a new group by taking all (ordered) n -tuples of the form (g_1, \dots, g_n) , where $g_i \in G_i$ for $i = 1, \dots, n$, as the new elements, and defining the new operation component-wise using the operations of each G_i in turn. In many cases, several different operations can be defined; see Chapter 7. For example, suppose $n = 2$ and $G_1 = G_2 = T_1$. The elements of the product group are

$$(1, 1), \quad (1, -1), \quad (-1, 1), \quad (-1, -1),$$

and the operation is given by $(a, b)(c, d) = (ac, bd)$. This group is called the *4-group* and is denoted by T_2 ; it is a product of two copies of T_1 ; in Chapter 7, we use the standard notation $C_2 \times C_2$ for this group. Some authors use K (for Klein group) or V (for ‘Viergruppe’ the German word for ‘4-group’ or ‘fours group’) for this group. Note that the square of every element in T_2 is the neutral element $(1, 1)$, and it is an example of an *Elementary Abelian Group* as defined in Problem 4.18.

Matrix Groups

Matrix groups form one of the most important collections in the theory. Let F be a field (for instance, the rational numbers \mathbb{Q}) and let $m \geq 1$. The set of non-singular $m \times m$ matrices with entries from F and operation matrix multiplication forms a non-Abelian group (if $m > 1$) called the $m \times m$ *general linear group* over F , it is denoted by $GL_m(F)$. The group axioms can be shown to hold using some elementary matrix algebra; the matrices are non-singular, and so inverses exist by definition. See Section 3.3 for further details.

As we shall show later, subgroups (Section 2.3) of these matrix groups provide a further wide range of examples. For instance, (a) by considering only those matrices with determinant 1 in $GL_m(F)$ we obtain the $m \times m$ *special linear group* denoted by $SL_m(F)$, or (b) by considering those matrices that have zeros at all entries below the main diagonal we obtain the group of $m \times m$ upper triangular matrices denoted by $UT_m(F)$; see Section 3.3. Also many examples can be obtained by choosing different fields F . So if F is finite, these matrix groups provide a variety of examples of finite non-Abelian groups. For instance, $SL_2(\mathbb{F}_4)$ (which we usually write as $SL_2(4)$, the group of all 2×2 matrices A with $\det A = 1$ and entries in the four element field \mathbb{F}_4 —see page 254) is an important example of a *simple* group; as given by Definition 2.33. Many other simple groups can be defined using similar constructions; see Sections 12.2 and 12.3.

Symmetries of Geometric Objects

The symmetry properties of geometric objects provide a number of group examples. In Chapter 1 (page 3), we discussed the symmetries of an equilateral triangle, the

group in question being called the *dihedral group* of the triangle denoted by D_3 . The elements of the group are the rotations and reflections that give the same geometric figure, and the operation is composition. A similar construction can be carried out for a regular polygon with n sides: the clockwise rotations about the centre are now by $2\pi/n$, and ‘reflection’ or ‘turning over’ is as before. This group is denoted by D_n and again called *dihedral*. For example, D_4 is the group of symmetries of the square, it has order 8. (Note that a few authors write D_{2n} for D_n , see page 303.) Some other regular geometric objects have non-neutral (rotational) symmetry groups, for example, the tetrahedron (A_4 , see Problem 3.10), the octahedron (S_4 , see page 170) and the dodecahedron (A_5 , see Section 3.2 and Web Section 3.6).

Also under this heading is the topic of *sphere packing* in various dimensions. Consider a large container filled with identical balls, some will touch adjacent balls and some will not. In dimension 2, where we have identical discs, a regular pattern forms and the set of disc centres gives a lattice (of equilateral triangles), and we can consider the symmetries of this lattice just as we have done for the triangle. In dimension 3, no such regular pattern forms where all adjacent balls touch. In this case, there are infinitely many ways to fit twelve balls around a central ball all touching it (there is always some room to spare), but thirteen never quite fit. In dimensions 8 and 24, ‘regular touching’ patterns do again form, the lattices given by the centres of the ‘spheres’ have some remarkable properties and give rise to some remarkable groups. For further details, see Conway and Sloane (1993). As a preliminary to this you should consider the following. The *kissing number* for these lattices is the maximum number of spheres that can fit around a central sphere S so that every sphere touches (kisses) S . In dimension 2, the kissing number is well-known to be six, and in dimension 3 it is, as noted above, twelve with some room to spare. But in dimension 8 it is 240, and in dimension 24 it is 196560! The first of these lattices has connections with the Mathieu group M_{24} , and the second with the sporadic group called the ‘Monster’ or ‘Friendly Giant’, see Chapter 12, the ATLAS (1985), and the reference quoted above.

Permutations

Permutations play a vital role in group theory, especially in the early development. If X is a set and S_X denotes the collection of all permutations on X (that is, bijections of X to itself), then this collection forms a group under the operation of composition called the *symmetric group* on X . If X is finite with n elements, we usually take X to be the set $\{1, 2, \dots, n\}$ and write S_n for S_X . See page 12 for the case $n = 3$. Note that S_n is non-Abelian if $n > 2$, and has order $n!$ (count all possible maps). As with many other groups, the symmetric groups have a number of important subgroups, that is, subsets that form groups; see Definition 2.11. For example, the *alternating group* A_n which is the group contained in S_n of all even permutations (a permutation is *even* if it can be expressed as an even number of interchanges of pairs of symbols; see Section 3.1)

Examples from Analysis

Some classes of functions form groups. For example, let Z denote the set of all continuous, strictly-increasing functions f which map $[0, 1]$ onto $[0, 1]$, and satisfy $f(0) = 0$ and $f(1) = 1$. This set Z forms a group if the operation is taken to be composition of functions (the identity function f_0 , where $f_0(x) = x$ for all x , acts as the neutral element, and inverses exist as the functions f are continuous and strictly monotonic). We can construct further groups (subgroups) inside this one, for instance, we could consider only those functions in Z which are differentiable. These are examples of ‘topological groups’, see page 6.

Free Groups and Presentations

This construction provides another way to introduce groups, it will be discussed in more detail in Section 3.4 and Web Section 4.7. Consider an *alphabet* of letters $A = \{a, a', b, b', \dots\}$. The letter a' is going to act as the inverse of a , *et cetera*, see page 57. A *word* $c_1c_2 \cdots c_k$ consists of a finite string of letters c_i from the alphabet A , for example,

$$aabb'a', b, \text{ or } ababa$$

are words. The set of words with the operation of concatenation forms a semigroup; to obtain a group we proceed as follows. We define a *reduced word* as a word in which all pairs of consecutive letters $aa', a'a, bb', \dots$ do not occur or have been removed, for example, $aabb'a'$ reduces to a , whilst b and $aba'b'a$ are reduced. As a' will act as the inverse of a , *et cetera*, each of these removals corresponds to the use of axiom (iv) in Definition 2.2. The operation of the group is as for the semigroup, that is concatenation—write one reduced word and then write the second reduced word immediately following the first, except that the resulting word must be reduced by removing all pairs $aa', a'a, bb', \dots$ if they are formed by the concatenation, or by previous removals. For instance,

$$\text{the product of } ac'b \text{ and } b'ca'c \text{ is } c.$$

The *empty word*—that is the word with no symbols from A which is written as e where $e \notin A$ —acts as the neutral element of the group, and inverses are constructed as in the example above—for instance, the inverse of $aab'cbc'$ is $cb'c'ba'a'$. The group is denoted by $\langle a, b, c, \dots \rangle$ (in this notation it is assumed that the letters e, a', b', \dots are also present), and the letters a, b, c, \dots are the *generators*. It is called *free* because there are no constraints on possible words other than those ensuring the group properties hold; note that all free groups are necessarily infinite. A free group with just one generator a , say, is called an *infinite cyclic group*, it is isomorphic to \mathbb{Z} and so we denote it either by $\langle a \rangle$ or by \mathbb{Z} . Non-free groups have more condi-

tions called *relations*, or sometimes *defining relations*. For example, the finite cyclic group C_n of order n can be treated as the infinite cyclic group $\mathbb{Z} \simeq \langle a \rangle$ with the extra relation

$$a^n = e.$$

In this group, each time a^n occurs it is replaced by the neutral element e in the same way that terms of the form aa' or $a'a$ are replaced by e . In Section 3.4, we shall see that this method for constructing groups has a number of advantages, but also some disadvantages. For instance, in a few cases it may be difficult, or sometimes impossible, to determine the group order.

Elliptic Curves

The collection of solutions of some equations can be formed into groups. For example, consider the set of rational solutions of the equation

$$y^2 = x^3 + k \quad \text{where } k \in \mathbb{Z} \setminus \{0\}. \quad (2.2)$$

Suppose $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ lie on the curve. The straight line P_1P_2 passing through the points P_1 and P_2 meets the curve in exactly one further point $P_3 = (x_3, y_3)$, say, and the pair (x_3, y_3) forms a new solution of (2.2), and if $x_1, \dots, y_2 \in \mathbb{Q}$ then also $x_3, y_3 \in \mathbb{Q}$. If $P_1 = P_2$, then the line is the tangent to the curve at P_1 ; and the whole procedure is called the *chord–tangent process*.

Points on the curve with rational coordinates form the elements of a group, and the operation is defined using the chord–tangent process. It is closed because, given rational points P_1 and P_2 on C , a rational point P_3 on C always exists, and we set $P_1 + P_2 = -P_3$. The neutral element is the ‘point at infinity’ on the curve in the y -direction. (To set this procedure up properly we use homogeneous coordinates $(x : y : z)$, where

$$(tx : ty : tz) = (x : y : z) \quad \text{for all } t \in \mathbb{Q}^*.$$

The usual notation for a point (x, y) is identified with $(x : y : 1)$, and the point $(x : y : 0)$ lies on the ‘line at infinity’. Equation (2.2) becomes $y^2z = x^3 + kz^3$. The point $(0 : 1 : 0)$, the neutral element of the group, clearly lies on the curve, and is the ‘point at infinity’ in the y -axis direction. We set $P_1 + P_2$ to equal ‘minus’ P_3 to obtain a valid inverse operation, so using the standard two variable (affine) coordinates, the inverse of the point $P_1 = (x_1, y_1)$ is $-P_1 = (x_1, -y_1)$.) In this ‘projective geometry’ all vertical lines ‘meet’ at the point at infinity $(0 : 1 : 0)$, and some results from algebraic geometry are needed to prove associativity. These groups can be finite or infinite, and they are Abelian because the line through the points P_1 and P_2 is clearly the same as the line through P_2 and P_1 . See for example Rose (1999), Chapters 15 and 16, for further details.

Examples from Topology

The basic structure of a topological space is best described using groups. For example, the *fundamental group* of a space, which was first defined by H. Poincaré over a century ago, is constructed as follows:

Fix a point P in a path-wise connected topological space T , and consider the set of all continuous closed and directed loops from P to P . Call two loops ‘equivalent’ if one can be continuously deformed into the other (topologists call them ‘homotopic’), the group operation is composition. The neutral element is the set of loops that can be continuously contracted to the point P , and the inverse of the loop L is L with its direction reversed. For instance, the fundamental group of the real plane \mathbb{R}^2 with the origin removed is the infinite cyclic group (all loops through P that do not enclose the origin can be contracted to P , but, for example, a loop that passes around the origin clockwise four times, say, cannot be contracted and ‘equals’ four times a loop which passes around the origin clockwise only once).

Although the definition appears to depend on the point $P \in T$, it can be shown that fundamental groups for different points P are isomorphic; that is, there exists a fundamental group for the space T . Further details can be found in a standard book on general topology, for example, Kelley (1955) or Willard (1970). Algebraic topology is another area where groups—homology and cohomology groups—provide insights into the structure of topological spaces, see for example Benson (1991).

Examples from the Physical Sciences

Particle physicists make extensive use of group theory. Many of the essential properties of the basic constituents of matter are best described using the language and properties of groups. At least one elementary particle was discovered using the abstract theory. A collection of particles was associated with a particular class of groups, and it was realised that there was one more group (that is, 28) than known particles in this collection (at the time, 27); this led the experimental workers to look for the ‘missing’ particle (called Ω^-), and it was duly found a few years later! An excellent ‘down-to-earth’ account of this topic is given in Close (2006), and Williams (1994) provides a good technical introduction.

Some chemists use groups to describe the structure of molecules. A notable example was given in 1985 when a crystalline form of carbon, called Carbon60, was discovered by the chemists Kroto, Curl and Smalley;² its structure is closely related to that of a dodecahedron, and so also to the alternating group A_5 ; the subsection on symmetries above, Section 3.2, and Web Section 3.6 all give some details.

²They were awarded the Nobel prize in chemistry for this work.

2.3 Subgroups, Cosets and Lagrange's Theorem

Most groups contain a number of smaller groups using the same operation, we shall consider these now.

Definition 2.11 A *subgroup* H of a group G is a non-empty subset of G which forms a group under the operation of G .

We write $H \leq G$ when H is a subgroup of G . For example, if G is the group \mathbb{Q} , then \mathbb{Z} is a subgroup, that is, $\mathbb{Z} \leq \mathbb{Q}$. But note that \mathbb{Q}^+ is not a subgroup of \mathbb{Q} even though the underlying set in the first group is contained in the second; reader, why?

Definition 2.12 (i) A subgroup J of a group G is called *proper* if $J \neq G$, this is denoted by $J < G$.

(ii) The singleton set $\{e\}$ forms a subgroup of all groups, it is called the *neutral subgroup* and is denoted by $\langle e \rangle$.

(iii) A subgroup H of a group G is called *maximal* in G if it is a *proper* subgroup of G , and whenever a subgroup J exists satisfying $H \leq J \leq G$, then either $J = H$ or $J = G$, so no subgroup lies strictly between H and G .

Notes (a) The neutral subgroup $\langle e \rangle$ is sometimes called the identity, trivial, or unit, subgroup; see page 4.

(b) Clearly $G \leq G$; so all groups with more than one element have at least two subgroups; some have no more, see Theorem 2.34.

(c) Maximal subgroups are not necessarily 'large'. For an extreme example, consider the alternating group A_{13} which has order 3113510400, remarkably it possesses a maximal subgroup of order 78. Also arbitrarily large groups with maximal subgroups of order 2 exist—Problems 3.20 and Corollary 6.12.

(d) There are connections between maximal subgroups and generators, see Problem 2.13 and Section 10.2, and reasoning with maximal subgroups is used in several proofs, for example, in that for the Frattini Argument (Lemma 6.14).

The next result gives conditions for a group subset to be a subgroup.

Theorem 2.13 If H is a subset of G , then $H \leq G$ if, and only if,

- (a) H is non-empty, and
- (b) whenever $a, b \in H$, we also have $a^{-1}b \in H$.

Proof Clearly (a) and (b) are valid if $H \leq G$ (Definitions 2.2 and 2.11). Conversely, suppose (a) and (b) hold for a subset H of G . By (a), there is at least one element $a \in H$, and so, by (b), $e = a^{-1}a \in H$. Applying (b) again, we have, as $a, e \in H$, $a^{-1} = a^{-1}e \in H$, and so H is closed under inverses. Thirdly, if $a, b \in H$, then $a^{-1} \in H$, and so together these give

$ab = (a^{-1})^{-1}b \in H$ by Theorem 2.7(ii), that is, H is closed under the operation of G . Finally, we note that associativity holds in H because it holds in G ; the result follows. \square

There is also a 'right-hand version' of this result where in (b) ' $a^{-1}b \in H$ ' is substituted by ' $ab^{-1} \in H$ '. In practice, it is often better to replace (b) by:

- (b1) if $a, b \in H$ then $ab \in H$, and
- (b2) if $a \in H$ then $a^{-1} \in H$.

For example, suppose $G = GL_2(\mathbb{Q})$ and H is the subset of these matrices with determinant 1. The identity matrix I_2 belongs to H , and so H is not empty. Also if $A, B \in H$, then $\det A = \det B = 1$ and so, as $\det(AB) = \det(A)\det(B) = 1$, we deduce $AB \in H$. Finally, if $C \in H$, then $1 = \det C = \det C^{-1}$, and so $C^{-1} \in H$; this gives $H \leq G$. We use the notation $SL_2(\mathbb{Q})$ for H , see Section 3.3. Some further examples are given in Problem 2.10.

We consider now some set-theoretic operations on subgroups.

Corollary 2.14 (i) If $H \leq J$ and $J \leq G$, then $H \leq G$, that is the subgroup relation is transitive.

(ii) If $H, J \leq G$ and $H \subseteq J$, then $H \leq J$.

Proof Both of these results follow from Theorem 2.13, see Problem 2.5. \square

Intersections of subgroups are always subgroups (but unions are usually not subgroups because closure fails). See the note concerning subgroup lattices on page 32.

Theorem 2.15 Suppose I is a non-empty index set. If $H_i \leq G$, for each $i \in I$, and $J = \bigcap_{i \in I} H_i$, then $J \leq G$.

Proof As $e \in H_i$ for all $i \in I$, we have $e \in J$, so J is not empty. Secondly, if $a, b \in J$, then $a, b \in H_i$ for all $i \in I$, but each $H_i \leq G$ so, by Theorem 2.13, $a^{-1}b \in H_i$, for all $i \in I$, which shows that $a^{-1}b \in J$. Now use Theorem 2.13 again. \square

In Section 2.1 (page 13), we introduced the notion of a *generating set* for a group, this can be formally defined by

Definition 2.16 A subset X of the underlying set of a group G is said to *generate* G if the intersection of all subgroups of G that contain X coincides with G , or to put this another way, the only subgroup of G that contains X is G itself. This intersection is denoted by $\langle X \rangle$.

Theorem 2.17 Suppose X is a non-empty subset of the underlying set of the group G . The set X generates G if and only if the set of all products of powers (positive and negative) of elements of X equals G .

Proof By Theorem 2.15 and Definition 2.16, $\langle X \rangle \leq G$. Suppose $\langle X \rangle = G$. Let Z denote the set of all powers of products of elements of X ; $Z \subseteq G$. The set Z is non-empty as X is non-empty, and so $Z \leq G$ by Theorem 2.13 and the definition of Z . Also $X \subseteq Z$, and so Z is one of the subgroups used in the formation of the intersection $\langle X \rangle$; hence $\langle X \rangle \leq Z \leq G$. Therefore, as X generates G (by supposition), we have $Z = G$.

For the converse suppose $Z = G$. Now for given H , if $X \subseteq H$ and $H \leq G$, then $Z \leq H$, again by Theorem 2.13 and the definition of Z . This holds for all such H , and so it holds for $\langle X \rangle$ by Theorem 2.15; that is, $Z \leq \langle X \rangle$. But by our supposition $Z = G$, and so $\langle X \rangle = G$, and the result is proved. \square

We set $\langle X \rangle = \langle e \rangle$, if X is empty.

Now we consider group elements in more detail. For $g \in G$ we write $\langle g \rangle$ for the set of powers of $g \in G$, that is $\langle g \rangle = \{g^t : t \in \mathbb{Z}\}$; see Section 4.3. We have

Theorem 2.18 *If $g \in G$ then $\langle g \rangle \leq G$.*

Proof The set $\langle g \rangle$ is clearly not empty, and if $m, n \in \mathbb{Z}$, then $g^m, g^n \in \langle g \rangle$, and $(g^m)^{-1}g^n = g^{n-m} \in \langle g \rangle$. Result follows by Theorems 2.9 and 2.13. \square

We say that g is a *generator* of the subgroup $\langle g \rangle$ of G (page 13). This result ensures that almost all groups have at least some non-neutral proper subgroups, see Theorem 2.34 for the exceptions.

Examples (a) Let $G = \mathbb{Z}$ and $g = 7$, then $\langle 7 \rangle$ is the proper subgroup of \mathbb{Z} consisting of the set of integers divisible by 7.

(b) Secondly, let $G = (\mathbb{Z}/7\mathbb{Z})^*$ and $g = 3$. In this case, the subgroup $\langle 3 \rangle$ is G itself because the powers of 3 modulo 7 generate the whole group; the reader should check this and also consider the case $g = 2$.

Theorem 2.18 and these examples suggest the following

Definition 2.19 Let $g \in G$.

- (i) The subgroup $\langle g \rangle$ given by Theorem 2.18 is called *cyclic*.
- (ii) The *order* of g , denoted by $o(g)$, is defined by $o(g) = o(\langle g \rangle)$; that is, $o(g)$ equals the order of the cyclic subgroup generated by g in G .
- (iii) An element of order 2 is called an *involution*.
- (iv) The *exponent*, if it exists, of a group G is the least common multiple of the orders of all of the elements of G ; that is, the least positive integer m with the property: $g^m = e$ for all $g \in G$.

Notes (a) All parts of this definition are relative to a fixed group G .

(b) Orders can be finite or infinite, and if the orders of two elements are finite it does not follow that the order of their product is finite (Problem 2.7).

(c) If G is finite, it has an exponent which is not greater than $o(G)$. The group \mathbb{Q} is an example of an infinite group with no exponent. In 1902, W. Burnside (1852–1927) conjectured that a group G with finite generating set and finite exponent must be finite, and this is true if G is Abelian. But it can be false if G is not Abelian as was shown by Adian and Novikov in 1968 for a group with an exponent larger than 665; see Vaughan-Lee (1993).

(d) Elements of order 2 are called *involutions* to signal the fact that they play a unique role in the theory, particularly to CFSG. (It is the subgroups called *centralisers* of these involutions, see Section 5.2, that play this vital role.) Also, apart from the neutral element e they are the only group elements which equal their own inverses. Further properties are given in Problems 2.28, 3.1(iv) and 3.20, and in the note about Coxeter Groups on page 64.

We illustrate these concepts with the following result.

Corollary 2.20 *If a group G has exponent 2, then it is Abelian.*

Proof Suppose $a, b \in G$, then $ab \in G$ and $e = (ab)^2 = abab$. Multiplying on the left by a and on the right by b , we obtain

$$ab = aeb = a(abab)b = a^2bab^2 = ba$$

as both a and b have order 2. This holds for all $a, b \in G$. □

Given a prime p , an Abelian group all of whose non-neutral elements have order p is called an *Elementary Abelian p -group*. We shall see later (Problem 4.18) that these groups can be treated as vector spaces defined over a p -element field. The corollary above shows that all groups of exponent 2 are of this type, this is not true for primes $p > 2$; an example is given in Problem 6.5.

Cosets and Lagrange's Theorem

For our next results, we require some new notation. If X and Y are non-empty subsets of a group G , then we write XY for the subset

$$XY = \{xy : x \in X \text{ and } y \in Y\} \subseteq G.$$

If X is the singleton set $\{x\}$, then we write xY for $\{x\}Y$ (and Yx for $Y\{x\}$). Note that if $X, Y, Z \subseteq G$ then, by associativity,

- (i) $X(YZ) = (XY)Z$, and
- (ii) $XY = YX$, if G is Abelian.

Definition 2.21 For $H \leq G$ and $g \in G$, the set $gH = \{gh : h \in H\}$ is called a *left coset* of H in G , and the set Hg is called a *right coset* of H in G .

Cosets play an important role in the theory, here they lead to our first major result—Lagrange’s Theorem, and in Chapter 4 they form part of the important ideas associated with factor groups. One of the origins of this work is Gauss’s development of modular arithmetic undertaken two centuries ago (page 18): if $G = \mathbb{Z}$ and $H = n\mathbb{Z}$, then the cosets are

$$kH = \{k + nz : z \in \mathbb{Z}\} \quad \text{for } k = 0, \dots, n-1;$$

the coset kH equals the set of integers congruent to k modulo n .

When referring to the set T of cosets of H in G , we often write $T = \{gH : g \in G\}$. Here we are using the convention that in an un-ordered set duplication is ignored, for instance, the set $\{\dots, a, a, \dots, a, \dots\}$ is the same as $\{\dots, a, \dots\}$. If we did not use this convention in the coset case, we would need to specify a unique g in each coset gH , and this would cause problems.

We begin with some basic lemmas. The first will be used often in the following pages, it characterises the coset representatives.

Lemma 2.22 *If $H \leq G$ and $a, b \in G$, then*

$$aH = bH \quad \text{if and only if} \quad a \in bH \quad \text{if and only if} \quad b^{-1}a \in H.$$

There is an exactly similar result for right cosets; the reader should write it out and redo the following proof in this second case.

Proof Suppose firstly $aH = bH$. As H is a subgroup, $e \in H$ and so $a = ae \in aH = bH$. Secondly, suppose $a \in bH$, then there exists $h \in H$ satisfying $a = bh$, and so $b^{-1}a = h \in H$. Lastly, suppose $b^{-1}a \in H$. As above this gives $a = bh$ for some $h \in H$, and hence

$$ah_1 = bhh_1 \in bH \quad \text{for all } h_1 \in H;$$

that is, $aH \subseteq bH$. For the converse inclusion, as $H \leq G$, we have by Theorem 2.13, $a^{-1}b = (b^{-1}a)^{-1} \in H$, and so we can repeat the previous argument with a and b interchanged, the equation $aH = bH$ follows. \square

To derive Lagrange’s Theorem, we require the following three lemmas, the first shows that cosets are either disjoint or identical.

Lemma 2.23 *If $H \leq G$, then the underlying set of G can be expressed as a disjoint union of the collection of all left cosets of H in G . There is an exactly similar result for right cosets.*

Proof Clearly, each element $g \in G$ belongs to a left coset because $g \in gH$. Suppose further $g \in aH$ and $g \in bH$, then by Lemma 2.22, $aH = gH = bH$, and the lemma follows. The right coset version follows similarly. \square

Lemma 2.24 *If $H \leq G$ and $g \in G$, then $o(H) = o(gH) = o(Hg)$.*

Proof We give the proof for left cosets, the right coset result is proved similarly. To establish this lemma, we construct a bijection between the sets involved. Let ϕ be the map from H to gH defined by

$$h\phi = gh;$$

see note on ‘left or right’ on page 68. If $h\phi = h'\phi$ then $gh = gh'$, and by cancellation (Theorem 2.6) this gives $h = h'$, and so ϕ is injective, hence it is bijective because it is clearly surjective. \square

Lemma 2.25 *If $H \leq G$, then the number (cardinality) of left cosets equals the number of right cosets.*

Proof As in the previous proof, we construct a bijection between the sets. Let θ be the map from the set of left cosets to the set of right cosets given by

$$(gH)\theta = Hg^{-1}.$$

This is well-defined; for if $gH = g_1H$, then $Hg^{-1} = Hg_1^{-1}$ (use left and right versions of Lemma 2.22 and closure under inverses). It is also clearly surjective because each element of G is the inverse of some element in G (Theorem 2.8). To prove injectivity, suppose

$$(gH)\theta = (g_1H)\theta, \quad \text{that is} \quad Hg^{-1} = Hg_1^{-1}.$$

Using the right-hand version of Lemma 2.22, this gives $g_1^{-1} \in Hg^{-1}$, and hence $g_1^{-1} = hg^{-1}$ for some $h \in H$. Therefore, $g_1 = gh^{-1} \in gH$ (as H is a subgroup), and so $g_1H = gH$ by Lemma 2.22 again. \square

Having established these lemmas, we can now derive Lagrange's Theorem. Much of the early work in algebra was concerned with properties of polynomials defined over the rational numbers. J.-L. Lagrange (1736–1813), an Italian mathematician working in France, studied these polynomials as well as in many other topics in mathematics. He postulated a result similar to that given in the last part of Problem 5.1 which relies on what we now call ‘Lagrange's Theorem’; and it is for this reason that the following result is so named. In fact, Galois gave the first proof of the theorem for permutation groups in 1832, and it was probably C. Jordan (1838–1932) who gave the first proof for general groups some thirty years later.

We begin by making the following

Definition 2.26 Let $H \leq G$. The number (cardinality) of left cosets of H in G is called the *index* of H in G , it is denoted by $[G : H]$.

By Lemma 2.25, this equals the number of right cosets of H in G .

Theorem 2.27 (Lagrange's Theorem) *If $H \leq G$ then $o(G) = o(H)[G : H]$.*

Proof By Lemma 2.23, the underlying set of G is a disjoint union of $[G : H]$ cosets, and by Lemma 2.24, each of these cosets has the same cardinality (number of elements), that is $o(H)$, the theorem follows. \square

This result is particularly useful in the finite case where it shows that H can only be a subgroup of G if $o(H) \mid o(G)$; that is, the prime factorisation of the order of a group G is an important invariant of G . For instance, a group of order 30 cannot have subgroups of order 4, 7, 8, 9, 11, \dots , 29. Also, it cannot have elements of order 4, 7, \dots , see Definition 2.19. In the infinite case, the theorem shows that either the order of the subgroup, or the index (or both), must be infinite. Note that there exist infinite groups all of whose proper subgroups are finite, see Problem 6.7.

2.4 Normal Subgroups

The last topic in this chapter concerns a special type of subgroup in which left and right cosets are equal, they play a vital role in the theory. These subgroups were first defined by Galois in the 1820s when he was working on the solution of polynomial equations by radicals; see the Introduction to Chapter 11.

Definition 2.28 (i) Let $K \leq G$. The subgroup K is called *normal* in G if, and only if,

$$gK = Kg \quad \text{for all } g \in G.$$

This is denoted by $K \triangleleft G$.

(ii) If $g, h \in G$, $h^{-1}gh$ is called the *conjugate* of g by h in the group G .

(iii) For a fixed element $g \in G$, the set $\{h^{-1}gh : h \in G\}$, that is, the set of conjugates of g in G , is called the *conjugacy class* of g in G ; see also Definition 5.17.

Notes (a) The subgroups $\langle e \rangle$ and G are normal in G for all groups G .

(b) If G is Abelian, all subgroups are normal, all conjugates of g equal g , and so the conjugacy class of g in G is $\{g\}$.

(c) We reserve the symbol ' K ', possibly with primes or subscripts, to denote a normal subgroup, but other symbols will occasionally be used where necessary. In Chapter 4, we discuss the connection between normal subgroups and *kernels* of homomorphisms— K for kernels and so also for normal subgroups.

(d) Conditions stronger than normality are useful at times. The first is *characteristic*, for a definition and basic properties see Problem 4.22; the main point is that characteristic is a transitive property whereas normality is not. Some authors use an even stronger property called *fully invariant* which is defined similarly to characteristic except that in the definition on page 89 the word 'automorphism' is replaced by 'endomorphism', see Definition 4.2.

The following theorem gives two conditions for normality, see note below the statement of Lemma 4.6.

Theorem 2.29 (i) If $K \leq G$, then the following conditions are equivalent:

- (ia) $K \triangleleft G$;
- (ib) for all $g \in G$, $g^{-1}Kg \subseteq K$;
- (ic) for all $g \in G$ and all $k \in K$, $g^{-1}kg \in K$.

(ii) Suppose $K \triangleleft G$. If $k \in K$, then all conjugates of k in G belong to K , and K is the union of a collection of the conjugacy classes of G .

Proof Note first that both parts of (ii) follow immediately from (i). Suppose (ia) holds, so if $g \in G$, $gK = Kg$ by definition. Hence, for all $k \in K$, we can find $k' \in K$ to satisfy

$$gk' = kg, \quad \text{that is} \quad g^{-1}kg = k' \in K,$$

which gives (ib). Secondly, note that (ic) follows immediately from (ib) (as $g^{-1}kg \in g^{-1}Kg$). Finally, suppose (ic) holds. So if $g \in G$ and $k \in K$, we can find $k' \in K$ to satisfy

$$g^{-1}kg = k', \quad \text{which gives} \quad kg = gk' \quad \text{and so} \quad K \subseteq gK,$$

as this argument holds for all $k \in K$. For the converse, we have $gkg^{-1} = (g^{-1})^{-1}kg^{-1} \in K$, and so we can find $k'' \in K$ to satisfy $gkg^{-1} = k''$ or $gk = k''g$. This gives the reverse inclusion and (ia) follows. \square

Notes To prove that $K \triangleleft G$ it is necessary to prove both $K \leq G$ and K is normal in G . Secondly, normality is not transitive (cf. Corollary 2.14); that is, if $K \triangleleft G$ and $H \triangleleft K$, it does not follow that $H \triangleleft G$; see Problem 2.19(iii) for an example. On the other hand, if $K \triangleleft G$ and $K \leq H \leq G$, then $K \triangleleft H$; see Problem 2.14. A stronger property called *characteristic* which is transitive was mentioned in (d) opposite.

Our first application of the normal subgroup concept answers the question: When is the product HJ of two subgroups H and J itself a subgroup? Note that in general HJ is not a subgroup because it is not closed under the group operation. We use the notation $H \vee J$ (or sometimes $\langle H, J \rangle$)—the *join* of H and J —for the group generated by the elements of both H and J (Definition 2.16). Clearly $HJ \subseteq H \vee J$, we have

Theorem 2.30 Suppose $H, J \leq G$.

- (i) If either H or J is a normal subgroup of G , then $HJ \leq G$ and $H \vee J = HJ = JH$.
- (ii) If both $H \triangleleft G$ and $J \triangleleft G$, then $HJ \triangleleft G$.

Proof (i) Suppose $h_i \in H$, $j_i \in J$, $i = 1, 2$, and $H \triangleleft G$ (the proof is similar if $J \triangleleft G$). Then $j_1^{-1}(h_1^{-1}h_2)j_1 = h^*$ for some $h^* \in H$ (as $h_1^{-1}h_2 \in H$, $j_1 \in J$ and $H \triangleleft G$). Hence

$$(h_1j_1)^{-1}(h_2j_2) = j_1^{-1}h_1^{-1}h_2j_1j_1^{-1}j_2 = h^*j_1^{-1}j_2 \in HJ,$$

and, as HJ is clearly not empty, $HJ \leq G$ follows by Theorem 2.13. A similar argument shows that a product of terms each of the form hj , for $h \in H$ and $j \in J$, is itself of this form; that is, $HJ = H \vee J$. The last equation in (i) follows because $H \vee J = J \vee H$, or we can show directly as above that $HJ \subseteq JH$ and $JH \subseteq HJ$.

(ii) By (i), we only need to check normality. If $g \in G$, $h \in H$ and $j \in J$, we have $g^{-1}h j g = g^{-1}h g g^{-1}j g \in HJ$ by hypothesis, the result follows. \square

Subgroup Lattices

Using Corollary 2.14 and Theorems 2.15 and 2.30, the collection of subgroups of a group forms a (complete) lattice L , that is, a non-empty partially ordered set (Definition A.5 in Appendix A) in which every subset has a greatest lower bound and a least upper bound in L . Note that both the intersection and the join of two subgroups of a group G are themselves subgroups of G . Some examples are given in Chapter 8. The structure of this lattice can have an important bearing on the group in question. The first major result (Ore 1938) states that the lattice of a finite group G is distributive (that is, $H \vee (J \cap K) = (H \vee J) \cap (H \vee K)$, *et cetera.*) if and only if G is cyclic. It should be noted that non-isomorphic groups can have identical subgroup lattices; see Problem 6.4. For a detailed account of this aspect of the theory, the reader should consult Schmidt (1994).

The *centre* of a group is an important example of a normal subgroup, it is given by

Lemma 2.31 *In a group G , the set*

$$J = \{a \in G : ag = ga \text{ for all } g \in G\}$$

forms a normal Abelian subgroup of G .

Proof Suppose $a \in J$. For all $g \in G$, we have $eg = ge$, $ag = ga$ implies $a^{-1}g^{-1} = g^{-1}a^{-1}$ by Theorem 2.7, and if $ag = ga$ and $bg = gb$ then $abg = agb = gab$; and so $J \leq G$ by Theorem 2.13. Also J is Abelian by definition. Lastly, note that $ag = ga$ implies $g^{-1}ag = a$, and so $J \triangleleft G$ by Theorem 2.29. \square

Definition 2.32 The subgroup J of G given in Lemma 2.31 is called the *centre* of G , it is denoted by $Z(G)$.

Notes The notation $Z(G)$ is used because German authors call this subgroup the *Zentrum*. The centre of a group G gives some important information about G . Clearly, $Z(G) = G$ if and only if G is Abelian. On the other hand, some groups are *centreless*, that is, $Z(G) = \langle e \rangle$; examples are D_3 and S_4 , see Problem 2.26. A centreless group can in some ways be treated as the opposite of an Abelian group.

We end this chapter by introducing *simple groups*. We shall show later they can be treated as the basic ‘building blocks’ for the construction of all finite and some infinite groups; see Chapter 9.

Definition 2.33 A group G is called *simple* if it contains no proper non-neutral normal subgroup.

The term ‘simple’ is perhaps not well-chosen because some simple groups are very complicated! But as noted above they can be used as the basic constituents of all groups; of course, they are all centreless. A full list of finite simple groups is now known; see the ATLAS (1985) and Chapter 12. Many simple groups are given by Lagrange’s Theorem for we have

Theorem 2.34 *If $o(G)$ is a prime number, then the group G is simple and cyclic.*

For the converse see Theorem 9.6.

Proof By Lagrange’s Theorem (Theorem 2.27), the order of a subgroup of G divides $o(G)$. But in this case, the only positive divisors of the integer $o(G)$ are 1 and p , hence G has no proper non-neutral subgroups at all, and so clearly no proper non-neutral normal subgroups. Also by Theorem 2.18 and Definition 2.19, every element has order 1 or p . There is only one element, e , of order 1 (Lemma 2.4). Hence G has $p - 1$ elements of order p ; let a be one of them. As a has p distinct powers (including $p^0 = e$), it follows that all elements of G equal powers of a , and so G is cyclic. \square

In fact, ‘most’ simple groups (counted by the size of their orders) are of this type, that is Abelian (and cyclic). For example, there are 173 (isomorphism classes of) simple groups with order less than 1000 but only five are non-Abelian. The construction of non-Abelian simple groups is a much more difficult task, in the next chapter we introduce the first groups of this type—*alternating groups*, and more will be discussed in Chapter 12. These include a number of infinite classes of matrix groups, especially the linear groups $L_n(q)$ and the unitary groups $U_n(q)$, and also 26 (!) so called *sporadic groups*. These groups range in size from 7920 (Mathieu group M_{11}) to about 10^{84} (Friendly giant M) and they have a wide variety of constructions. The existence of these non-Abelian simple groups is surely one of the most interesting and challenging aspects of the theory.

2.5 Problems

A number of the problems given below have important applications in the sequel. For an explanation of the symbols \star and \blacklozenge , see page 9.

Problem 2.1 (i) Write out a proof of Theorem 2.8.

(ii) Using induction on n , prove the *generalised associativity law* for groups: If $g_1, \dots, g_n \in G$, then all expressions formed by inserting or deleting brackets (in corresponding pairs) in the term $g_1 \odot \cdots \odot g_n$ are equal.

Problem 2.2 Show that the following sets with operations form groups, and indicate which are Abelian.

- (i) $\mathbb{Z}/7\mathbb{Z}$ with addition modulo 7.
- (ii) $(\mathbb{Z}/7\mathbb{Z})^*$ with multiplication modulo 7.
- (iii) The set \mathbb{Q} with the operation $*$ where, for $a, b \in \mathbb{Q}$, we have $a * b = a + b + 3$.
- (iv) $GL_2(\mathbb{Q})$ with matrix multiplication, see also Problem 2.10 below.
- (v) The set of powers of products Q (that is, the group generated by) of the complex matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ with the operation of matrix multiplication. What is the order of this group?
- (vi) Let $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ where the symbol ∞ satisfies the usual naive rules: $1/0 = \infty$, $1/\infty = 0$, $\infty/\infty = 1$ and $1 - \infty = \infty = \infty - 1$. Define six functions mapping $\overline{\mathbb{R}}$ onto itself by:

$$\begin{aligned} f_1(x) &= x, & f_2(x) &= \frac{1}{x}, & f_3(x) &= 1 - x, \\ f_4(x) &= \frac{1}{1 - x}, & f_5(x) &= \frac{x}{x - 1}, & f_6(x) &= \frac{x - 1}{x}. \end{aligned}$$

Show that this set forms a finite group under the operation of composition.

- (vii) Let R denote the real plane \mathbb{R}^2 , let d denote the standard distance function (metric) on R , and let Θ denote the set of bijective maps of R to itself which preserve distance—if $x, y \in R$ and $\theta \in \Theta$, then $d(x, y) = d(\theta(x), \theta(y))$. A function of this type is called an *isometry*; rotation by $\pi/3$ about the origin is an example. Show that Θ with the operation of composition forms a group.

The reader needs to be convinced that all the sets with operations described in Section 2.2 are, in fact, groups.

Problem 2.3 Why are the following sets with operations not groups?

- (i) The integers \mathbb{Z} with subtraction.
- (ii) The set of odd integers with addition.
- (iii) The set $\left\{ \begin{pmatrix} a & r \\ 0 & b \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} c & 0 \\ s & d \end{pmatrix} \right\}$ where $a, b, \dots, s \in \mathbb{R}$ and $ab = 1 = cd$, with matrix multiplication.
- (iv) The rational numbers \mathbb{Q} with multiplication.

Problem 2.4 (i) Let S be a semigroup with cancellation, so it has closure under its operation which is associative, and for all $a, b \in S$, we can find $x, y \in S$ to solve the equations

$$ax = b \quad \text{and} \quad ya = b.$$

Show that S forms a group.

(ii)* If T is a semigroup, and for all $a \in T$ there is a unique $a^* \in T$ satisfying

$$aa^*a = a,$$

prove that T is a group.

Problem ♦ 2.5 If $H, J \leq G$ and in (iii) p is a prime, show that

- (i) If H is a subset of J , then $H \leq J$.
- (ii) $H \cap J = H$ if, and only if, $H \leq J$.
- (iii) If $o(H) = o(J) = p$, then either $H = J$ or $H \cap J = \langle e \rangle$.

Problem 2.6 Prove that if G is a group and $S \leq G$, then $SS = S$. Conversely, if T is a non-empty finite subset of G and $TT = T$, prove that $T \leq G$. Is this true if T is infinite?

Problem ♦ 2.7 (Order Function) Let $g, h \in G$. Prove the following properties of the order function.

- (i) $o(gh) = o(hg)$.
- (ii) If $o(g) = n$ and $m \in \mathbb{Z}$, then $o(g^m) = n/(m, n)$; see page 284.
- (iii) If $o(g) = m$ and $(m, n) = 1$, there exists $h \in G$ satisfying $h^n = g$.
- (iv) If $o(g) = m$, $o(h) = n$, and g and h commute, then $o(gh) = \text{LCM}(m, n)$; see part (vii).
- (v) If G is finite and $g \in G$, then $g^{o(G)} = e$, and $o(g) \mid \text{ex}(G)$ where ex denotes the exponent of G , see Definition 2.19.
- (vi) Suppose $g \in G$ and $o(g) = mn$ where $(m, n) = 1$. Show how to find unique $a, b \in G$ to satisfy $ab = g = ba$, $o(a) = m$ and $o(b) = n$.
- (vii) In (iv), if we drop the commutativity condition show that $o(gh)$ can be infinite. (Hint. Try $G = \text{GL}_2(\mathbb{Q})$.)

Problem 2.8 (i) Suppose G is a finite group and $o(G)$ is even. Is the number of elements of order 2 in G odd—does a group of even order always contain an involution? See also Cauchy's Theorem (Theorem 6.2).

(ii) Using the group $(\mathbb{Z}/p\mathbb{Z})^*$ where p is prime, see the definition on page 18, give a proof of Fermat's Theorem:

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{if } (a, p) = 1.$$

(iii) Using the same group as in (ii), show that $(p-1)! \equiv -1 \pmod{p}$, a result sometimes (wrongly) known as Wilson's Theorem. You are given: If $p > 2$, then $(\mathbb{Z}/p\mathbb{Z})^*$ contains exactly two elements of order at most 2 (Theorem B.13 in Appendix B).

Problem 2.9 (Multiplication Tables) Given a group G of order n with elements g_1, \dots, g_n where $g_1 = e$, we can form a square array or table, with n rows and n columns, whose (i, j) th entry is the product $g_i g_j$. Show that each row and each column of this table is a permutation of the elements g_1, \dots, g_n . What can you say about the first row and first column?

Is the converse true? That is, if we have a square array of elements such that each row and each column is a permutation of some fixed set, and the first row and column have the property mentioned above, does the corresponding array always form the multiplication table of a group?

Problem 2.10 Show that the following subsets are subgroups of the corresponding groups, and determine whether they are normal.

- (i) The set $\{1, -1\}$ in \mathbb{R}^* .
- (ii) The set of permutations on $Y = \{1, \dots, 6\}$ which leave 3 fixed in S_6 , the set of all permutations on Y ; see Section 3.2.
- (iii) The subsets of $GL_2(\mathbb{Q})$ of matrices (a) which have determinant 1, and (b) which are upper triangular (that is, the bottom left-hand entry is zero); see page 19 and Section 3.3.
- (iv) The set of complex numbers with absolute value 1 in \mathbb{C}^* .
- (v) The set of differentiable functions in the group Z described in the subsection on groups in analysis on page 21.

Problem 2.11 (i) Show that a finite subgroup of the multiplicative group of the complex numbers \mathbb{C}^* is cyclic. (Hint. Consider roots of unity.)

(ii) Find as many subgroups as you can of the additive group of the rational numbers \mathbb{Q} ; see Web Section 7.5.

Problem 2.12 List the left and right cosets of the subgroups given in Problem 2.10; note that the last part is not easy!

Problem 2.13 (i) Can a subset of a group G be the left coset of two distinct subgroups of G ?

(ii) If G is finite and has a unique maximal subgroup H , show that it is cyclic. (Hint. Consider an element in $G \setminus H$.)

Problem ♦ 2.14 (Normality Properties) Prove the following statements—all widely used in the sequel.

- (i) If $K \triangleleft G$ and $K \leq H \leq G$, then $K \triangleleft H$.
- (ii) A subgroup of the centre of a group G is normal in G .
- (iii) If $K_i \triangleleft G$ for $i = 1, 2, \dots, n$, then $\bigcap_{i=1}^n K_i \triangleleft G$.
- (iv) If $H, J, K \leq G$ and $K \triangleleft J$, then $K \cap H \triangleleft J \cap H$.

Problem ♦ 2.15 (i) Show that if $[G : H]$ is finite and $H \leq J \leq G$, then

$$[G : H] = [G : J][J : H].$$

(ii) Prove that if $H, J \leq G$ with $[G : H] = m$ and $[G : J] = n$, then $[G : H \cap J] \geq \text{LCM}(m, n)$, and equality occurs if, and only if, m and n are coprime.

Problem ♦ 2.16 (Derived Subgroup) If $g, h \in G$ we set $[g, h] = g^{-1}h^{-1}gh$, it is called the *commutator* of g and h . Also the subgroup of G generated by the set of all products of powers of the commutators of G is called the *derived* (or *commutator*) *subgroup* of G , and it is denoted by G' . In some cases, the set of commutators of a group does, in fact, form a subgroup of the group, but not always; for an example, see Rotman (1994), page 34. More generally, if $H, J \leq G$, we let $[H, J]$ denote the subgroup generated by all commutators of the form $[h, j]$ where $h \in H$ and $j \in J$; so, for example, $[G, G] = G'$. See also Problem 4.6(ii), and Section 11.1, especially page 234.

- (i) Show that $G' \triangleleft G$.
- (ii) Find G' when G is (a) \mathbb{Z} , (b) D_3 , and (c) Q , see Problem 2.2(v).
- (iii) Prove that if $J \leq G$ and $J \supseteq G'$, then $J \triangleleft G$ —an important fact with many applications.
- (iv) Show that if $K \triangleleft G$ and $K \cap G' = \langle e \rangle$, then $K \leq Z(G)$, and so in particular K is Abelian.
- (v) Finally, prove that if $K \triangleleft G$ and $J = [K, G]$, then $J \leq K$ and $J \triangleleft G$.

Problem 2.17 (Commutator Identities) Prove the following identities where $[a, b, c] = [[a, b], c]$ for a, b and c in the same group G . Identity (iv) is called the *Hall–Witt Identity*.

- (i) $[b, a] = [a, b]^{-1}$,
- (ii)* If $a, b \in G$, and both a and b commute with $[a, b]$, show that

$$\begin{aligned} [a^r, b^s] &= [a, b]^{rs} \quad \text{for } r, s \in \mathbb{Z}, \\ (ab)^t &= a^t b^t [b, a]^{t(t-1)/2} \quad \text{if } t \geq 0. \end{aligned}$$

(Use induction on t , (i), and the given relationship between G' and $Z(G)$.)

- (iii) $[ab, c] = (b^{-1}[a, c]b)[b, c]$ and $[a, bc] = [a, c](c^{-1}[a, b]c)$,
- (iv) $b^{-1}[a, b^{-1}, c]bc^{-1}[b, c^{-1}, a]ca^{-1}[c, a^{-1}, b]a = e$.
- (v) If $a_1, \dots, a_m, b_1, \dots, b_n \in G$ and $H = \langle a_1, \dots, b_n \rangle$, then we can express $[a_1 \dots a_m, b_1 \dots b_n]$ as a product of conjugates of $[a_i, b_j]$ by some $c_{ij} \in H$.
- (vi) If $H, J \leq G$ where $G = \langle H, J \rangle$, then $[H, J] \triangleleft G$.

Problem ♦ 2.18 Suppose $A, B, C \leq G$ and $A \leq B$. Show that

- (i) $B \cap (AC) = A(B \cap C)$,
- (ii) if $G = AC$ then $B = A(B \cap C)$,
- (iii) if $AC = BC$ and $A \cap C = B \cap C$, then $A = B$.

(Note that AC and/or BC may not be subgroups of G , also (i) and (ii) are sometimes known as *Dedekind's Modular Laws*.)

- (iv) Now suppose $A, B, C, D \leq G$ where also $AB, CD \leq G$. Show that if $A \leq D$ and $C \leq B$ then

$$AB \cap CD = AC(B \cap D).$$

Problem ♦ 2.19 Let $H, J \leq G$. Prove the following results.

- (i) If $[G : H] = 2$, then (a) $H \triangleleft G$, and (b) $a^2 \in H$ for all $a \in G$ —facts we use many times.
- (ii) If G is finite and $o(H) > o(G)/2$, then $H = G$ —no finite group can have a proper subgroup of order larger than half the group order. Further, if G is also simple and $J \leq G$, then $o(J) \leq o(G)/3$. For large simple groups, the denominator 3 can be replaced by a much bigger integer; see example below Theorem 5.15, page 101.
- (iii) Show that normality is not transitive (that is if $H \triangleleft J$ and $J \triangleleft G$, it does not follow that $H \triangleleft G$); one example occurs in D_4 using (i).
- (iv) If H and J are proper subgroups of G , prove that there exists $g \in G$ which does not belong to either H or J .
- (v) Show that $HJ \leq G$, if $HJ = JH$; cf. Theorem 2.30(i).

Problem 2.20 Using Corollary 2.20, Lagrange's Theorem (Theorem 2.27) and Problem 2.5, show that up to isomorphism there are only two groups of order 4, and only two groups of order 6—that is, there are exactly two isomorphism classes of groups of order 4, and also exactly two of order 6. (Hint. For order 6, show that the group always contains an element of order 3.) See Problem 4.2(i), different methods to prove these facts are given in Chapters 5 and 6.

Problem 2.21 Let G be a group. If $H_i \leq G$ and $[G : H_i]$ is finite for $i = 1, \dots, n$, show that

$$\left[G : \bigcap_{i=1}^n H_i \right] \leq \prod_{i=1}^n [G : H_i].$$

(Hint. Derive the result for $n = 2$ first.)

Problem 2.22 (Poincaré's Theorem) Prove that the intersection of a finite number of subgroups of G , each with finite index, is itself a subgroup of G with finite index.

Problem ♦ 2.23 If $H \leq G$ and $g \in G$, then $g^{-1}Hg$ is called a *conjugate subgroup* of H (Definition 2.28). Prove the following statements:

- (i) $g^{-1}Hg \leq G$,
- (ii) $o(g^{-1}Hg) = o(H)$,
- (iii) $g^{-1}Hg = \{j \in G : gjg^{-1} \in H\}$.

Problem ♦ 2.24 (Core of a Subgroup) If $H \leq G$, the *core* of H in G , $\text{core}(H)$, is defined by

$$\text{core}(H) = \bigcap_{g \in G} g^{-1}Hg,$$

see Section 5.2. Show that

- (i) $\text{core}(H) \triangleleft G$,
- (ii) $\text{core}(H)$ is the join of all normal subgroups of G which are contained in H ,
- (iii) $\text{core}(H)$ is the unique largest normal subgroup of G contained in H .

Problem 2.25 (Normal Closure of a Subgroup) If $H \leq G$, then the *normal closure* H^* of H is defined as the intersection of all normal subgroups of G which contain H . Show that

- (i) $H^* \triangleleft G$,
- (ii) $H^* = \langle g^{-1}Hg : g \in G \rangle$,
- (iii) H^* is the smallest normal subgroup of G containing H .

Problem 2.26 Find the centres of the following groups.

- (i) Integers \mathbb{Z} ,
- (ii) Dihedral group D_4 ,
- (iii) Dihedral group D_5 ,
- (iv) 2×2 General linear group $GL_2(\mathbb{Q})$, and
- (v) Permutation group S_3 .

Problem 2.27 Prove that if $H, J \leq G$, then

$$o(HJ)o(H \cap J) = o(H)o(J).$$

One method is as follows. Define a map $\theta : H \times J \rightarrow HJ$ by $(h, j)\theta = hj$. Show that if $g = hj$ where $h \in H$ and $j \in J$, then

$$g\theta^{-1} = \{(ha, a^{-1}j) : a \in H \cap J\},$$

by proving inclusion both ways round. Further, show that if $(ha, a^{-1}j) = (hb, b^{-1}j)$ then $a = b$, and so $o(g\theta^{-1}) = o(H \cap J)$. Lastly, count ordered pairs using the property $o(H \times J) = o(H)o(J)$.

Note that (a) HJ need not be a subgroup of G , and (b) a second proof of this result is given in Theorem 5.8.

Problem ♦ 2.28 Suppose G is a finite simple group of even order. Using Problem 2.8, show that G is generated by its involutions. (Hint. Note that an involution is self-inverse.) By the Feit–Thompson Theorem (Chapters 11 and 12), this shows that all finite non-Abelian simple groups are generated by a set of their involutions.

Problem 2.29 (Double Cosets) Suppose $H, J \leq G$ and $a \in G$. The set $H a J = \{h a j : h \in H, j \in J\}$ is called the *double coset* of a with respect to H and J . Show that

- (i) Each element of G belongs to exactly one double coset.
- (ii) G is the disjoint union of its double cosets.
- (iii) Each double coset (with respect to H and J) is a union of right cosets of H , and a union of left cosets of J .
- (iv) The number of right cosets of H in the double coset $H a J$ is $[J : J \cap a^{-1} H a]$. Hence

$$[G : H] = \sum_{c \in C} [J : c^{-1} H c]$$

provided this sum is finite, where C is a set of double coset representatives for H and J .

- (v) Using the notation set up in Section 3.1, if $G = S_4$, $a = (1, 2)$, $H = \langle (1, 2, 3) \rangle$, $J_1 = \langle (1, 2, 3, 4) \rangle$ and $J_2 = \langle (1, 4)(2, 3) \rangle$, write out the double cosets $H a J_i$ for $i = 1, 2$.

Problem 2.30 (i) Suppose $J_1 \leq J_2 \leq \dots \leq G$, that is we have an infinite sequence of subgroups of G . Let $J = \bigcup_{i=1}^{\infty} J_i$. Show that $J \leq G$. Note that in general a union of subgroups is not itself a subgroup.

- (ii) In (i), if J_i is simple for infinitely many i , show that J is also simple.

Problem 2.31 (Project) Whilst reading this book, list all those theorems which apply without restriction or caveat, for example, one of the first is Cancellation (Theorem 2.6).



<http://www.springer.com/978-1-84882-888-9>

A Course on Finite Groups

Rose, H.E.

2009, XII, 311 p., Softcover

ISBN: 978-1-84882-888-9